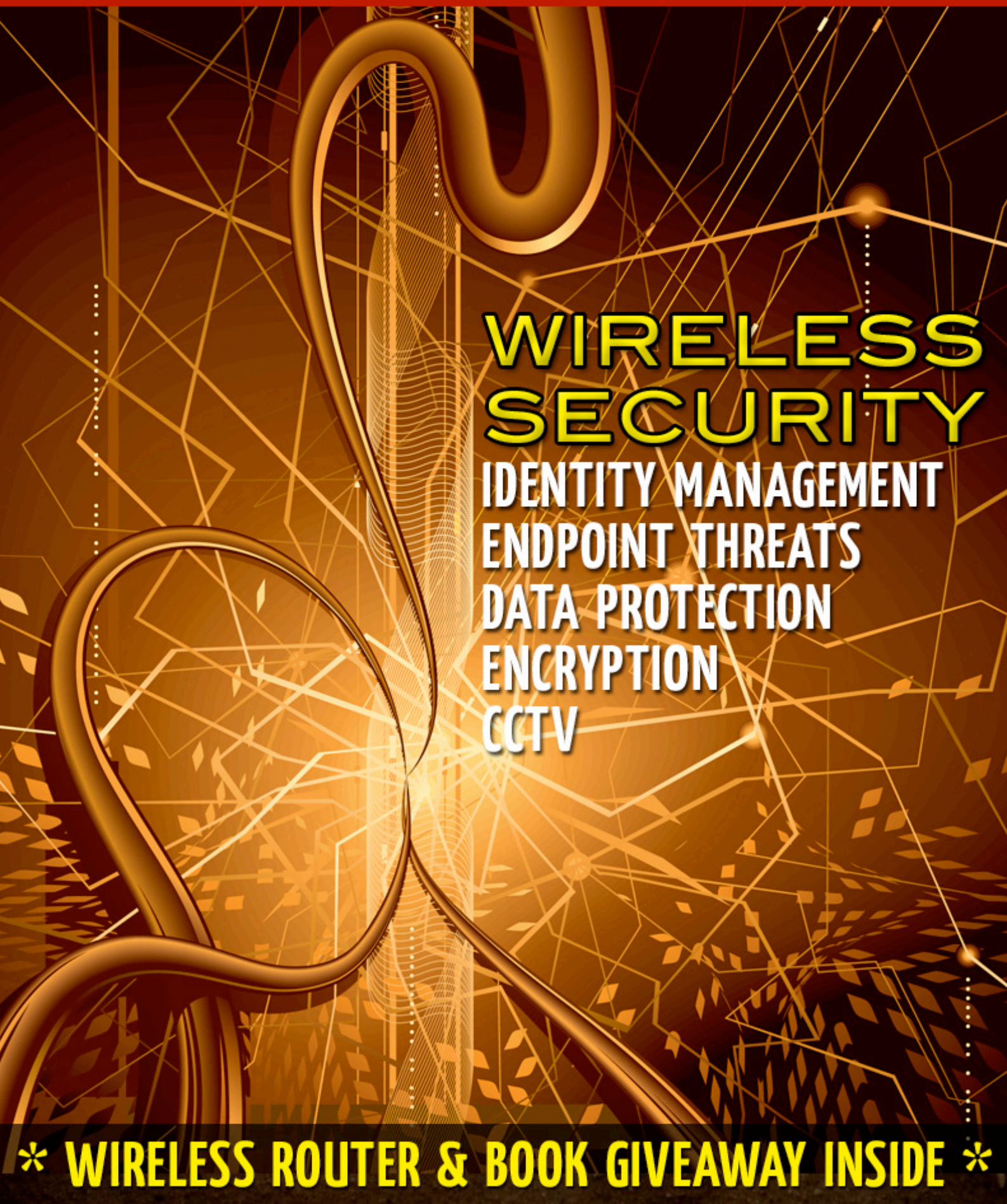
[IN]SECURE

OPEN. INFORMATIVE. TO THE POINT. Issue 14 - November 2007



WIRELESS SECURITY

IDENTITY MANAGEMENT
ENDPOINT THREATS
DATA PROTECTION
ENCRYPTION
CCTV

* WIRELESS ROUTER & BOOK GIVEAWAY INSIDE *

SECURITY AS A SERVICE

NOW AVAILABLE AT A BROWSER NEAR YOU

Software-as-a-Service (SaaS) has been described as the most disruptive delivery model to ever face the enterprise software market for one simple reason: ***it works***

Qualys is the first company to deliver an on demand solution for security risk and compliance management. QualysGuard® is the widest deployed security on demand platform in the world, performing over 150 million IP audits per year — with no software to install and maintain.

For a free trial, go to a browser near you.

www.qualys.com/SaaSTrial

TABLE OF CONTENTS

Welcome to another issue of (IN)SECURE. This time around we bring you articles covering topics such as the future of encryption, data security, attacks on consumer embedded devices, PCI DSS, and much more. Our feature topic for this issue is wireless security and we managed to gather six experts from world-renowned companies that provide an overview of the current wireless security threats and offer predictions for the future. Given the focus of this issue, our **giveaway** focuses on wireless security and I'm sure you're going to like it so check out page 104!

I'd like to thank all the potential authors and organizations that got in touch with us. We're always pleased to hear that (IN)SECURE is distributed in several Intranets worldwide and that the readership is growing strong. Don't forget to visit www.insecuremag.com and subscribe for free. We're always interested in new authors and topics so if you'd like to get in front of a large audience drop me an e-mail.

Mirko Zorz
Chief Editor

Visit the magazine website at www.insecuremag.com

(IN)SECURE Magazine contacts

Feedback and contributions: Mirko Zorz, Chief Editor - editor@insecuremag.com

Marketing: Berislav Kucan, Director of Marketing - marketing@insecuremag.com

Distribution

DefensePro with an adaptive behavioral server-based IPS feature set

The latest version of DefensePro's flagship Intrusion Prevention System provides adaptive behavioral server-based IPS feature set, protecting against misuse of application authorization and preventing break-in attempts to enterprise critical application servers, with no need for human intervention. This allows the network to automatically respond to attacks targeted at revenue-generating applications. The new version complements Radware's DefensePro existing signature and behavioral network- based protections and reinforces the company's vision to provide business-smart networking solutions. (www.radware.com)

New security features in Google Apps Premier Edition

The new security, compliance, policy management, and message recovery services added to Google Apps Premier Edition give customers the ability to:

• Set configurable spam and virus filtering that are customized for the nature of the business, complementing the spam and virus filters already included in Google Apps.

• Centrally manage all outbound content policy, including adding footers to every message based on business policy rules, blocking messages with specific keywords or attachments, and preventing emails with sensitive company information from being sent.

• Create, manage, and report on policies that apply to user groups or individual users.

• Give administrators the option of visibility into all email within their organization for the purposes of compliance. (www.google.com)

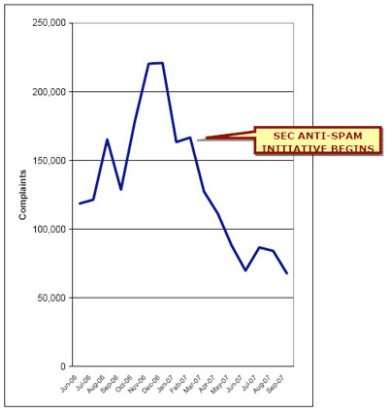
New innovative ID verification system using grids

GrIDsure Limited has announced its revolutionary new approach to authentication - designed to tackle many of the problems currently being suffered by consumers buying both online and on the high street. Users create a simple pattern by choosing a set number of squares on a grid, in a shape of their choice - such as an 'L' or a 'tick'. Because the grid is then filled with random numbers at authentication time, new 'PIN' or pass codes are created each time. Best of all, GrIDsure can work without the need for extra hardware such as tokens, generating one-time codes that are more secure and resilient to spyware threats. (www.gridsure.com)

Secure printing of sensitive documents with new HP appliance

HP introduced an automated, comprehensive solution that enables the secure printing of sensitive documents in corporate and government networks. HP Secure Print Advantage minimizes business risk by addressing printer security vulnerabilities across the disparate systems, servers and clients typical to most enterprise environments. HP Secure Print Advantage enables IT to automatically set and enforce policies across systems, applications and the print network. To safeguard against malicious attacks, the solution integrates the highest level of federal and international security assurances available in the market today – both FIPS 140-2 Level 4 and Common Criteria EAL 4+ security technology – into print environments. (www.hp.com)

SEC's Anti-Spam Initiative causes reduction in financial spam



The Securities and Exchange Commission continued its assault on stock market e-mail spam by suspending trading in the securities of three companies that haven't provided adequate and accurate information about themselves to the investing public. The trading suspensions are part of the Commission's Anti-Spam Initiative announced earlier this year that cuts the profit potential for stock-touting spam and is credited for a significant worldwide reduction of financial spam. A recent private-sector Internet security report stated that a 30 percent decrease in stock market spam "was triggered by actions taken by the U.S. Securities and Exchange Commission, which limited the profitability of this type of spam." (www.sec.gov)

SDK for building fingerprint biometric applications for Linux systems

DigitalPersona announced the DigitalPersona One Touch for Linux SDK, their new software development kit that enables developers to create fingerprint enabled applications for the Linux operating system. The new SDK is the first Linux product for DigitalPersona, which is expanding into the quickly evolving open-source space to enable fingerprint support for multiple Linux distributions. (www.digitalpersona.com)

Secure USB flash drive with a self-destruct sequence

IronKey recently launched Enterprise Special Edition of their secure flash drive designed for use on sensitive government, military and enterprise networks. The IronKey: Enterprise Special Edition has been designed to be the world's most secure USB flash drive, using onboard hardware encryption to protect the gigabytes of files that can be stored on the device. No software or drivers need to be installed on your computer to use an IronKey. A password is used to unlock your IronKey, and this is verified in hardware. If an IronKey is lost or stolen, attempts to unlock or tamper with the IronKey will trigger a self-destruct sequence, ensuring data is kept confidential. (www.ironkey.com)

New advanced quality and security WLAN testing solution

Codenomicon introduced DEFENSICS for WLAN, an advanced quality and security testing solution that gives developers of wireless consumer devices, public broadband infrastructure vendors and network service providers the means to identify previously unknown product flaws and security vulnerabilities early in the production process - before any business or consumer information is compromised or service maliciously interrupted. It can be used to extend quality assurance and security-readiness processes of vendors, service providers, enterprises and municipalities deploying Wi-Fi and WiMax networks. (www.codenomicon.com)

Secure file transfer solution for IBM mainframes

SSH Communications Security announced the general availability of SSH Tectia Server 5.5 for IBM z/OS which allows enterprises to secure file transfers and other data in transit with little or no changes to scripts, applications or infrastructure. SSH Tectia Server for IBM z/OS is an advanced, cost-effective file transfer solution for the IBM environment supporting key mainframe features such as: direct MVS file system access, hardware encryption acceleration, SMF logging, automatic character set conversion, strong authentication through RACF, ACF and TopSecret, X.509 certificate support as well as fast data streaming technology. (www.ssh.com)

IBM DB2 gets database encryption capabilities

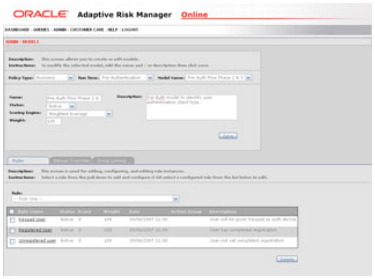
Vormetric partnered with IBM to deliver database encryption capabilities for DB2 on Windows, Linux and Unix. IBM will offer Vormetric's highly acclaimed data security solution as part of its data server portfolio, addressing customer demand for increased protection of sensitive data. This new capability is delivered in IBM Database Encryption Expert, initially available for the new DB2 9.5 "Viper 2" data server. (www.vormetric.com)

Strong user authentication via leading enterprise smartphones

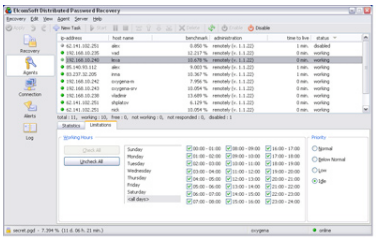
RSA announced the availability of the RSA SecurID Software Token 2.2 for Symbian OS and UIQ. Symbian develops and licenses Symbian OS, the market leading operating system for smartphones. Symbian OS is licensed by leading mobile phone manufacturers; to date, more than 145 million Symbian smartphones have shipped worldwide to more than 250 major network operators. Businesspeople who use smartphones based on UIQ and Symbian OS can now leverage their devices to access protected corporate information securely, eliminating the need to carry a separate, stand-alone authenticator. (www.rsa.com)

New Oracle security product: Oracle Adaptive Access Manager 10g

Oracle announced general availability of Oracle Adaptive Access Manager 10g, a comprehensive solution designed to prevent online identity theft and fraud, Oracle Adaptive Access Manager 10g features a number of enhancements including: turnkey Knowledge-Based Authentication and system monitoring dashboard features, increased support for financial and retail compliance requirements, a hot-pluggable architecture and tight integration with Oracle Access Manager. (www.oracle.com)



Forensics edition of password recovery bundle



Elcomsoft released Password Recovery Bundle - Forensics Edition. Using innovative technology, ElcomSoft's package of password recovery products lets authorities unlock more than one hundred file formats and programs. The bundle includes programs and technologies that are not available from other software companies: Elcomsoft System Recovery, a boot-disk application that makes it easy to access your computer's Windows password settings, Proactive Password Auditor, a password audit and security test tool that makes it easy for Windows systems administrators to identify and close security holes in their networks and Elcomsoft Distributed Password Recovery, an innovative way to harness the power of multiple computers to recover lost passwords. (www.elcomsoft.com)

Good Mobile Messaging Secure Multipurpose Internet Mail Extensions

Motorola recently introduced Good Mobile Messaging Secure Multipurpose Internet Mail Extensions (Good S/MIME). Designed specifically to meet federal government security policy requirements, it supports the Motorola Q family of smartphones and gives the Department of Defense and associated government agencies a mobile messaging solution that is more personalized and easier to manage and administrate than other alternatives. Good S/MIME works with the Motorola Q family of smartphones, Bluetooth CAC-readers and standard DoD-issued common access cards to seamlessly secure CAC communication, sign and encrypt emails and attachments, and deliver a superior user experience. (www.motorola.com)

When attacking a network you must look at the "network" as the holistic system that allows the organization to share, create, and maintain information.

When you are deciding on which targets to attack on the network, I like to remind people of my favorite movie quote which comes from the 1992 film called "Sneakers". In it the bad guy named "Cosmo", played by Ben Kingsley, is explaining his strategy and motives for world domination (a popular goal by bad guys in the movies). In the final breath taking scenes Cosmo proclaims, "…it's not about whose got the most bullets. It's about who controls the information. What we see and hear, how we work, what we think... it's all about the information!" There are so many parallels between this quote and information security that it could warrant an article all on its own. However, lets take just the line that states "its all about the information", which couldn't be more true today.

As an attacker, "whitehat" or "blackhat", what is your goal? Why, to get the information of course! When you evaluate risk for your organization the most important variable in any risk calculation is the importance of the data, and much of our careers as information security professionals are spent trying to protect that data.

When looking at the network holistically, would you choose a target that contains some of the organization's data or a target that all of the data flows through transiently? Let's think about that for a moment. If you compromise a server or workstation that contains some Word documents, is that most likely the latest version of that data or the entire company's document collection? Or, is it better to gain control of a printer or network switch that is sending or printing the latest version of that document? By attacking, and subsequently "owning", the individual devices that make up the network, we can own the information. This is better from an attacker perspective than gaining access to a single server or desktop for several reasons. First, there is typically not a monitor, mouse, keyboard, or end-user associated with a network device. Console connections are the closet thing, however typically they are used only when performing maintenance or to recover a device from a failure.

The absence of a user interface makes it much easier to hide our presence. Embedded devices also have a stealthy characteristic associated with them because administrators or end users do not pay attention to them unless they are broken. I worked for several years in the networking department of a fairly large organization who lived by the words “if it ain’t broke, don’t fix it”. I have also spoken with countless end users who will say such things as, “Don’t touch that, it works just fine!”

The remainder of this article will focus on exploring vulnerabilities, and associated risk, with wireless access points, routers, printers, and some other common devices on the network. The methods of vulnerability discovery and defense against attacks can be applied to many different types of embedded devices in different environments.

Goals of exploitation

Replacing the firmware

Being able to modify the device’s firmware, or even replacing it, is one of the most powerful attacks against embedded devices. Unlike workstations and servers, it is quite easy and feasible to replace the entire operating system on an embedded device. Attackers can even go to the extent of creating a firmware that looks exactly like the firmware running on the device, for example imitating the look and feel of the Linksys web management interface. The new operating system could not only duplicate the functionality of the original, but also add “special features”. In the context of a home cable modem/router/firewall, the new functionality could intercept usernames, passwords, credit card numbers, or other personal information.

These attacks are not out of the realm of possibility; many different firmware distributions exist for several common home routers [toh.openwrt.org]. Even if an attacker does not have replacement firmware to work with already, it is possible to take any device using firmware and write custom code for it. For example, Stephen Lewis presented at the 21st Chaos Communication Congress and released proof-of-concept code that could insert custom code into an embedded device running the Motorola 68EC020 processor that could send and receive packets on the network through the management interface [tinyurl.com/ytbrod].

Manipulate settings

If an attacker cannot easily replace firmware on devices, they will most likely resort to changing the settings in the existing firmware. This idea has been explored on devices such as printers, where everything from the display to the number of pages printed can be modified [tinyurl.com/2fudev]. However, network settings are a target too. If an attacker can modify the DNS settings on a wireless home gateway, they can redirect the user to phishing sites with ease. Also, a printer’s routing table can be manipulated such that all network traffic goes through a specific workstation, allowing an attacker to view all of the print jobs going through it.

Other settings manipulations include enabling remote administration, or disabling wireless security. The idea of doing evil things with home routers by changing the settings was explored in a paper from Symantec titled “Drive-By Pharming”, which details using Javascript and Java tricks on the client to take advantage of a default password and manipulate a router’s configuration [tinyurl.com/2vpb8r].

Denial Of Service

Denial of service conditions on embedded devices can often happen by accident. However, some devices may become intentionally targeted for denial of service. Examples include web cameras used to provide security monitoring, or SCADA devices that are used to monitor and run energy sources that may be under attack from cyber terrorists. Unfortunately for the defenders, triggering a denial of service on an embedded device is far to easy, and sometimes is not easy to recover from. A good example is the HP printer FTP denial of service exploit [5], which when sent to a device corrupts the firmware. Once the firmware is corrupted, you will need to perform some form of recovery, which may entail a JTAG device that needs to be interfaced with the hardware directly. In the case of the HP printer, it has to be sent back to the factory for recovery.

Example attacks against embedded devices

As a society we hope that if we learn from history, we will not be doomed to repeat it. Lets start by taking a look at a vulnerability in an embedded device that was responsible for sparking the router hacking revolution (with a little help from the GPL [tinyurl.com/c56wz]), the infamous “Ping Hack”. In the firmware that shipped with Linksys WRT54G series routers there was a bug in the Ping functionality built into the web interface, which is now a common target for attackers on all embedded platforms. By browsing to the web management interface a user was able to enter an IP address, click the “Ping” button, and test connectivity. Fortunately for the hacking community, the developers did not do a very good job implementing input validation checks, making it possible to run arbitrary commands on the device. For example, consider the following commands that could be entered into the “ping” dialog box:

```
;cp${IFS}*/*/nvram${IFS}/tmp/n
;*/n${IFS}set${IFS}boot_wait=on
;*/n${IFS}commit
```

The above commands will enable the boot_wait parameter on a WRT54G, allowing you to TFTP new firmware to the device when it boots up. This helps us accomplish our goal of installing our own firmware on the device and/or installing our own end-user software. Installing a tool such as dnsiff on a router gives the attacker a very powerful tool enabling credentials to be sniffed via many different protocols. This program does not need to exist on the end-users computer, but only on the router where it can remain undetected. It's amazing how we really do not learn from history as a very similar vulnerability exists in the La Fonera FON routers, which contain a remote command execution vulnerability that allows us to install custom firmware. For example, to manipulate the firewall on a La Fonera router, consider the following POST request:

```
<form method="post" action="http://192.168.10.1/cgi-bin/webif/connection.sh"
enctype="multipart/form-data">
<input name="username" value="$(/usr/sbin/iptables -I INPUT 1 -p tcp --dport 22 -j
ACCEPT)" size="68" >
```

Whoops, looks like the connection.sh script forgot to do input validation on the username field. This, of course, opened up the La Fonera to firmware hacking and allows us to install OpenWrt, an open-source firmware for embedded devices. Installing software within OpenWrt is easy, with one command we can have the dsniff suite of tools available to us:

```
# ipkg install dsniff
```

Linksys and La Fonera are not alone. There are many embedded devices that are vulnerable to a wide range of attacks. Take the 2wire 2071 Wireless/Ethernet/ADSL router, which is thought to be one of the most popular home DSL router in Mexico [tinyurl.com/2ahy38]. It contains a default configuration that has no password. This allows for a really easy CSRF (Cross Site Request Forgery Attack) to occur. Consider the following attack URL:

```
http://192.168.1.254/xslt?PAGE=J38_SET&THISPAGE=J38&NEXTPAGE=J38_SET&
NAME=www.bank.com&ADDR=2.2.2.2
```

The above command will add a static DNS entry for www.bank.com and resolve it to 2.2.2.2. All the end user would need to do is click on this URL, and a new DNS server would be added. This easily allows an attacker to perform phishing attacks, as now they can control where your web traffic goes. Mexico is not alone; many ISPs are now shipping DSL/Router/Wireless Access point combined devices with default passwords and vulnerabilities. A good example involves a router in widespread use in the United Kingdom from British Telecom (BT).

The “BT Home router” is one of the most popular DSL/Cable routers in Britain, claiming 2+ million installations [tinyurl.com/2fpbtf]. It too suffers from CSRF vulnerabilities that allow an attacker to manipulate the configuration without the need for a password. While the group responsible for finding the vulnerabilities has not released all of the details, they can manipulate the router due to an authentication bypass vulnerability. Who needs to rely on the default password when we can just bypass authentication altogether!

There are also US based providers shipping insecure default configurations as well (i.e. a default password of “password”), and my fear is that they may become targets of attack. If an attacker knows that everyone from XYZ ISP has a router with a default password, they can use data mining techniques to collect those users email addresses (i.e. user@xyzisp.com) and target them with attacks that will manipulate the configurations on their routers in some way. Authentication bypass vulnerabilities present in home routers are not new, nor are they limited to the ones distributed by the ISP. A researcher by the name of Ginsu Rabbit discovers that WRT54G version 5 routers running firmware version 1.00.9 are vulnerable as well [tinyurl.com/2ejhc9]. The danger of this vulnerability is that to fix it a user must update firmware, which so many users simply do not do.

Unfortunately many people leave the default username and password set to the default even on devices that they purchase themselves. For example on most Linksys WRT54G routers it’s set to a username of admin and a password of admin. All it really takes is to entice a client to go to the following URL:

```
http://admin:admin@192.168.1.1/apply.cgi?submit_button=index&change_action=&submit_type=&action=Apply&wan_dns0_0=192&wan_dns0_1=168&wan_dns0_2=1&wan_dns0_3=13&wan_dns1_0=0&wan_dns1_1=0&wan_dns1_2=0&wan_dns1_3=0&wan_dns2_0=0&wan_dns2_1=0&wan_dns2_2=0&wan_dns2_3=0&wan_wins=4&wan_wins_0=0&wan_wins_1=0&wan_wins_2=0&wan_wins_3=0&time_zone=-08+1+1&_daylight_time=1
```

This works on a Linksys WRT54G with the default username and password and allows us to change the routers DNS servers as we did before.

Vulnerability discovery methods

Nmap

Nmap, the world famous portscanner, has proven a useful tool to finding vulnerabilities in embedded devices. A little known fact about Nmap is that due to printers printing endless pages, port 9100 is ignored when doing certain scans. While this is not a vulnerability per se, it will deplete the resources of a printer. I have personally crashed many printers doing operating system fingerprinting with Nmap.

Most recently while doing some work for a client on a penetration test I was testing the wireless network. This particular wireless network was a managed system, meaning that the access points were “dump” and only provided the radio functionality, while all of the intelligence (encryption, captive portal, etc..) was provided by a central controller. During the test I associated to the open SSID and tried to go to a web site. Working as advertised, the captive portal kicked in and redirected my request to the login page sitting on the wireless controller’s web server. This means that any wireless client has access to at least one open port on the controller itself. I started my testing by launching an Nmap scan against the controller to gain some insight into its setup:

```
Nmap -0 -P0 -T4 <ip address of captive portal>
```

The above command produced a message from Nmap that said it was scanning port 80, but during the scan port 80 appeared to be closed (i.e. it responded with reset packets). It was then apparent that the captive port web server crashed, and was no longer serving web requests. This caused a serious problem for the wireless network. If the web server was down, the captive portal was still redirecting users to the captive portal page, which

displays a page not found error. This prevents even legitimate users from entering their credentials and using the wireless network. Even more interesting was that to solve this problem the wireless controller had to be rebooted, which means all clients lose wireless connectivity because the access points are “thin” and rely on the controller. This is now a very useful took for attackers, as causing all users to disassociated and re-associated to the wireless network is a powerful action. The attacker can do this, and then capture WPA-PSK traffic for later brute forcing, pretend to be a wireless access point (aka. Evil twin), or spoof the SSL certificate of the captive portal and capture usernames and passwords.

Metasploit

Metasploit is a fantastic tool for finding vulnerabilities in embedded devices, and as an added bonus is one of the best frameworks available for exploit development when you are ready to take it to the next step [tinyurl.com/2zqbzu]. Metasploit 3.0 has a couple of modules that you can use to fuzz wireless (802.11) stacks. I like to use the auxilery/dos/wireless/fuzz_proberesp module to find weaknesses in wireless access points. It is convenient to use the msfcli program, which lets you execute metasploit commands from the command line, to fuzz wireless drivers. For example:

```
./msfcli auxiliary/dos/wireless/fuzz_proberesp DRIVER=madwifing
ADDR_DST=AA:BB:CC:DD:EE:FF PING_HOST=192.168.1.1 CHANNEL=6 E
```

The above command will send bogus probe response packets to the device at the listed address. Probe response packets are typically sent by the wireless client to the access point in response to beacon frames and indicate that the client would like to associate to the access point. The ping host is the IP address to ping while doing testing to see if the host being tested is till alive. It is important that you associate to the access point with a different wireless adapter on the same subnet as the access point you are testing.

For example, if you crash the wireless driver, but the access point is till running, you want the ping test to fail. If you’ve plugged into the Ethernet port on the access point, your ping packets would only fail if you caused a system wide crash. If you miss enough ping packets Metasploit will spit something out like:

```
"P\000\000\000\000\032pu\265\375+\r\311xTM+\r\311xTM\000\366\215\364\314\325z%\3
14N\311g\e\345\000\336TkVGjC1mTEQRmNrulZNV8lqpoEa5WOxOqTZewkL2e6WBr0aQQgQFKLVkjw
8Wg5gRNTV3qEYXBHqKBWyHJc7s7puT6nFaI5sVRFOglbe98864GMLb0RSPEQ7nILpqM9kW6V8r8J47MR
X03PDf69v9LgqPZPBdQd4kdA93nWClwTHOieDK4sWvq2uXwJhxaIdchxo12s8SOCoKZGc1cQnVW94SAI
xC72\001\b\202\204\213\226\f\0300H\003\001\006\t#Mj\272\\\254\225\000\323\310\"\
272X3J\364m\214\005\344\251tH\302w\362\330\351j\232R%*\376\317\221h\217\361\360\
200i\340nw\326\243\216}\315:\225\226\n\025w\323\201\251\343\320\310\003v\325\017
\030\235\327\300\354\200\267\277!\207\233\326Z\325\344453Y\333\t9\266\260\235Z\2
11\260\235t\253\212\377\246\351\272\226\020\324e\254\233\nm\247-\254\251]{\375\2
05\2020\022\344f_07\275\210\326\246\023\372W\205\276\034w!\301:C\261T\316\206\25
3\365k<\233\222]\261\201K\335\266\255\377w\v\234\233\267\026\232u\243nV\330XM\34
6GM\016\eGU\a\230/\325z\331}s%\t:4\207\001\253y\203g\037\024\025\020L;\225Fw\t&J
0\036\230\2512H\357'z\30 1\313s\274\000"
```

The above is the raw packet information, which can be interpreted by the ruby functions within Metasploit.

Protecting your embedded devices

Keep your firmware up-to-date

Just as it is important to keep your operating system and associated software up-to-date, its equally as important to keep your firmware up-to-date. It may seem like a daunting task to update the firmware on all of the printers in your environment, however given the current threats and research trends it’s a task that must be completed on a regular basis. If you are a home user, updating firmware on your router will protect you from many of the current threats. With all embedded devices, even if it means scheduling regular maintenance time, it is critical to keep them up-to-date.

Default settings cannot be trusted

I'd say the number one downfall of embedded devices with respects to security are default settings. Wireless routers come with default SSIDs and username password combinations that allow for easy attacks. The OpenWrt project has addressed this issue with its Kamikaze release, which disables the wireless network by default and prompts the user to enter a password rather than come with one by default. You have to harden your embedded devices just as you would your workstations and servers. This means disabling services that are not in use, enabling firewalls and filtering rules, and most importantly changing default passwords.

Monitor embedded devices just like every other host

Do you have intrusion detection on your management networks? Would you detect an attack aimed at your printer, or even originating from your printer? Monitoring is a critical piece of your overall security strategy, and it must include all of your embedded devices. This could manifest itself as an intrusion detection sensor, and/or be a centralized logging facility that includes routers, wireless access points, printers, and web cameras. Having remote logs from these devices will help you to detect nefarious activity that may occur on the various platforms that do not have the capability to log locally.

Separate and protect your embedded devices

Put printers (and other embedded devices of similar security requirements) on their own subnet and firewall them from the rest of the network. Then, tailor the rules just like you would for your servers and only allow the ports that are required.

Conclusion

As the information security field evolves, changes, and improves, so do the attackers and their techniques. Embedded devices are ripe for the pickings, and attackers will begin to target and compromise embedded devices to achieve their goals.

Embedded devices carry our sensitive information and allow for sophisticated attacks that can be used to control various aspects of our network and compromise our security. Changing the way we treat our embedded devices is the key to success. We need to recognize that embedded devices need to be locked down and secured just as any other device in our organization.

Paul Asadoorian is the weekly host of PaulDotCom Security Weekly (www.pauldotcom.com), a security podcast focused on the latest security news and hacking. He is also the author of the new SANS course titled "Embedded Device Hacking".

Paul would like to thank Raul Siles for his input and direction in the writing of this article.

Qualys is a key player in the on-demand vulnerability management and policy compliance market. The company's flagship service QualysGuard is used to conduct automated security audits without any need of software or hardware installation by its users. The service is provided through a very fast and stable online application which does over 150 million IP audits per year.

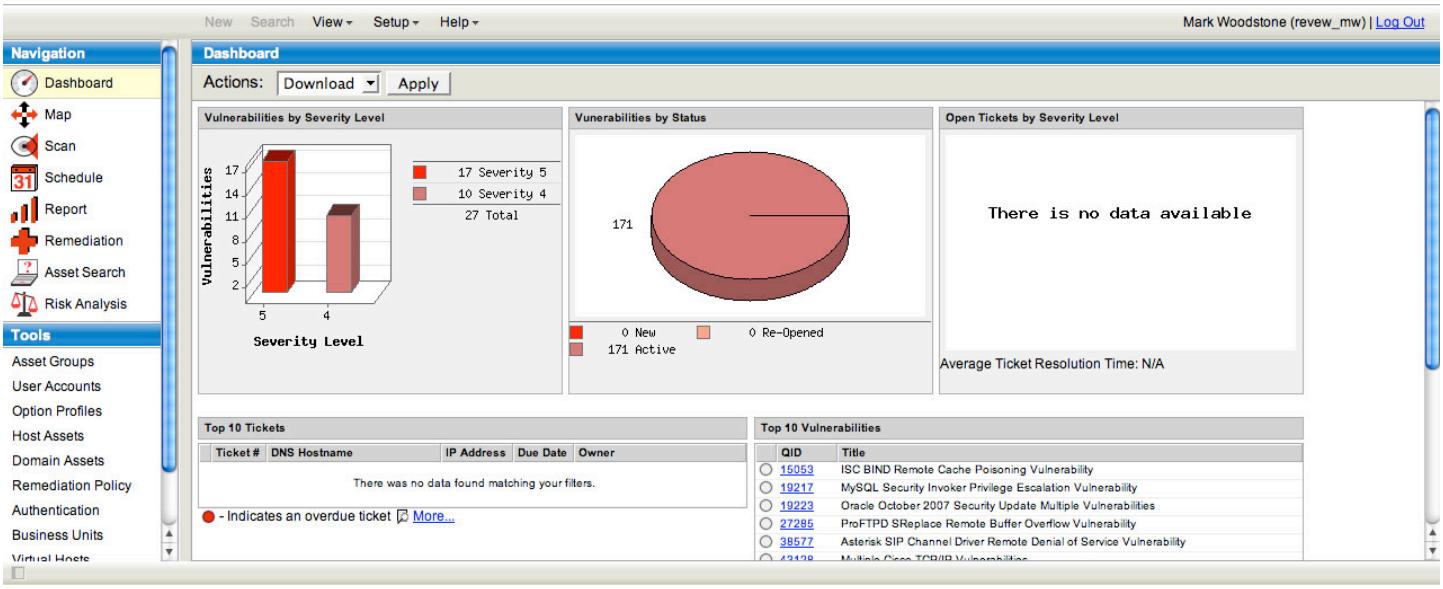
The user interface is very adaptive and you will need just a couple of minutes to make yourself comfortable in it. The application is divided into a couple of content frames, making it easy to work with. The left menu navigation opens all the important QualysGuard modules, while the top drop down menus offer configuration and setup options for the currently active module.

Besides the technical options, you will also find a large collection of support documents, containing detailed information on every possible aspect of the application usage. If this is not enough, you also get access to both e-mail and phone support that will give you all the answers you need.

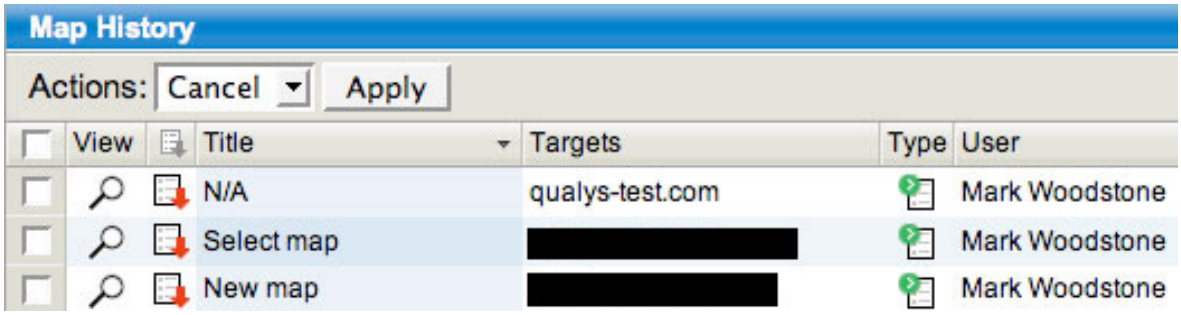
This article will cover main aspects of QualysGuard usage which I divided into five sections - mapping, scanning, reporting, remediation and risk analysis.

Mapping

The first step of your network security scan starts with a mapping module. While you can skip this part and target the specific IP address or a network block, it is recommended to use it because you will get a glimpse of all the computers that can be mapped from the outside. Before you create a new map, you should add your target domains. Each domain may include one or more netblocks (IPs and IP ranges). Before running the map, my suggestion would be to fill QualysGuard with all the possible data on your network by creating asset groups. An asset group can include IPs, domains/netblocks, and scanner appliances that exist in your account. Each of the groups can contain a specific set of computers and network devices and can be very useful in the scanning process where you want to target particular assets.

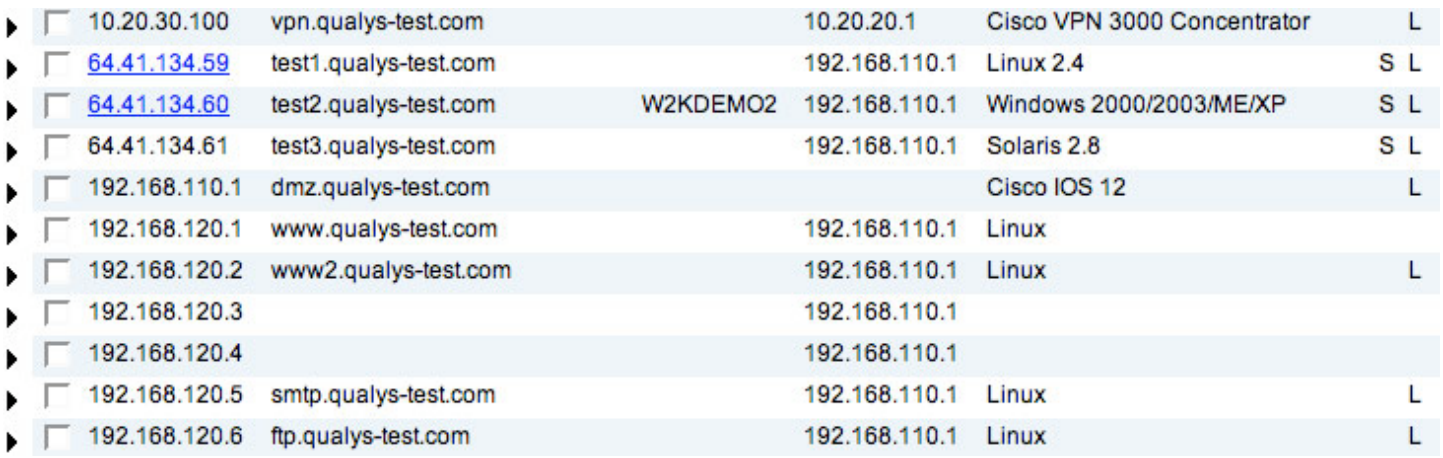


QualysGuard user interface



Repository of mapping results

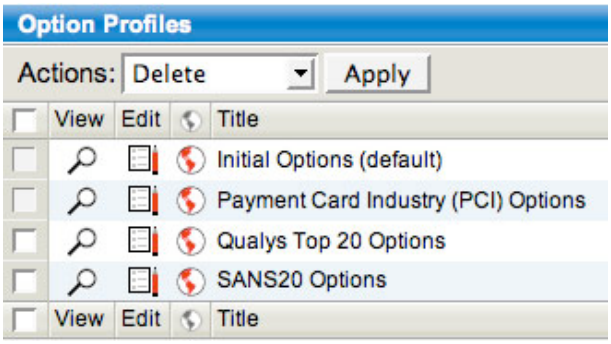
For launching the map you will need to manually select the domain or asset group you want to work with and in just a couple of seconds the detailed map will be available within the interface. You will have the possibility of downloading the results in a number of different formats, as well as checking out the detailed report on the discovered hosts. The data is very well presented, so with a click of a mouse you will be able to add hosts to new asset groups, as well as start or schedule security scans on them.



Example map of the Qualys test network

Scanning

Starting the scan is also a no frills process. If you worked your way through the mapping stages you already have all of your hosts sitting comfortably in a line for scanning. By default the system has some default scanning profiles including the default one, Payment Card Industry (PCI), Qualys Top 20 and SANS20 scan. The latter three are self descriptive, as they cover a specific set of threats and the first one is a general scan that should very interesting to a large number of users. The user can chose one of those scans, but can also customize them through an "Option profiles" selection in the tools menu. There you can chose the advanced mode that will offer quite an extensive list of setting you can change. These options are related to ports, performance, load balancers, brute forcing, vulnerability detection, as well as authentication. By setting up authentication credentials, the scanner can log into hosts at scan time to extend detection capabilities.



Option profiles for the vulnerability scan

After the scan is started, the process goes into the background and you can watch its status through the Scan interface. Depending on your network or scan complexity, this can take some time (30-45 minutes per host). After it is successfully completed, you will immediately be able to check the results. In the same type of user interface as with mapping, you can both download the report or view a full status that opens in a pop-up window.

Vulnerabilities (27)

4	SSH Protocol Version 1 Supported	port 22/tcp
3	Discovery of Unix Account Names Vulnerability	port 80/tcp
3	Webalizer Web Usage Statistics Accessible	port 80/tcp
3	SSL Server Has SSLv2 Enabled Vulnerability	port 443/tcp over SSL
3	SSL Server Supports Weak Encryption Vulnerability	port 443/tcp over SSL
3	SSL Server May Be Forced to Use Weak Encryption Vulnerability	port 443/tcp over SSL
3	Discovery of Unix Account Names Vulnerability	port 443/tcp
3	Webalizer Web Usage Statistics Accessible	port 443/tcp
3	OpenSSH Key-Based Source IP Access Control Bypass Vulnerability	port 22/tcp
2	Web Server HTTP Trace/Track Method Support Cross-Site Tracing Vulnerability	port 80/tcp
2	SSL Certificate - Expired	port 443/tcp over SSL
2	SSL Certificate - Self-Signed Certificate	port 443/tcp over SSL
2	SSL Certificate - Subject Common Name Does Not Match Server FQDN	port 443/tcp over SSL
2	SSL Certificate - Improper Usage Vulnerability	port 443/tcp over SSL
2	SSL Certificate - Signature Verification Failed Vulnerability	port 443/tcp over SSL
2	Netscape/OpenSSL Cipher Forcing Bug	port 443/tcp over SSL
2	OpenSSL Insecure Protocol Negotiation Weakness	port 443/tcp over SSL

Vulnerabilities found on one of the hosts

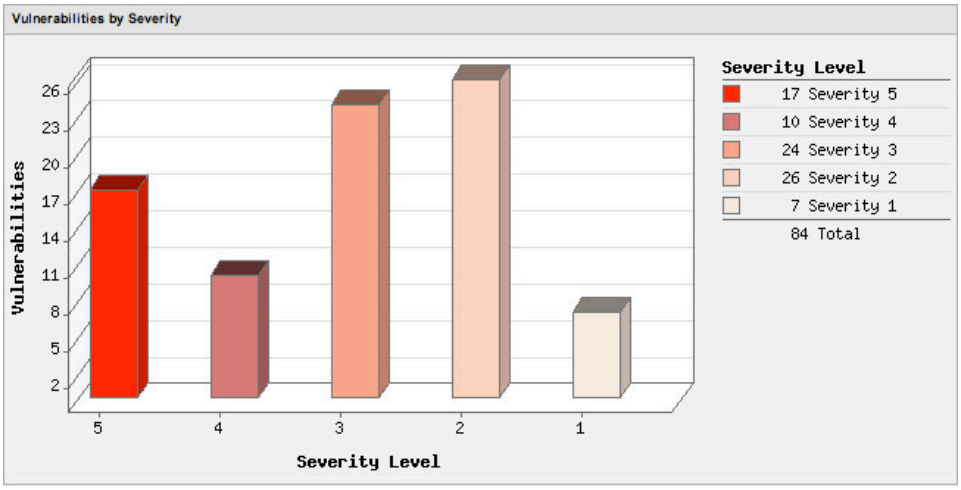
Reporting

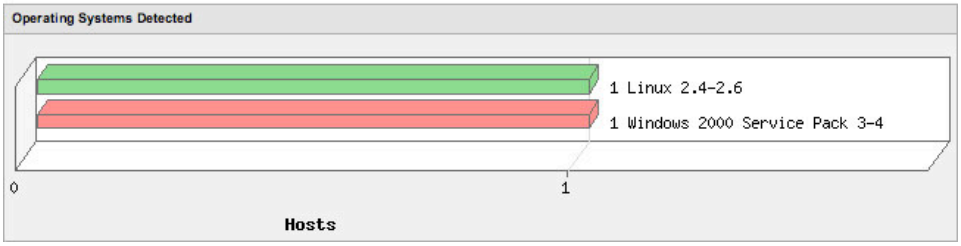
The default report template provides a rather comprehensive amount of information on the found vulnerabilities. You will get a standard set of host information, followed by a vulnerability summary charts and images, as well as a quite detailed list of the vulnerabilities sorted by its importance. Every detected vulnerability hosts detailed facts about the issue, containing the threat description, impact, possible workaround solution and further links helping the user to remediate the problem.

While the default report seems to be sufficient, there are of course a number of people in the organization you will need to present to. Therefore, the "Report" section of the QualysGuard applications hosts quite a lot of different templates focused on particular subjects. You will find ways to satisfy your executives (Executive Remediation Report, Executive Report,Payment Card Industry Executive Report), as well as your technical peers (Payment Card Industry Technical Report, Technical Report, High Severity Report). Besides these vulnerability and compliance reports, there are also templates for the popular SANS and Qualys top 20 lists, as well as ticket reports that are related to the remediation module discussed later in the article.

For more advanced QualyGuard usage, there is a simple way of creating your own customized report templates.

Report templates in QualysGuard





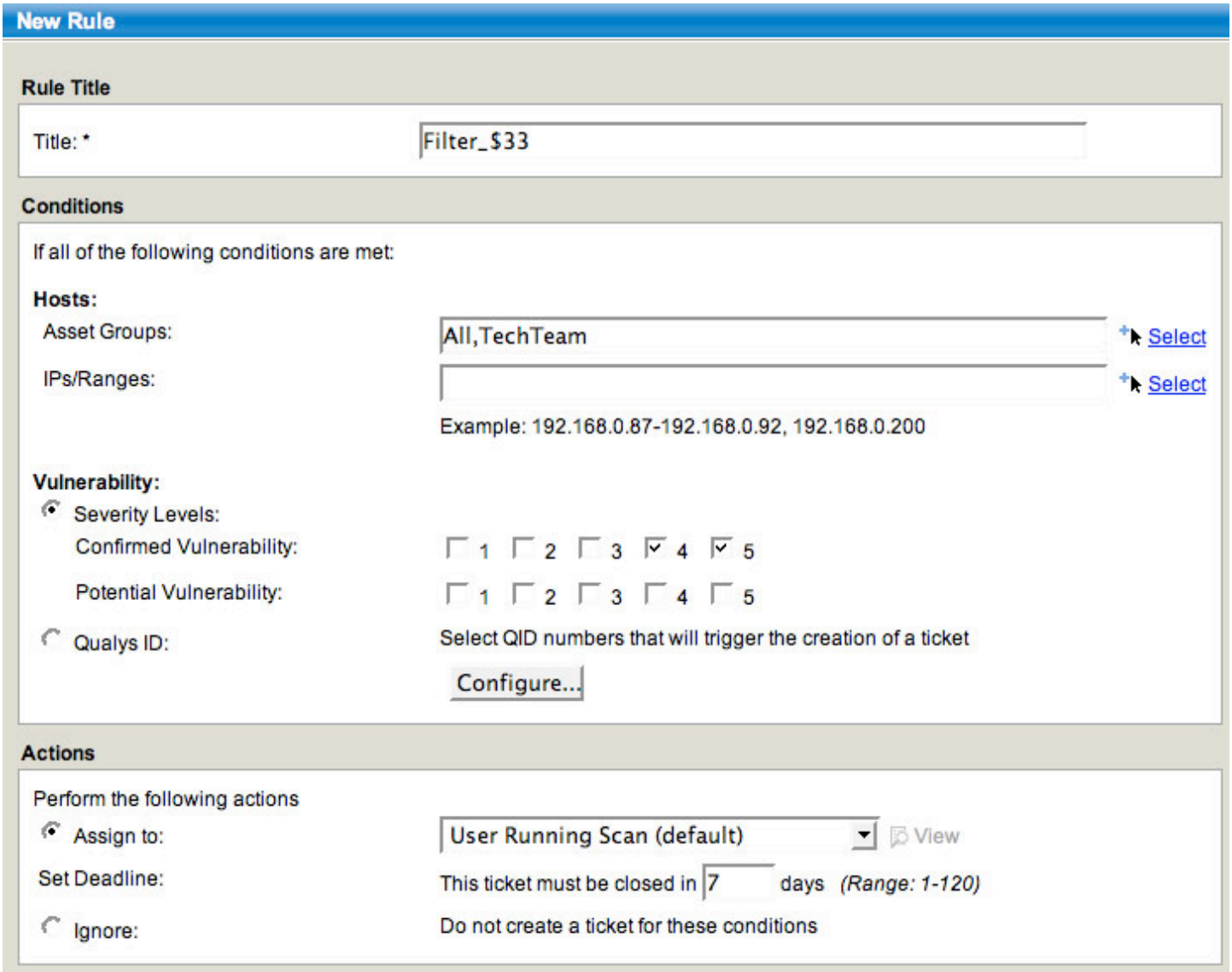
Snippet from a vulnerability report

Choosing the "New map template" from the menu opens a pop-up window with advanced settings containing host types, discovery methods, operating systems and much more needed to create a totally new report template focused on the needs of your organization.

Remediation

Within the application you will find a dedicated ticketing service for prioritizing and fixing vulnerabilities by using recommended solutions (patches or workaround scenarios provided in the scanning reports).

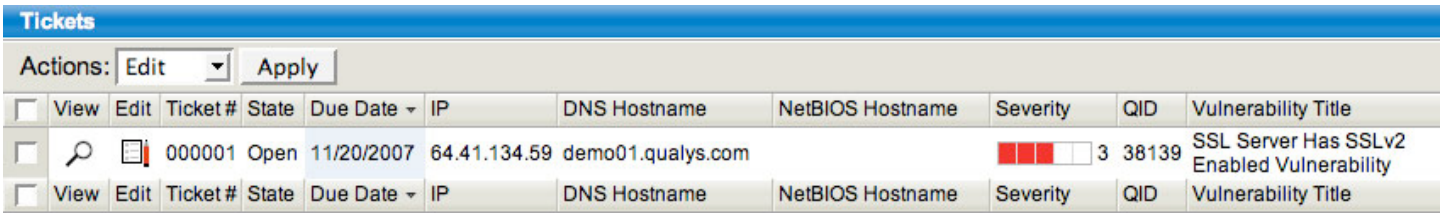
Each created ticket is connected to a specific vulnerability that is accompanied with a unique Qualys ID (QID). If you are using the ticketing, it is recommended to create a customized policy that will push automatic creation of tickets.



Creating a custom policy

Each policy rule contains details connected to the scanning hosts, type of vulnerabilities and ticket actions. As regarding the vulnerabilities, the best way is to target higher levels of security issues, but the application can also target just the particular vulnerabilities. The vulnerability database is regularly updated and you can easily search it to find the QID you are after. Under the ticket action menu you can assign tickets to different users, as well as create deadlines and ticket expiry dates.

The remediation module has its own report templates including Executive Remediation Report, Tickets per Vulnerability Report, Tickets per User Report and Tickets per Asset Group Report.



Tickets

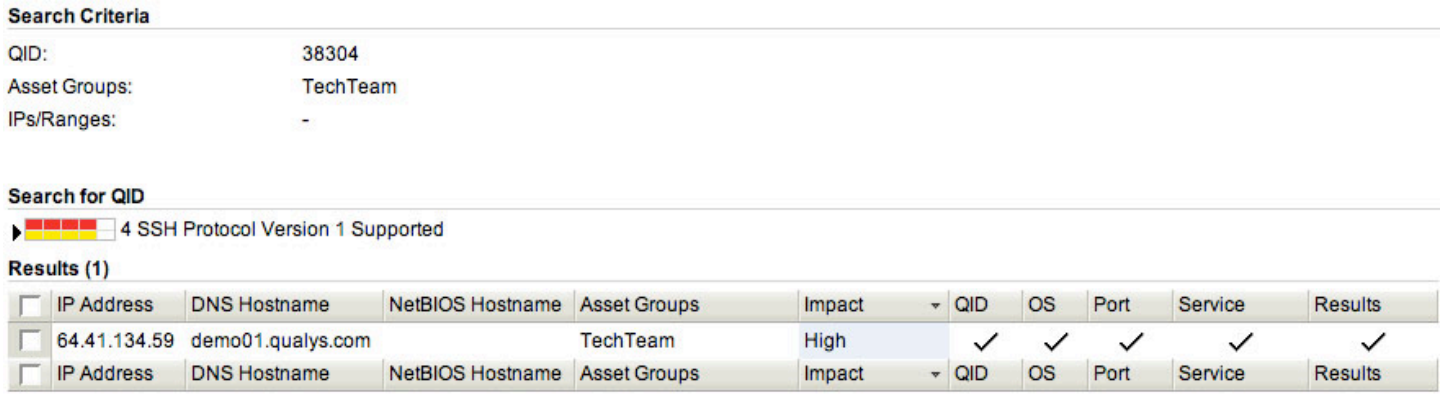
Actions: Edit Apply

View	Edit	Ticket #	State	Due Date	IP	DNS Hostname	NetBIOS Hostname	Severity	QID	Vulnerability Title
		000001	Open	11/20/2007	64.41.134.59	demo01.qualys.com		3	38139	SSL Server Has SSLv2 Enabled Vulnerability

Active ticket related to an SSL server

Risk analysis

Risk analysis is a quite interesting option for checking out your network security status for specific vulnerability. Within just a couple of seconds you hosts will be scanned for the particular security issue (based on a QID) and you'll get a report stating whether your hosts are affected by it. The service is also able to determine whether hosts are likely to be at risk to potential vulnerability by comparing exploit data to known information from past scans.



Search Criteria

QID: 38304
Asset Groups: TechTeam
IPs/Ranges: -

Search for QID

4 SSH Protocol Version 1 Supported

Results (1)

IP Address	DNS Hostname	NetBIOS Hostname	Asset Groups	Impact	QID	OS	Port	Service	Results
64.41.134.59	demo01.qualys.com		TechTeam	High	✓	✓	✓	✓	✓

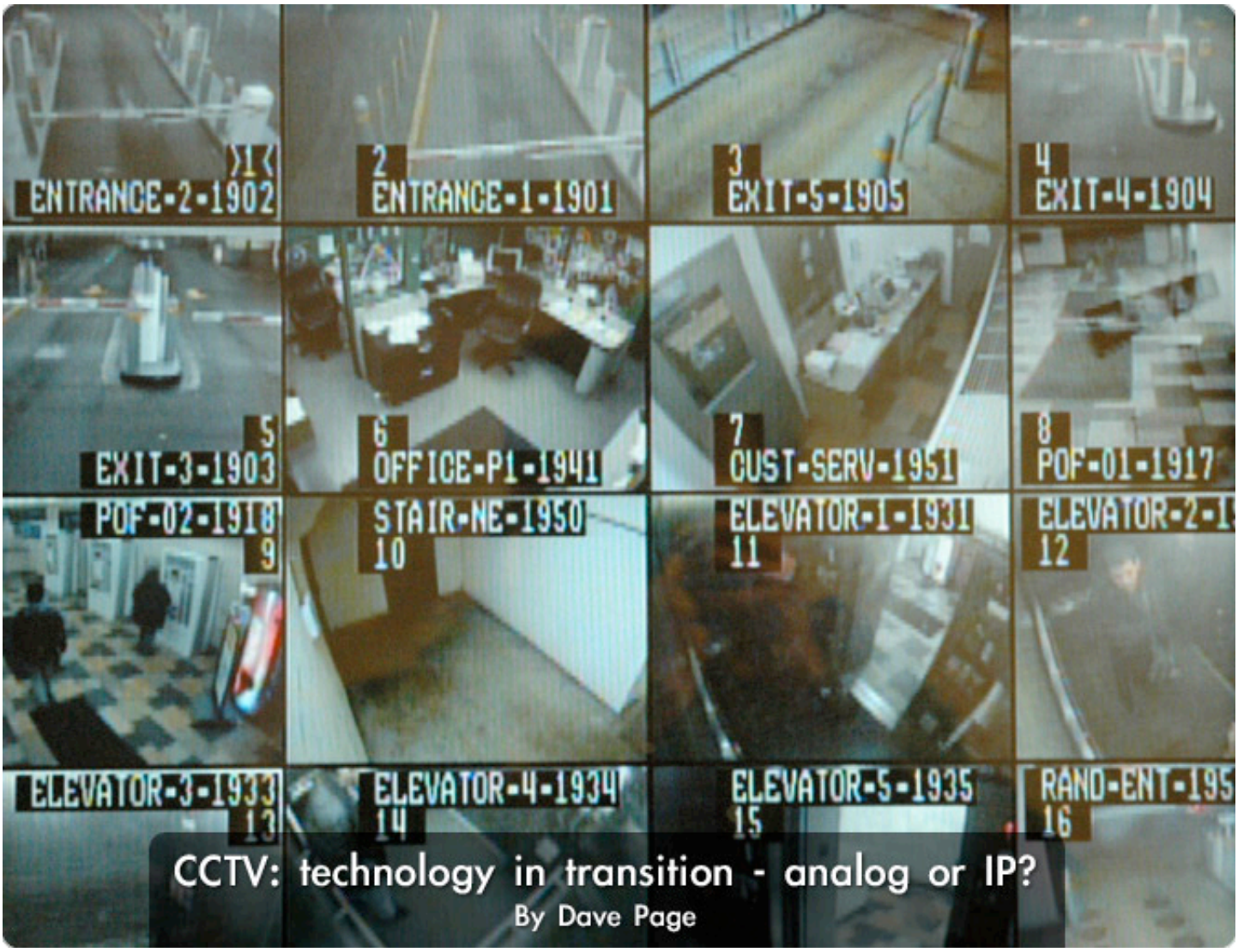
Results of a risk analysis test for a sample vulnerability

Final thoughts

I tested QualysGuard for a couple of days and I can really say that it is a terrific security solution for both large organizations with dispersed and complex networks, as well as small businesses.

With its powerful technology provided through a web browser user interface, QualysGuard is perfect solution that combines efficient automated security scans, powerful reporting and a must have ticketing procedure for tracking the remediation status of active vulnerabilities.

Mark Woodstone is a security consultant that works for a large Internet Presence Provider (IPP) that serves about 4000 clients from 30 countries worldwide.



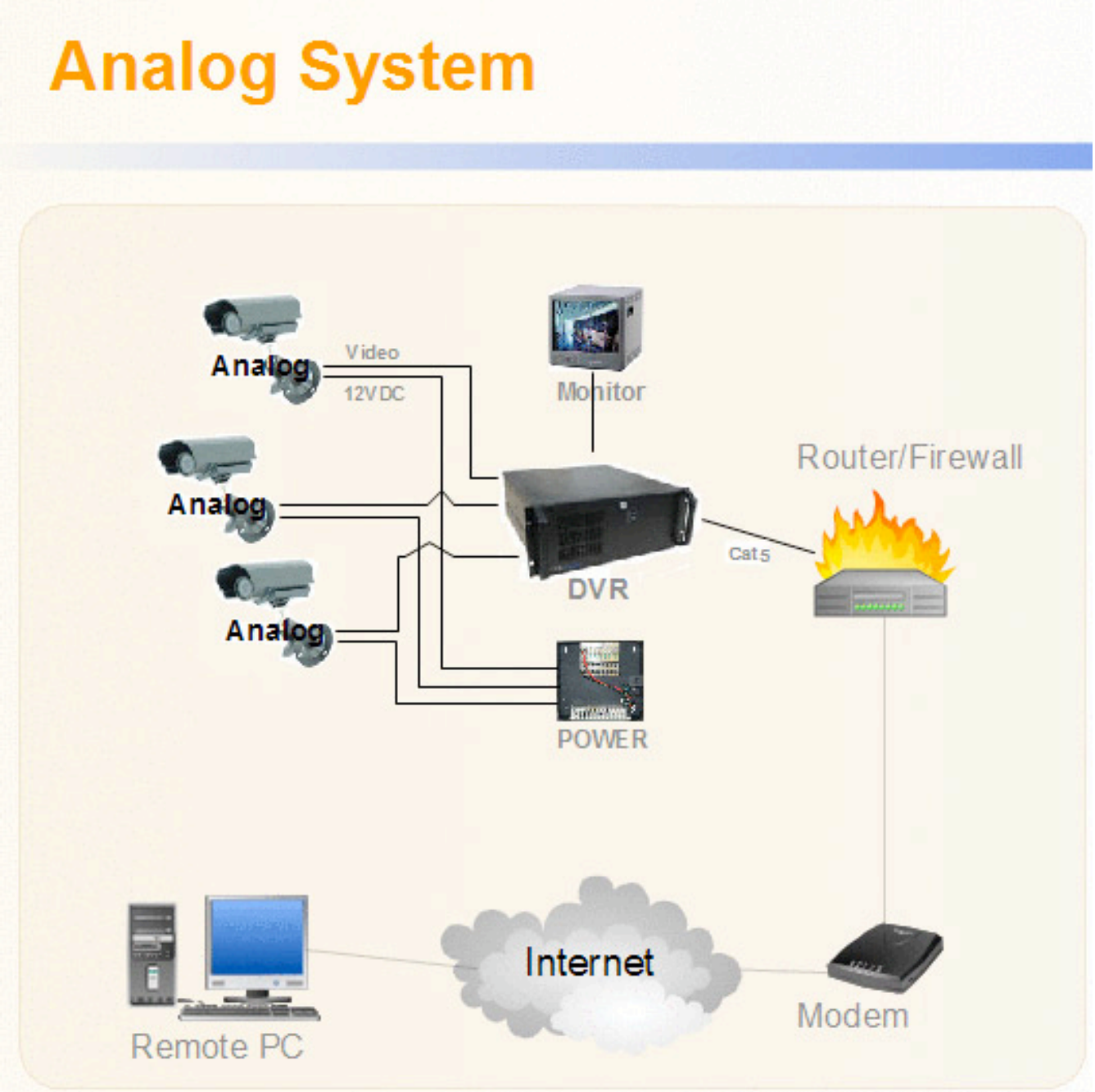
CCTV technology is in a period of rapid evolution. A key component of this change is the emergence of network based or Internet Protocol (IP) cameras. The transition from analog to IP is a difficult one because it requires knowledge of two previously separate disciplines - traditional CCTV technology and networking technology. There is a huge learning curve for existing CCTV resellers and installers that must be overcome for IP technology to be applied productively. This article will answer some basic questions about the differences between the analog and network-based approaches and where each is best employed.

Overview

The first diagram on the following page depicts the basic setup of an analog camera system and a network-based, or IP camera system. In the traditional analog CCTV application, security cameras capture an analog video signal and transfer that signal over coax cable to the Digital Video Recorder (DVR). Each camera may be powered by plugging in the power supply right at the camera or by using RG59 Siamese cable which bundles the video and the power cables. The DVR converts the analog signal to digital, compresses it, and then stores it on a hard drive for later retrieval.

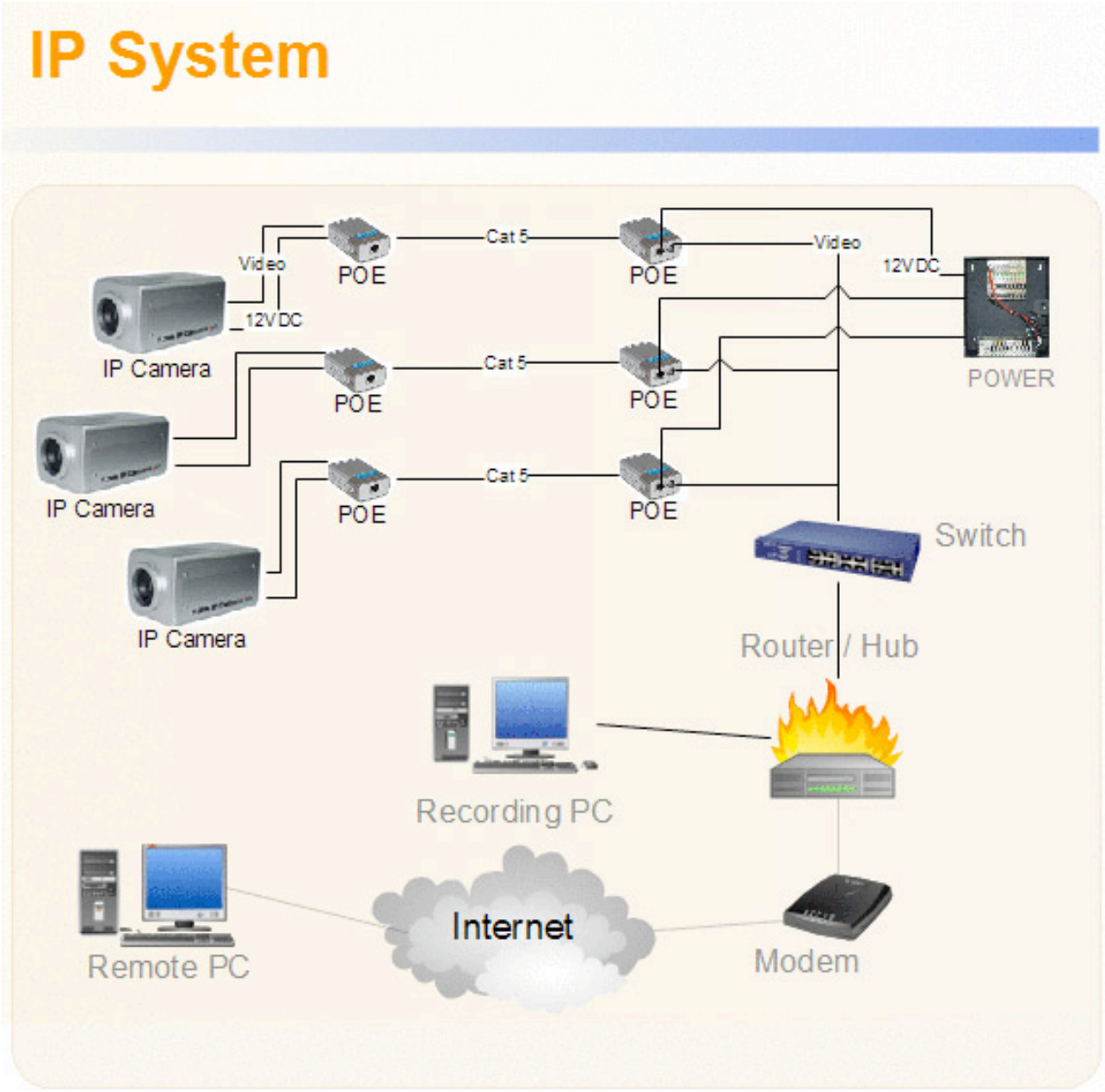
Intelligence is built into the DVR to handle such things as scheduling, motion detection, and digital zoom. Monitors for viewing the video are connected to the DVR, or it can be set up to publish over an internal network for viewing on PCs. The DVR can also be set up to broadcast over the Internet and can add password protection and other features.

When broadcasting over the Internet, the video for all of the cameras is transmitted as one stream (one IP address). Therefore, it is very efficient.



In the IP world, each network camera captures an analog image but immediately converts it to digital inside the camera. Some digital processing can happen right at the camera, such as compression and motion detection. The digital video stream is then broadcast over the IP network using Ethernet (CAT5) cable. The power supply may be plugged in at the camera or can be run over the ethernet cable by using Power-Over-Ethernet (POE) adapters. The CAT5 cable for each camera is plugged into a switch which feeds into the network hub. As with all network devices, some set-up needs to be done for each network camera to set up its IP address and other identifying attributes.

Software is required on each PC that you want to view the cameras or playback video. Another high powered PC is set up with the appropriate software to record the cameras. Since communication standards are not consistently followed in this industry yet, the viewing and recording software must be purchased from the same vendor that sells the IP cameras. This can make switching or mixing camera vendors very expensive.



Typically that requires a high-powered PC with considerable hard drive space. Often, that will cost as much as or more than a DVR. Even more significant is the price of the recording software which tends to be expensive. Licenses are typically based on number of cameras, and per user. The IP camera signal is broadcast over the Internet in the same way that a DVR signal is. However, each camera is a separate stream and has its own IP address or port. This can greatly affect bandwidth as we'll see below. When viewing remotely each camera can be pulled up individually by its IP address. If you want to see all of the cameras side-by-side, additional software (again, from the same camera vendor) must be installed.

Which approach is more cost-effective?

For now, installing analog cameras coupled with DVRs is the most cost-effective approach for most security applications. Later on, a couple of scenarios will be introduced whereby an IP-based solution might be less expensive.

A typical medium quality analog dome camera sells retail for about $100 to $200. A similar quality IP camera sells for at least twice that amount. Analog cameras are available with many different features: varifocal lenses, high resolutions, and long distance infrared, for example.

Finding just the right combination of features in a network camera for your application might be difficult and very expensive. Sometimes you may have to buy an analog camera and add a separate video server to do the job. Single-channel network video servers currently start at about $300 retail.

IP advocates will point out that a digital video recorder is not required in an IP solution. That is true, but some device will still be needed to record the camera images. Typically that requires a high-powered PC with considerable hard drive space. Often, that will cost as much as or more than a DVR. Even more significant is the price of the recording software which tends to be expensive. Licenses are typically based on number of cameras, and per user.

IP advocates may also point out that businesses often have IP networks in place and therefore no additional cabling or hardware is needed. However, each camera requires a port to plug into the switch, so more or bigger switches may need to be purchased. POE adapters might need to be added. If the existing network will not handle the load of the additional network devices, upgrades might need to be made, thereby making the installation more expensive.

Finally, bandwidth on the network needs to be considered. Video uses a lot of bandwidth. The bandwidth used by each camera varies by many factors including the resolution, the compression method, and even the amount of movement in the field-of-view.

As a general rule, a camera using full CIF (352 x 288) resolution, 30 frames per second (30 fps), and MPEG4 compression will require about 720K bits per second (720Kbps). Therefore, if we put 100 IP cameras on a network, we would use about 72Mbps more bandwidth. This number will double if audio is also transmitted. It should come as no surprise, then, that some companies have gone so far as to create an entirely separate IP network just to run their camera system.

To make bandwidth matters worse for IP – many of the newest IP cameras are coming out with 'megapixel' resolution. This is wonderful from the standpoint of how much clarity and field-of-view can be captured, but it comes at a huge price to bandwidth. A single 2-megapixel IP camera, running 30 fps with MPEG4 compression will use a whopping 6.5Mbps of bandwidth.

These high-resolution IP cameras also require a great deal of hard drive space to store the video. The 2-megapixel camera described above would require approximately 67 Gigs of hard drive space to record one day's worth of video.

It's worth noting that DVRs will also use bandwidth if viewed remotely over a network. However, the DVR will only use bandwidth if people are currently viewing the cameras. Otherwise, they will not. Furthermore, a DVR will combine several camera images into one video stream vs. a separate video stream for each camera, as in IP. For example, a typical 16 camera DVR will combine its camera images and throttle its output to a maximum 360Kbps. To run 16 similar IP cameras on a network would generate about 11Mbps.

Which approach is better quality?

There are poor quality components and good quality components no matter which type of system is used. That being said, network cameras do offer some technological advances in the areas of video quality and wireless installations.

Analog cameras cannot provide resolution above TV standards, the maximum being about 0.4 megapixel. Resolution of IP cameras can be many times higher (currently up to 3 megapixel) and they can capture a clearer image when objects are moving. This could make a difference in high risk applications such as for casinos and law enforcement. Wireless communication over IP networks has fewer problems with interference, and encryption security is built into the technology.

Which approach is easier to install and configure?

If an IP network is already in place at the installation site, and it can handle the additional load of the new cameras, then IP cameras will be easier to install.

If additional RJ-45 jacks are needed to plug in the network cameras, then the installer only has to run a CAT-5 cable from the camera to the nearest switch. An inexpensive switch can be installed right at the nearest wall jack. In contrast, each cable for analog cameras must be run all the way back to the DVR.

If upgrades need to be made to an existing IP network to handle the additional load, obviously the installation would be more difficult.

The power for the cameras can be handled fairly easily with either technology. For IP networks, use Power-Over-Ethernet (POE) transmitters to send the power through the existing CAT-5 cable.

For analog systems, use RG59 Siamese cable to combine the video and power cables into one jacket. Either way, there is no additional cabling for power. POE can run 300 feet without a repeater. RG59 can be run 1000 feet without a repeater.

Once the cabling is in place, configuring the system is less difficult for analog systems. With analog, you plug the cameras into the DVR and you've got video. For IP cameras, you have to assign each camera a network address and open up ports on the router. It's easier to set up cameras for internet viewing using a DVR because access is provided to all cameras at once by using one external IP address to the DVR.

What about wireless?

Analog wireless systems do not work well. This is because the government regulates on which frequencies analog wireless devices can run and how strong the signal can be. Interference from other wireless devices such as cell phones can cause the camera video to be distorted. Interference is especially problematic in buildings with florescent lighting.

Digital IP wireless is much better. The digital transmission does not get interference from other analog wireless devices, and the 802.11x communication standard used has encryption built in. Consequently, there is no problem with unauthorized access to the video.

For what applications should I consider IP?

IP cameras should be considered for large installation sites that already have a high bandwidth network installed – especially if the cameras will be spread out over a wide area, or if wireless cameras will be used.

For large installations with many cameras, some installers still prefer a multiple DVR solution to an IP solution. Software is bundled with higher-end DVRs that allows you to view and record cameras from multiple DVRs. Using analog cameras and multiple DVRs can be less costly than purchasing many IP cameras along with the required software licenses.

The multiple DVR solution also provides better fail-over protection. If the network goes down in an IP based system, video is lost from all the cameras. If the network goes down in an analog system, the DVRs are still recording the cameras. If one DVR has a problem, only the recorded video from the cameras on that particular DVR is lost. In contrast, if the recording PC goes down in an IP system, all video recording is stopped.

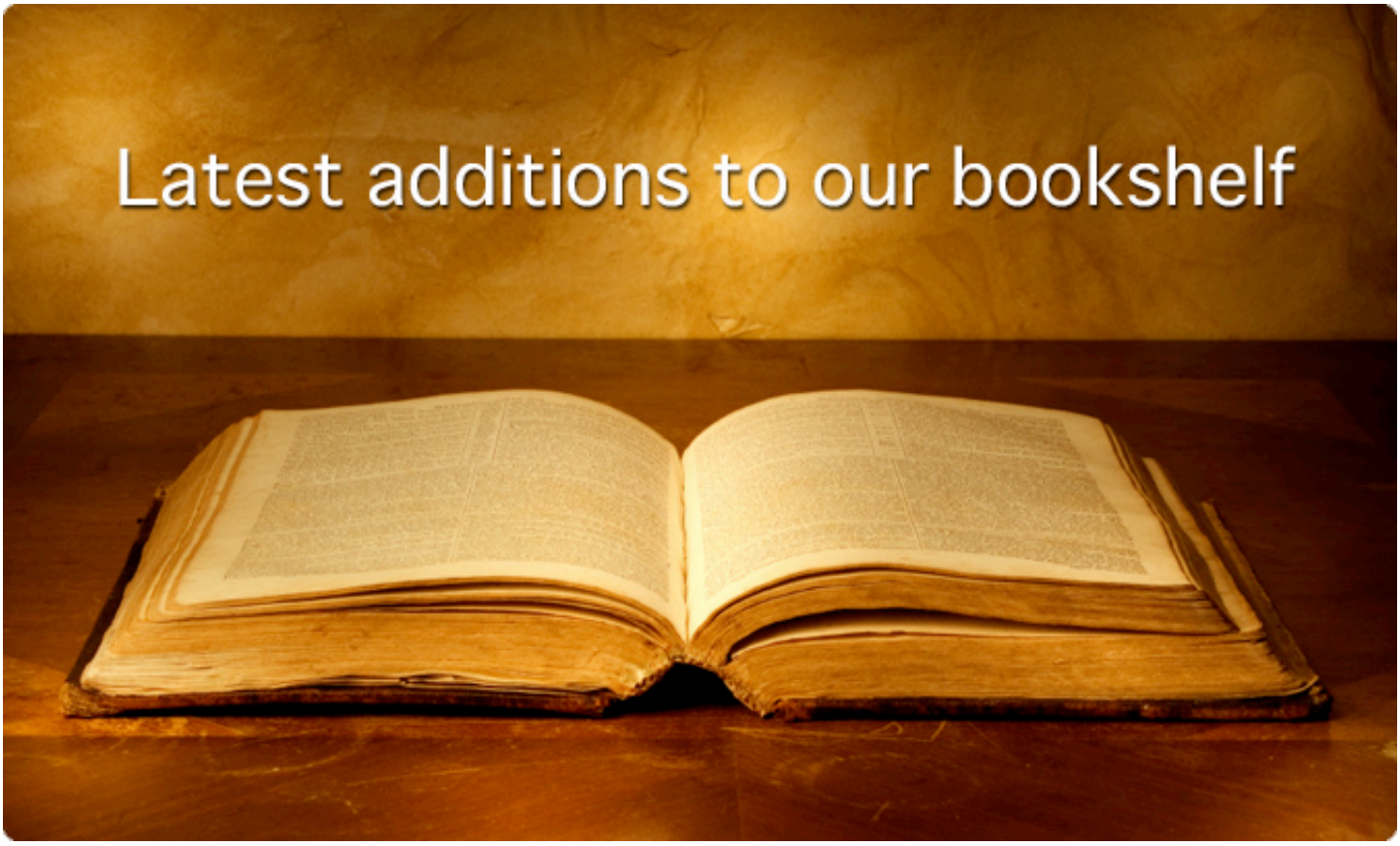
Conclusion

Network-based camera security is not yet the most cost-effective solution for most applications. The technology simply hasn't matured enough. Furthermore, professional skills are not widespread to effectively design and implement these systems.

Five years from now, the above questions will be obsolete, and new issues will take their place. Network CCTV technology will continue to evolve. New standards will be implemented, allowing the components to communicate more effectively with each other. Better standards will also allow third-party development of the software which will improve the software quality and bring down the overall cost.

With new products such as next-generation DVRs and network camera servers, the lines between these technologies will continue to dissipate. Hybrid solutions will be developed, which will employ both analog and digital components seamlessly.

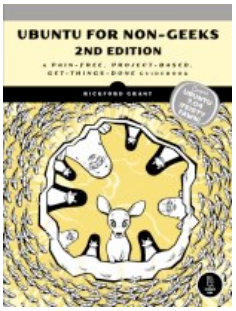
Dave Page is President of Discount Security Cameras, a US provider of professional security camera and surveillance equipment. See the website at www.discount-security-cameras.net.



Ubuntu for Non-Geeks, 2nd Edition: A Pain-Free, Project-Based, Get-Things-Done Guidebook

By Rickford Grant

No Starch Press, ISBN: 1593271522

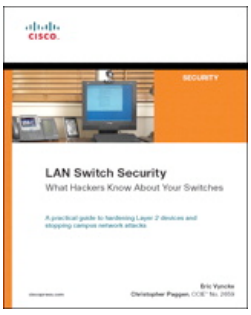


Tackling any operating system as a neophyte may be quite challenging. Thankfully, if you're thinking about giving Ubuntu Linux a spin, having this book on your desk will make life much easier. The book is divided into 18 chapters in which the author guides you through a myriad of tasks such as using the command line, installing applications, working with your iPod, updating software, and much more. The material is aimed at new users that want to get introduced to all that Linux has to offer.
Read a complete review at: www.net-security.org/review.php?id=167

LAN Switch Security: What Hackers Know About Your Switches

By Eric Vyncke, Christopher Paggen

Cisco Press, ISBN: 1587052563

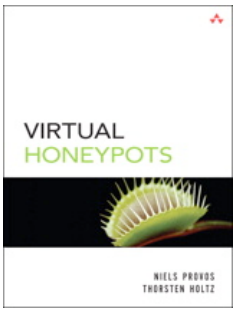


The majority of security books we review are focused on specific technologies, software platforms and hot security issues everyone is talking about. Cisco Press has a rather extensive line of books discussing their networking and security products and their publications often provide information on some lower level security issues. "LAN Switch Security" is a perfect sample of this kind of publications - authors Vyncke and Paggen are here to tell you why Ethernet switches are not inherently secure.
Read a complete review at: www.net-security.org/review.php?id=168

Virtual Honeypots: From Botnet Tracking to Intrusion Detection

By Niels Provos, Thorsten Holz

Addison-Wesley Professional, ISBN: 0321336321



In order to stay one step ahead the attackers you have to learn what they know. Virtual honeypots enable security professionals to identify potential risks and improve their defensive techniques.

Written by two industry veterans, "Virtual Honeypots" promises to tackle this topic heads-on, with lots of technical details.
Read a complete review at: www.net-security.org/review.php?id=164

Linux Firewalls: Attack Detection and Response with iptables, psad, and fwsnort

By Michael Rash

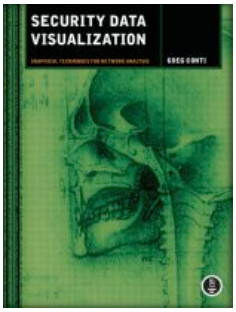
No Starch Press, ISBN: 1593271417

Linux Firewalls discusses the technical details of the iptables firewall and the Netfilter framework that are built into the Linux kernel, and it explains how they provide strong filtering, NAT, state tracking, and application layer inspection capabilities that rival many commercial tools. You'll learn how to deploy iptables as an IDS with psad and fwsnort and how to build a strong, passive authentication layer around iptables with fwknop.
Read a complete review at: www.net-security.org/review.php?id=165

Security Data Visualization: Graphical Techniques for Network Analysis

By Greg Conti

No Starch Press, ISBN: 1593271433

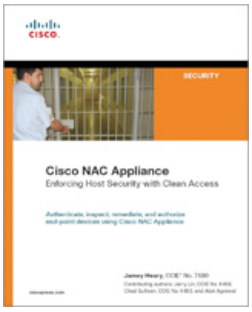


The visualization of security data is useful to the modern security analyst, and it will certainly become essential in certain environments very soon. Never has there been more traffic, more threats and a variety of other reasons to learn more about it. One thing is certain, after going through this book you'll realize that going through an endless stream of raw logs is not the only way to keep an eye on your network and identify potential threats.
Read a complete review at: www.net-security.org/review.php?id=169

Cisco NAC Appliance: Enforcing Host Security with Clean Access

By Chad Sullivan, Jamey Heary, Alok Agrawal and Jerry Lin

Cisco Press, ISBN: 1587053063

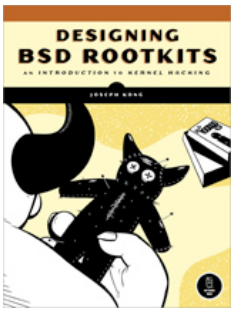


Cisco Network Admission Control (NAC) Appliance, formerly known as Cisco Clean Access, provides a powerful host security policy inspection, enforcement, and remediation solution that is designed to meet these new challenges. This Cisco Press publication provides you with all the information needed to understand, design, configure, deploy, and troubleshoot the Cisco NAC Appliance solution. You will learn about all aspects of the NAC Appliance solution including configuration and best practices for design, implementation, troubleshooting, and creating a host security policy.

Designing BSD Rootkits: An Introduction to Kernel Hacking

By Joseph Kong

No Starch Press, ISBN: 1593271425



Designing BSD Rootkits introduces the fundamentals of programming and developing rootkits under the FreeBSD operating system. In addition to explaining rootkits and rootkit writing, the book aims to inspire readers to explore the FreeBSD kernel and gain a better understanding of the kernel and the FreeBSD operating system itself. Written in a friendly, accessible style and sprinkled with geek humor and pop culture references, the author favors a "learn by example" approach that assumes no prior kernel hacking experience.

End-to-End Network Security: Defense-in-Depth

By Omar Santos

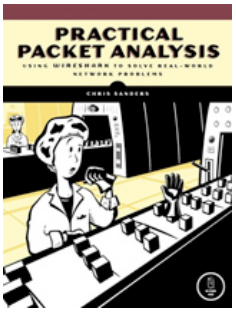
Cisco Press, ISBN: 1587053322

End-to-End Network Security is designed to counter the new generation of complex threats. Adopting this robust security strategy defends against highly sophisticated attacks that can occur at multiple locations in your network. The ultimate goal is to deploy a set of security capabilities that together create an intelligent, self-defending network that identifies attacks as they occur, generates alerts as appropriate, and then automatically responds. End-to-End Network Security provides you with a comprehensive look at the mechanisms to counter threats to each part of your network.

Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems

By Chris Sanders

No Starch Press, ISBN: 1593271492



Wireshark is the world's most powerful "packet sniffer", allowing its users to uncover valuable information about computer networks. Rather than simply take readers through Wireshark's tools Practical Packet Analysis shows how to use the software to monitor their own networks. The book is aimed at network engineers and system administrators, but it's clear enough even for Wireshark newbies. Includes a bonus CD with trace file examples as well as videos that show packet analysis in action.

Cisco ASA, PIX, and FWSM Firewall Handbook

By David Hucaby

Cisco Press, ISBN: 1587054574

This is a guide for the most commonly implemented features of the popular Cisco firewall security solutions. Fully updated to cover the latest firewall releases, this book helps you to quickly and easily configure, integrate, and manage the entire suite of Cisco firewall products, including ASA, PIX, and the Catalyst Firewall Services Module (FWSM). Organized by families of features, this book helps you get up to speed quickly and efficiently on topics such as file management, building connectivity, controlling access, firewall management, increasing availability with failover, load balancing, logging, and verifying operation.

Robert ("RSnake") Hansen (CISSP) is the CEO of SecTheory, an internet security consulting firm. Mr. Hansen founded the web application security lab at http://ha.ckers.org. He has worked for eBay, Realtor.com and Cable & Wireless. He has spoken at Blackhat, Microsoft's Bluehat, and he is a member of WASC, OWASP, and ISSA.

What is the proper way to manage web application security? What are the the most important things to keep an eye on?

One of the most important things to remember is to log. I see a lot of people using things like Google Analytics or Omniture, but because they use tracking pixles and JavaScript they miss almost all the interesting things that a website sees. If you can't see your traffic how can you possibly know what's going on? Once you have that, focus on the primary attack points. Typically on a site that has users, those are the authentication pages, the registration pages, the change password, change email address, change secret questions and inter-user communication pages.

Focus the majority of your security in those places. Of course, I always like to use libraries to mitigate things like CSRF, XSS and SQL Injection. Instead of having to worry each time about how to protect yourself, using libraries for each instance of insertion into a database (a database access layer) really helps to nail things down. Ultimately though, websites are pretty custom these days so it's a crap shoot on if you are doing a good job in your application if you don't know what you're doing. A crap shoot with really bad odds, I might add.

When doing research, how do you approach a potential vulnerability?

I generally start with an assumption of vulnerability - I'm rarely proven wrong, unfortunately. Unlike binary exploit development you don't see things crash - a lot of times I have a lot less information to go on than your traditional exploit author. However, one of the advantages of knowing how to program is I know what shortcuts and mistakes I'd probably make in an effort to ship something if I had

written the software. One thing you'll hear me saying over and over to people I meet is that the only difference between programmers and hackers is that programmers spend their entire day trying to make something work, while hackers spend their entire day trying to think of ways to make the same thing fail.

To be more precise, there is almost always additional functionality you can add into a program by understanding that most programmers don't really understand regex, they fail to sanitize and even if they do know what they're doing they often don't think of all the use cases. People say that a thief has to get it right every time while a police officer has the luxury of being able to hit and miss. Unfortunately in the virtual world it's reversed in some ways - the attacker has a huge advantage in that they only have to find one exploit, while the developer has to protect against everything.

With that in mind, I spend a great deal of time thinking of how things can be used in slightly different ways than they were intended and therefore abused. That's how I came up with most of the Intranet hacking stuff with JavaScript. By taking a step back and saying, "Wait, sure, my browser can contact anything on the internet, but is that always a good thing?" you start seeing that there are a lot of vulnerabilities in almost everything we use on the web.

In your opinion, how has the web security scene evolved in the last few years?

Honestly, when I started in webappsec it was back in the mid 90's. The last few years though have been the really interesting part. It's not due to AJAX, despite what a lot of people thing. It's due to SAAS (software as a service). People suddenly started thinking that everything they do needs to be on the web. Almost everything I want access to is now accessible with a credential and a browser. That makes things a lot more exciting from a security perspective. We basically eradicated one of the original reasons we had a firewall - to protect our sensitive data from the outside.

Two years ago I could count the interesting webappsec sites on one hand. Now there are dozens of them - too many to keep up with actually. In fact I have trouble keeping up with sla.ckers.org alone, and I run it! Now that people are becoming more aware of the issues, it's starting to manifest itself as more interesting tools, and techniques. I feel pretty confident a determined group of hackers could break into any website these days, and that's finally legitimized the niche of webappsec.

The only difference between programmers and hackers is that programmers spend their entire day trying to make something work, while hackers spend their entire day trying to think of ways to make the same thing fail.

What web application scanners do you use?

A better question would be which ones don't I use! I change around quite a bit depending on the website, the circumstances, and the time I have to audit. Unfortunately, the more comprehensive scanners can take days to scan a complex app (or more). A lot of times I don't have that kind of time, so I end up doing the majority of my work by hand. It's kind of sad that I end up finding more issues than most scanners, and more quickly - but I think that will change with time as the technology improves. But to answer your question, my favorite tools in my arsenal (including the manual ones) are: Burp Suite, THC Hydra, fierce, Nessus, Nikto, nmap, NTOSpider (commerical), httprint, Cain, sn00per, Absynthe, Sqlninja, a half dozen Firefox plugins like Webdeveloper, JSView, NoScript, Greasemonkey etc... and the entire suite of unix utils out there, like wget, telnet, ncftp, etc.

It's really sad that I don't need much more than that do be pretty effective at breaking into the majority of sites out there, now that I think about it.

When it comes to security, what's your take on the increasing use of Ajax in all sorts of web applications?

This is a tricky subject and depending on who you talk to you'll get different answers. Here's my take. AJAX for the most part doesn't add any additional vulnerabilities. There are some caveats to that though. The first is that traditional applications only have to sanitize output once (at the server level). AJAX apps have to do it twice, once at the server and once in the JavaScript. So it doubles up the potential for vulnerability, as you can send the information directly to the server bypassing the JavaScript protection. It also allows remote websites to pull in the JavaScript - so using JSON can be dangerous if it contains sensitive information.

The only new issue that I've seen it create is that sometimes people will throw all the sensitive information into the AJAX request and let the JavaScript parse it apart. All you need to do is watch the wire or look at the JS source and suddenly you get all the information you were after. That's rare, but it does happen, where it never happened before. Honestly though, I think AJAX is a bit over hyped from a security perspective except for the fact that more websites are building more dynamic applications - which is always a dangerous proposition unless they know what they are doing.

I think AJAX is a bit over hyped from a security perspective except for the fact that more websites are building more dynamic applications - which is always a dangerous proposition unless they know what they are doing.

You are one of the authors of "Cross Site Scripting Attacks: XSS Exploits and Defense". How long did the writing process take? What was it like to cooperate with other authors? Any major difficulties?

The whole thing from start to finish was only a few months (which you may be able to tell from some of the editing). But honestly, the group really came together once PDP got on board. I think we all struggling to find the time to write our sections until he got there and saved the day.

As it stands, I think PDP wrote 1/3, I wrote 1/3 and the rest wrote the remaining portions. We all contributed pretty heavily, and given how much material is in the book, I think it turned out very well. The only major difficulties were getting the time necessary. I had no idea how hard it would be to write that book, honestly.

Recently you've pointed out serious problems with WordPress security, can you share some details with our readers?

Fundamentally, WordPress suffers from all the same problems as any home-brew application that was organically built for the general public. It was never designed to be secure. It used to suffer from lots of cross site scripting and cross site request forgery exploits. Some of that stuff has been closed down, some hasn't. But really the underlying problem that I believe it suffers from is that it has the ability to write to disc, instead of being in the database context. It can overwrite php files, .htaccess files and does so as the www user. If there is ever any server vulnerability, kiss your website goodbye. If that's not scary enough, if you are running on a shared host, other users of the system can take over your website since the files need to be writable by the webserver user.

I'm just not a fan of that architecture - which is problematic since I run a WordPress powered blog. Over the last 6 months or so I've made heavy modifications, mostly involving removing most of the functionality people like about administering WordPress. A lot of people have asked me for the source, but I haven't made it open source. It's something I've considered, but there are lots of other more important projects on my radar than supporting an open source platform. So it's on the back burner for now.

What should be done to increase web application security awareness?

I've never been a fan of consumer education for security - I've seen reports where companies have spent millions on user education and not seen any lift in their fraud ratios as a result. But I think there is hope in educating security people of the issues. I know lots of people think that stupid users are to blame for getting hacked, but I totally disagree with that (I like to think I have a pretty modern view of security in this regard).

Let's take an example of a user who logs into a Windows machine for the first time. It complains that there is no AV or Firewall. So they turn on Windows firewall or install another one, and the AV of their choice. They patch up because Windows yells at them. Does that make them secure? They've followed every piece of advice that we as the security community have programatically offered them. The answer, unfortunately is that we, as a security community, have done a miserable job in giving consumers the correct tools to secure themselves.

I like to quote Hamlet, "The fault, dear Brutus, is not in our stars, But in ourselves..." I don't look to consumers to solve the security community's problems. We as a security community have a very serious problem to fix, and I think it mostly comes down to educating the people who can actually make the biggest difference - the browser and operating system community.

I've spent the last three or four years working closely with Microsoft and Mozilla to make them aware of the problem, offering suggestions and helping them test their emerging technologies. Demonstrating vulnerabilities and helping them fix their products is the only way to help consumers long term by coming up with best practices and better security technologies that fundamentally shift how we do business online.

We, as a security community, have done a miserable job in giving consumers the correct tools to secure themselves.

What are your future plans? Any exciting new projects?

Well, I'm getting my company up and off the ground - helping companies realize their exposure, and fixing the holes. So I've been pretty swamped with that. But I always have 50 projects in the wings. Most recently I've been doing a lot of work on understanding the costs of bots on a web application. There are lots of hidden costs, and most people don't get that the application is getting hurt in more than just a few ways by a single malicious robot. I'll write up some results once I get some time to sort through the data we've compiled.

Another project I've been working on for quite a while is the Fierce domain scanner (which is really helpful in finding non-contiguous IP blocks as a pre-cursor to an Nmap type scan). I've actually recently gotten a few volunteer requests to help out with future revisions so I'm hoping we'll see something interesting come of that. Really though, you never know, maybe one of these days I'll hire a full time technical research assistant to finally build all my crazy ideas for me!

As a parting thought, I'm pretty overwhelmed by the support of the community. A few years ago there was almost no one doing any noteworthy research and suddenly over the last two years everyone has started paying attention. I get a lot of credit for raising webappsec awareness, but I'm only one person.

Ha.ckers.org has been marked as a phishing site, a malware site, it's been taken offline, suffered countless attacks and it's been under scrutiny by just about every agency on earth. It's one of the hardest websites on earth to maintain. But the good news is the readers have taken the message home to their companies. None of this would have been possible without them and the other often unsung researchers in the space.

In today's world the protection of sensitive data is one of the most critical concerns for organizations and their customers. This, coupled with growing regulatory pressures, is forcing businesses to protect the integrity, privacy and security of critical information. As a result cryptography is emerging as the foundation for enterprise data security and compliance, and quickly becoming the foundation of security best practice. Cryptography, once seen as a specialized, esoteric discipline of information security, is coming of age.

No one would argue that cryptography and encryption are new technologies. It was true decades ago and it is still true today – encryption is the most reliable way to secure data.

National security agencies and major financial institutions have long protected their sensitive data using cryptography and encryption. Today the use of encryption is growing rapidly, being deployed in a much wider set of industry sectors and across an increasing range of applications and platforms. Put simply, cryptography and encryption have become one of the hottest technologies in the IT security industry – the challenge now is to ensure that IT organizations are equipped to handle this shift and are laying the groundwork today to satisfy their future needs.

Last line of defense for personal data

As many merchants and retailers take action in order to meet the stringent Payment Card Industry Data Security Standard (PCI DSS), the need to protect sensitive credit card data is first and foremost on their minds. This is highlighted in the recent finding by the Canadian government that the lack of proper encryption was to blame for the TJX breach that exposed at least 45 million customers' credit and debit card records. But looking more broadly the issue isn't limited to just credit card data. In September, more than 800,000 people who applied for jobs at clothing retailer the Gap Inc. were alerted to the fact that a laptop containing personal information such as social security numbers was stolen, exposing the applicants to potential identity theft.

It is clear that the protection of personal or private data is critical to the well being of any company that stores or processes this information. Encryption has become a last line of defense for data protection because, once data is encrypted, if stolen or even simply misplaced, it is rendered unreadable without the keys to decrypt that data.

Survey says

A recent independent survey conducted by industry analyst firm Aberdeen Group shows an increasing use of encryption and a growing need for centralized and automated key management. The survey, "Encryption and Key Management" found that Best-in-Class organizations (a category that Aberdeen defined as including organizations that have seen the most improvement in their IT security effectiveness over the past 12 months) demonstrated a tremendous increase in the number of applications and locations deploying cryptography in order to protect sensitive data compared with one year ago and, consequently, an increase in the number of encryption keys they have to manage.

Eighty-one percent of respondents had increased the number of applications using encryption, 50 percent had increased the number of locations implementing encryption and 71 percent had increased the number of encryption keys under management compared with one year ago.

How is the growth of encryption and the need to manage the keys changing organizations' behaviors? In order to address the challenges brought about by the increased deployment of cryptography, Best-in-Class companies have shifted their thinking and were 60 percent more likely than the industry average group to take a more strategic, enterprise-wide approach to encryption and key management than the traditional more tactical approach of addressing particular and isolated points of risk within their infrastructure such as the theft of laptops or back-up tapes. To further quantify this shift, the Aberdeen Group survey describes the significantly higher priorities and corresponding investments by the same Best-in-Class companies in specific encryption and key management technologies to complement other organizational structure and process related topics. The survey concludes that these pioneering organizations have already benefited by lowering the instances of actual or potential exposure while simultaneously reducing actual key management costs by an average of 34 percent.

Cryptography - embedded security by default

As Aberdeen and other independent analysts have discussed, access to encryption technology is getting easier and easier, with it often coming along for free, and has already made its way into a host of devices we use every day. Laptop computers, wireless access points, and even devices we don't think of as being part of a typical IT infrastructure such as vending machines, parking meters, gaming machines and electronic voting terminals, have encryption embedded. The same is true for business applications and data center hardware such as back-up tape devices and database software. This is steadily resolving one of the big challenges with encryption, how to upgrade existing systems to support encryption without penalizing performance or costing a fortune in custom developments or 'bolt-on' encryption products.

Don't forget the keys

The widespread availability of encryption is good news but without a clear way of managing its deployment a number of pitfalls remain. Organizations of all sizes and in all industries need to look seriously at the management of the cryptographic keys, the secret codes that lock and unlock the data. Unless organizations begin laying the groundwork today this new age of encryption will present serious management challenges. Encryption is a powerful tool, but getting it wrong either from a technology or operational perspective can at best result in a false sense of security and, at worst, leave your data scrambled forever.

Protecting data is important, but if a key is lost, access to all of the data originally encrypted by that key is also lost. To put it bluntly, encryption without competent key management is effectively electronic data shredding. Just as with house keys, office keys or car keys, great care must be taken to

keep back-ups and special thought needs to be given to who has access to keys. Establishing a key management policy and creating an infrastructure to enforce it is therefore an important component of a successful enterprise security deployment.

Key management brings encryption under control

Key management can't just be an after thought, it is the process by which encryption and cryptography become effective security and business tools. Key management is about bringing encryption processes under control, both from a security and a cost perspective. Keys must be created according to the correct process, backed up in case of disaster, delivered to the systems that need them, on time and ideally automatically, under the control of the appropriate people and, finally, deleted at the end of their life-span. In addition to the logistics of handling keys securely, which are secrets after all, it is also critical to set and enforce policies that define the use of keys – the who, when, where and why of data access. Archiving, recovery and delivery of keys are all crucial parts of the equation. For instance, if a laptop breaks down or a back-up tape is stolen the issue is not just one of security, but also business continuity. Information recovery takes on a whole new dimension, particularly in an emergency situation when the recovery process is performed in a different location, by a different team, governed by different policies and on protected data that is years or even decades old. What used to be a data management problem is now also a serious key management problem.

Enterprise key management recommendations

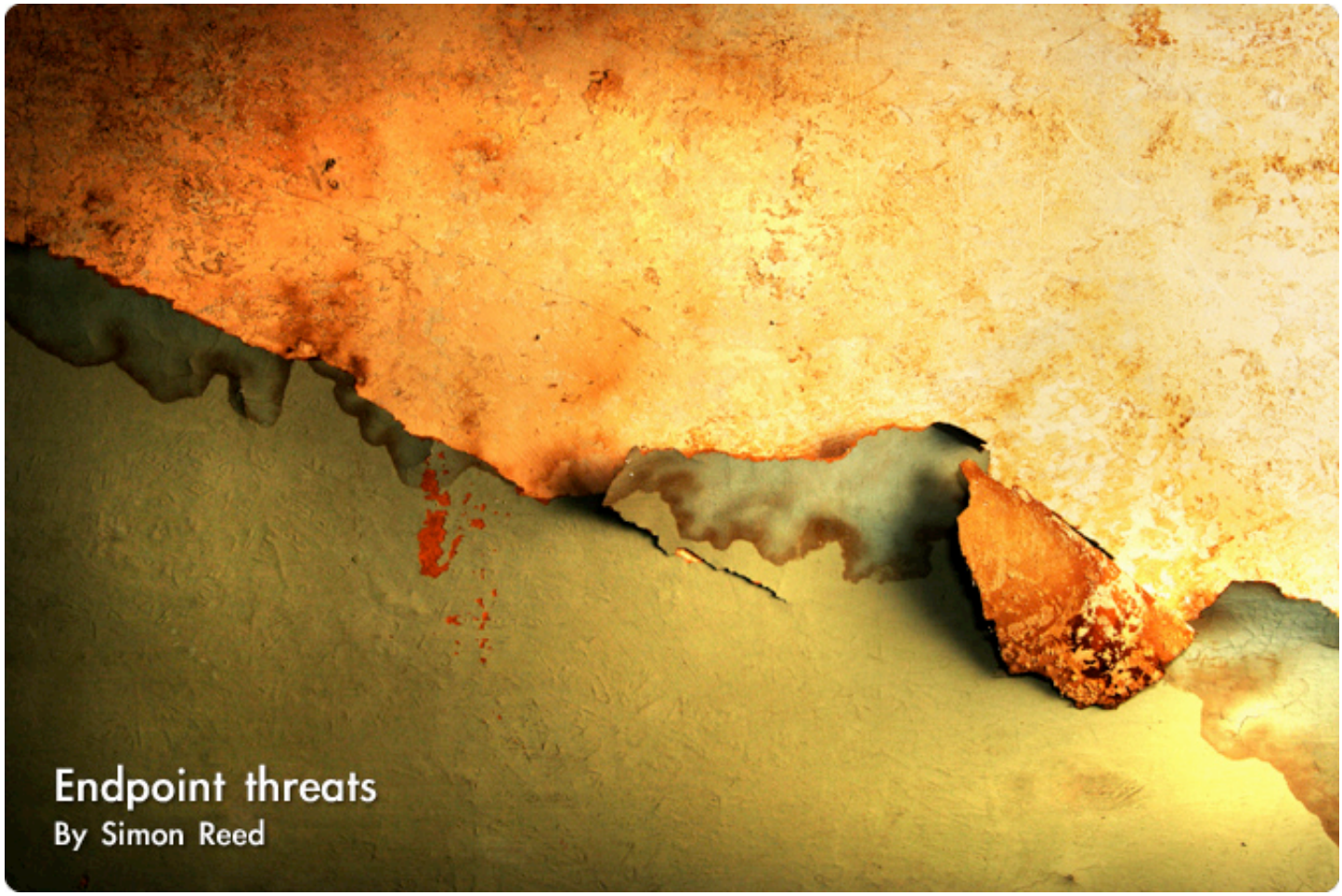
Traditionally key management has been tied to the specific applications in use and therefore quickly becomes fragmented and ad hoc as the number of applications increases. Scalability quickly becomes an issue as a result of relying on manual processes for renewing certificates, rolling-over keys or moving and replicating keys across multiple host machines and removing keys as machines and storage media are retired, fail or redeployed. This frequently results in escalating costs particularly in situations where security and audit ability are high priorities.

In many situations the only way to adequately deal with these challenges is through the use of a dedicated, general purpose key management system. Such a system can act as a centralized repository for storing keys on behalf of multiple applications or 'end-points', distributing keys on demand. This provides a simple mechanism to unify key management policies and automate key life-cycle management tasks, greatly reducing costs and easing time critical tasks such as key recovery, key revocation and auditing. Important product selection criteria include scalability and the range of end-points that can be managed both in terms of target application and type of host platform and operating system. Finally due to the unique security characteristics of key management tasks, the absolute security properties of the key management system become important additional selection criteria. This includes the security of the key repository, tamper controls surrounding audit capabilities and the fundamental integrity of the key management software.

Conclusion

At the end of the day we need to protect our data. Increasingly, encryption is being seen as the best way to ensure that data is protected, but the ever growing use of encryption creates a management challenge. The challenge, however, doesn't need to be daunting. Implementing a flexible and extensible solution that automates many of the time-consuming and error-prone key management tasks in an automated enterprise-wide manner is rapidly becoming a priority for many organizations. In order for enterprise-wide encryption to be deployed correctly, organizations need to deploy the correct tool to manage the keys. In the same way that data protection has moved from an IT challenge to a C-level issue, key management has become a high-level business imperative.

Richard Moulds is VP of product management at nCipher. He leads the company's product strategy including that of keyAuthority, nCipher's key management solution. Richard has more than 20 years of technology marketing and business development experience. Richard holds a bachelor's degree in electrical engineering from Birmingham University and an MBA from Warwick University, UK.



In spite of greater awareness of the risks and security threats facing companies and professional firms around the world today, security breaches are on the rise and seriously threatening the health of businesses and the privacy of their clients.

Even though IT administrators have at their disposal an extensive arsenal of security solutions, cyber criminals are still successfully attacking systems and stealing valuable data which they can use for credit card fraud, identity theft and other malicious activity – activity which is only limited to the imagination of the cyber criminal himself. Companies in every sector are continuing to report security breaches and yet still allow their most sensitive and confidential information to be exposed.

And the statistics confirm an unhealthy situation:

• According to the Privacy Rights Clearinghouse, between January 2005 and October 2007, more than 167 million records containing sensitive personal information have been involved in security breaches in the US alone. The actual figure is probably even higher because data leaks are almost certainly under-detected and under-reported.

• A 2007 survey conducted by Forrester Consulting among 151 enterprises entitled Data Loss Prevention and Endpoint Security: Survey Findings shows that 52% have lost confidential data through removable media such as USB drives in the past two years. The survey also found that intellectual property, customer data and company financials are the top three concerns for data loss at the endpoint while data loss via USB drives and other removable media is the top concern (72%) for endpoint security, followed by Trojans, spyware and other threats.

• The third annual Higher Education IT Security Report Card released by CDW Government, Inc. in October found that despite increased attention to better IT security in higher education, there has been little progress and concludes that less than half of

• campus networks are safe from attack, with 58% reporting at least one security breach in the last year. Data loss or theft has increased 10% in the last year, up to 43%. That includes loss or theft of staff and student personal information.

• Research carried out by GFI Software in Q2 found that 65% of companies were needlessly putting themselves at risk because they underestimated the threat posed to their network's security by USB sticks, flash drives, iPods and PDAs. Although 49% of 370 UK companies surveyed said they were concerned about data theft, 65% did not consider the use of these devices on their network to be a security threat and 83% admitted to giving their employees USB sticks or PDAs to enabled mobile working (76%) and make data sharing easier (61%).

• A recent Information Security survey in the European Union demonstrated the vulnerability of corporate information when it found that 45% of employees take data with them when they change jobs. Employees have taken anything from documents and lists to sales proposals and contracts.

The statistics are backed up by numerous incidents that have hit companies around the globe. The following examples are just the tip of the iceberg but serve to highlight the growing number of security breaches and data loss cases over the past 10 months and the ease with which data is being lost, stolen and used maliciously.

• Undoubtedly, the largest breach ever! TJX, parent company to the TJ Maxx brand, revealed that at least 45.7 million credit and debit card numbers were stolen by hackers who accessed their computer systems at the TJX headquarters in Framingham, United Kingdom, over a period of several years. That figure has now shot up to over 90 million.

• A US citizen stumbled across a computer memory stick at a filling station in Azle, Texas, a town of about 10,000 northwest of Fort Worth, which contained information about the Joint Strike Fighter, the US's most expensive weapons program.

• A former Boeing employee, accused of stealing 320,000 files and leaking them to a newspaper, copied the sensitive information to a portable drive during a period from 2004 to 2006, breaching Boeing's security policies. The firm calculated that the potential damage could cost between $5 and $15 billion.

• A Japanese policeman from the Metropolitan Police Department in Tokyo was sacked after the personal information of thousands of people relating to criminal investigations was leaked on to the internet from his computer. Personal details of 12,000 people related to criminal investigations were spread across the web and around 6,600 police documents were compromised.

• A huge German manufacturing company suffered an intellectual property breach in Q3, when it discovered that a competitor had copied one of their products. A foreman had sent detailed information about a component to an external design department without telling his IT department or encrypting this information, thus allowing the competitor to get hold of it.

The weakest link

The adoption of the internet as a core business requirement coupled with the massive uptake of consumer technologies – such as plug & play, USB devices, Wireless devices, mobile phones and so on – have led to an increase in the number of ways that can be used by cyber criminals to achieve their target and, in a way, they have made it easier for data to be leaked, copied and used fraudulently.

Most companies today deploy some form of security measure on their network. The most basic of approaches to network security focuses on the perimeter and the majority have a firewall, IDS, anti-virus and anti-spam software protecting them from outsiders. Larger enterprises which have a proper IT department in place are in a better position to dedicate more time and resources to the deployment of vulnerability management solutions and other security measures to close as many backdoors as possible and to narrow the hacker's window of opportunity.

But does this mean that their networks are secure? Have they considered every attack vector? The answer, unfortunately, is no.

Every network is as strong as its weakest link and it only takes one small kink in a company's armour for a cyber criminal to enter, exploit the network and make off with precious commercially sensitive data and confidential details belonging to hundreds if not thousands of clients who have put their trust in that entity. The proliferation of consumer devices and the increase in usage of social websites like Facebook and MySpace, have opened new avenues through which data can be obtained and these are not managed by 'traditional' security measures, because more often than not, the weakest link in a network's security is not technology in itself, but the people who use it.

The human element in network security

Computer users can be considered as the least predictable and controlled security vulnerability. In the majority of cases, a lack of education and an understanding of basic security principles and procedures are the main causes of security breaches rather than malicious activity (although the latter can never be ignored). However, the end-result is usually the same: priceless data is lost, the company loses credibility and so on.

It takes so little for a security breach to occur. Huge amounts of data are lost because employees put their passwords on sticky notes on their monitors, forget laptops or handheld devices in airports, gyms and restaurants or in their car, keep computers unlocked or switched on during lunch-breaks, overnight or over the weekend, leave USB sticks with sensitive company information unattended or surf the internet from home while connected to their company's networks. A recent study in the British Medical Journal found that the majority of house doctors interviewed stored patient details on a UBS stick and shared this with other doctors during changes in their shift. To add to the risk of a data leakage, very few bothered to encrypt the data. In an emergency situation it is extremely easy to drop or leave the USB stick somewhere only to be picked up by a passerby; and there is no guarantee that this person will return the stick.

Social engineering is another method how data can be coaxed out of people. The 'attackers' do not need to be security experts but creative people who charm their way into people's lives and then use the knowledge they obtain (such as passwords or access codes) to steal important information. An IT administrator can control employee activity on the network, but there is little he can do to prevent employees from unwittingly giving out security information to outsiders.

The popularity and scale of growth of social networking sites is very worrying. Apart from the obvious loss in productivity because employees are wasting time seeing who has posted what to their profile, there is a great risk that work details could be shared and passed on to third parties, maliciously or otherwise. Companies often believe that all employees will follow all regulations and policies to the letter, they will comply with every request and willingly not make use of any device or visit any unauthorized sites. Wishful thinking!

Another issue to deal with is the volume of data that can be stored on portable devices. When floppy disks surfaced in the 1970s they could store a mere 320KB going up to 1.44MB by the early 1980s. But since then portable storage devices have so much capacity – up to 8GB on a USB stick and 80GB on an iPod – that it is extremely easy for individuals to store personal information, software products and games on a memory stick that can be very easily concealed. The ease with which data can be copied to and from a network has increased the risk of data disclosure incidents. It has also facilitated the upload of malicious code (e.g. a virus) that can expose networks to trojans or rootkits which, in turn, may hijack services and open ports that a hacker can then use to compromise the network.

Portable storage devices also expose networks to other vulnerabilities: employees can download unlicensed or objectionable third party data such as peer-to-peer software, games or pornography for which the corporation can become legally liable through vicarious liability. This not only raises legal issues but it compromises networks because it can disrupt business continuity.

And in spite of all this, companies are still not taking the necessary action to plug these vulnerabilities. The statistics and examples given above as well as new research that GFI Software is carrying out in the United States confirm this rather sorry state of affairs and provide the answer to 'why are security breaches and data loss on the increase?'

Companies are underestimating the threat. Unfortunately, even faced with such hard proof, many businesses still believe that 'it won't happen to me' and this could be a very costly way of brushing aside the argument. Moreover, IT administrators are so concerned with traditional security issues that endpoint problems are too far down the list to raise any concern or merit further study. Endpoint security has featured regularly in the media this year and because of this, in part, companies' have started to ask whether the problem is as bad as security experts are saying.

The facts speak for themselves: endpoint security is a real threat… and getting worse. Companies have two options: they can either do something about it or simply bury their head in the sand and face the music.

The repercussions

Companies hit by security breaches can expect to pay a hefty price and suffer on many fronts through eroded trust, brand, loss of business, and in some cases, civil and even criminal penalties. Privacy compliance standards and regulations – SOX, PCI DSS, CA 1386, HIPAA, Basel II, and PDPSA, for example – often present their own consequences in the form of penalties ranging from contract termination to fines to jail terms.

A study by Forrester Research among 28 companies that had some type of data breach found that the average breach can cost anything between $90 and $305 per lost record. Although every company puts a different value to its data, the loss of sensitive data can have a crippling impact on an organization's bottom line. To this direct cost you also have to factor in the indirect losses to individuals, institutions and society at large when business people, lawmakers, and ordinary citizens lose faith in the institutions entrusted with data. A survey conducted earlier this year among 14,000 UK law firms found that 6% had lost clients or suffered damaged relationships as a result of security breaches in the previous past 12 months. Data entrusted to a company is valuable property, and it is not surprising that the 'owners' of this data rapidly lose patience with any entity that treats these rights lightly, or gives the appearance of doing so.

Clients are the lifeblood of any professional services company and mitigating the risk of damage to company reputation should be the top priority of managing partners and senior executives.

Addressing the problem

Companies need to take pre-emptive security measures to prevent these things from happening through education and technology barriers which enforce company policy. They need to make better use of the tools that are available to them and their IT teams and to start looking at security as an investment instead of an overhead. In a good number of cases, companies need to revisit their approach to network security. The enforcement of the Payment Card Industry Data Security Standard (PCI DSS) has proved to be a wake up call for many companies that thought their networks were adequately protected. The low level of compliance achieved over the past two years has revealed that many businesses don't even follow security best practices. This, in part, also explains why security breaches and data leakage remain a major problem.

Achieving network security is all about managing risks and this is a continuous process that includes:

- A thorough and continuous assessment of where risks lie
- Putting up barriers to mitigate the risks
- Taking a proactive approach to security in general.

Malicious individuals will go to great lengths to gain malicious access to networks, using all forms of subversion and attacks. Companies have to make sure that all loopholes are covered, all systems are patched, all not utilized system accounts are disabled and last but not least, make sure that corporate insiders are aware of the threats and are trained to counter these threats.

Every company should have an effective corporate security policy set up and made known to all corporate insiders – and subsequently they do not rely on the goodwill of insiders to abide with this policy. More importantly, this policy should cover and enforce concepts that should already be in force on all corporate networks.

10 steps to protect networks against human vulnerabilities

1. Start at the top with senior management. When management understands and acts tough on security, then the battle is half won.
2. Implement a clearly defined, and not complicated, security policy. Back it up with clear communication.
3. Educate employees to be careful not to leave mobile devices running around. Make them understand what is at stake
4. Instruct all staff on the basics of computer security such as good practices for password use, etc. Education is key in securing your network.
5. Introduce non-standard security measures such as biometric scans for top security areas. It is usually cheaper than a data theft incident.
6. Restrict remote network access strictly to those who need it. This also applies to internet access through the company's gateway.
7. Track employees' use of their computer resources. Establish control over your corporate network.
8. Limit user changes to a computer's settings and installed applications. Limit browsing, instant messaging, use of peer-to-peer applications and file-sharing.
9. Restrict the use of portable storage devices. Use only solutions enable you to provide read/write access or block access to those who do not need to use these devices
10. Implement a strong password policy. Regularly change passwords/access codes to limit damage caused by leaks through social engineering.

10 steps to protect your network from technology vulnerabilities

1. Install vulnerability management software. This enables you to centralize control of your network's security.
2. Take control of compliance efforts. Do not depend on end-user compliance for your security needs.
3. Implement your company's security policy. Define the responsibilities of each user, administrator or manager.
4. Upgrade security. Test and implement the latest stable versions of the OS and applications on computers, switches, routers, firewalls and intrusion detection systems.
5. Patch systems. Keep the operating systems and the applications up-to-date by installing the latest security updates.
6. Know your network. Create and maintain a list of all hardware devices and installed software.
7. Customize your security. Use custom settings and passwords rather than relying on the defaults that come with out-of-the-box software applications.
8. Scan the network regularly. Shut down unnecessary servers and services and turn off functional areas which are seldom used but potentially have vulnerabilities.
9. Follow the principle of least privilege. Keep the number of administrative accounts to a minimum and use administrator credentials at little as possible.
10. Partition your network according to its security level and enforce strong permissions/rights on folders and data. This eases administration and allows stronger security policies.

Conclusion

Security breaches and data theft can occur at any time. It is not a matter of 'if', it's a matter of 'when'. No business can every claim to be 100% secure and so long as humans and technology work together there will always be room for errors, new vulnerabilities and security threats. However, there are effective ways and means to limit the chances that someone somewhere is waiting patiently to inflict serious harm on your network and steal your data. By looking at the bigger picture, companies can successfully protect their businesses from financial, legal and reputation damage. In an ever-growing networked environment where risk is becoming a major concern, you have to be ahead of threats and not passively reacting to incidents. Remember: a single breach could have irreversible repercussions.

Simon Reed is Vice President of Engineering at GFI Software (www.gfi.com).

Black Hat DC 2008
18 February-21 February 2008
http://blackhat.com

Black Hat Europe 2008
25 March-28 March 2008
http://blackhat.com

Kiwicon 2k7
17 November-18 November 2007
https://kiwicon.org

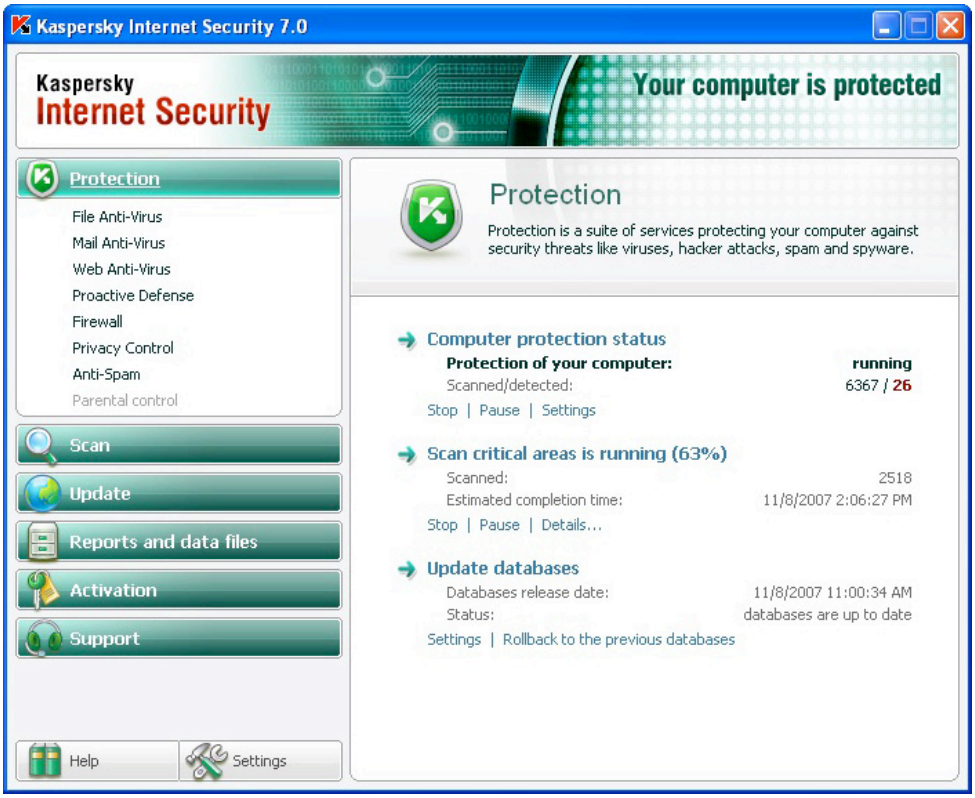
Net&System Security '07
27 November 2007
http://www.atsystemgroup.org/en/conventions/nss07

PacSec 2007
29 November-30 November 2007
http://pacsec.jp

24th Chaos Communication Congress 2007
27 December-30 December 2007
http://events.ccc.de/congress/2007

ARES 2008
4 March-7 March 2007
http://www.ares-conference.eu

Our computers used to be loaded with different computer virus protection products, personal firewalls, various adware and malware removers, anti spam tools - you name it. The only logical way was to combine all these functionalities into one product and that was the birth of Internet security bundles. This article covers the in-depth usage of one of them - Kaspersky Internet Security version 7.0.



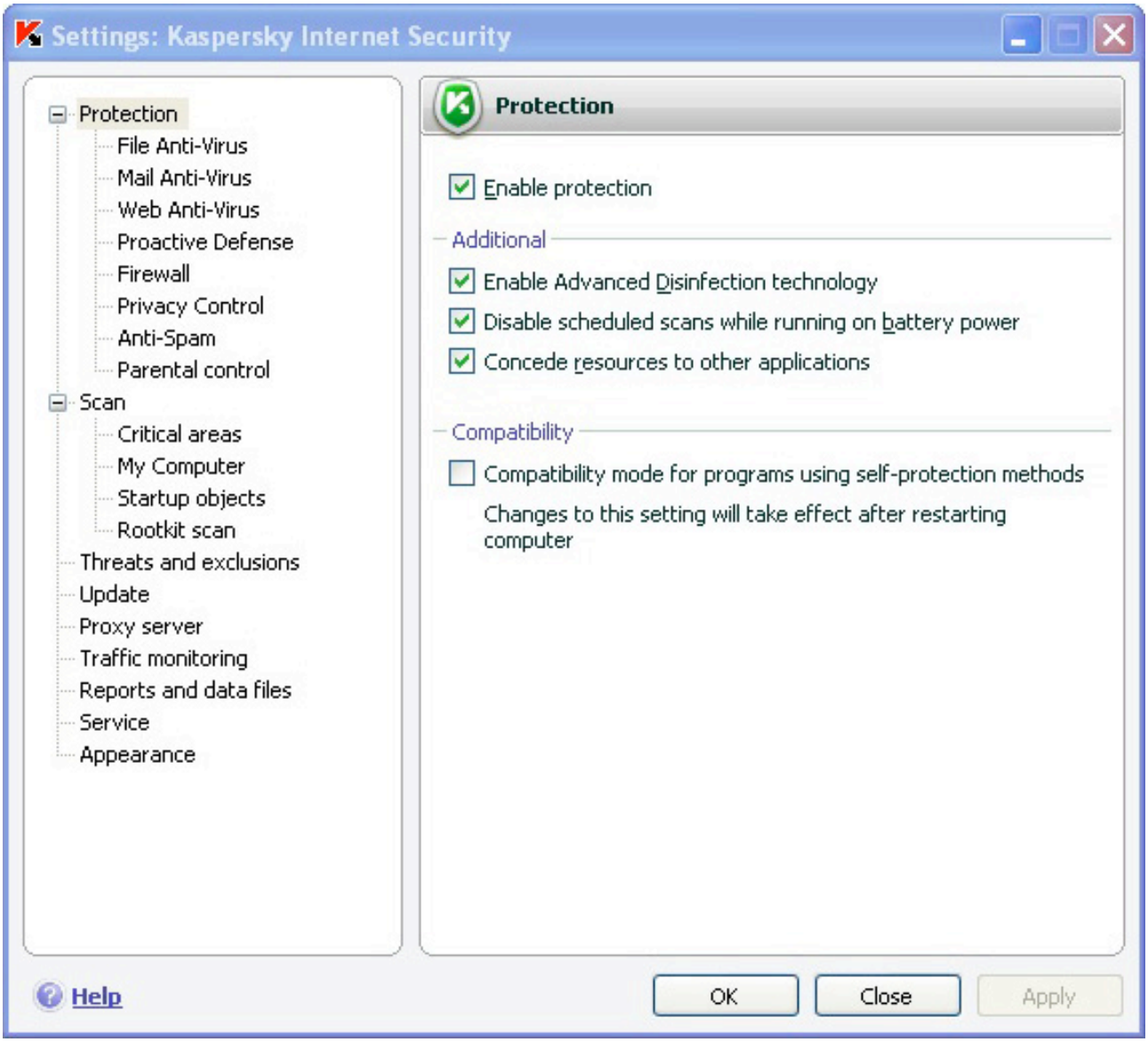
Kaspersky Internet Security user interface

Installation

The software installation is rather straightforward and hosts about five different steps of program customization. For starters, the usual difference in the express and custom installation types is the scope of the installed modules. As you bought the whole security bundle, I don't see why would you remove firewall or anti-virus from the installation, but this can be done. The software has one user interface and if you remove some modules, they will just be blocked out from the menu.

Kaspersky Internet Security 7.0 includes a self-defense mechanism for the anti-virus program. There is a number of malicious applications that attempt to block the anti-virus solution or even remove it from the computer. The self-defense mechanism blocks such attempts. You are given an option to enable this functionality before the program installation and I suggest you use it.

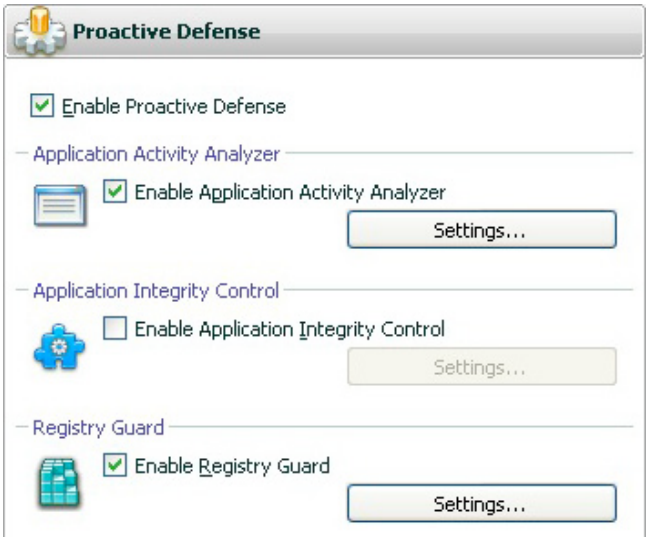
The next step is to setup the level of Interactive protection. The default option, suitable for most of the users, makes the software notify you of any dangerous activity. If you want a higher level of interaction, chose the Interactive mode where you can also give your saying on the activities the program finds suspicious. I will later cover some of the options that come with this level of protection - especially the training modes for the personal firewall, as well as the extended proactive defense. The last step focuses on an important function of updating the signatures database. The database can be refreshed automatically (I presume on an hourly basis), every 24 hours or manually. After the initial database update, you are ready to use the software in its full power.



The settings screen after the software setup

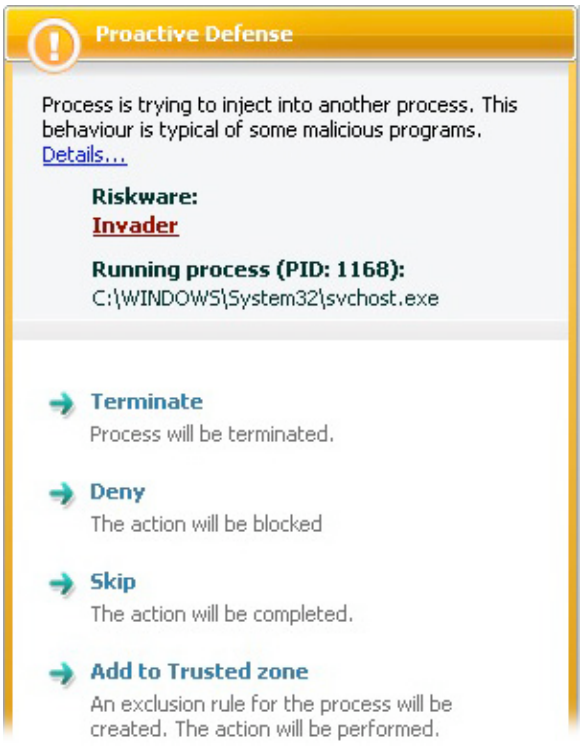
Proactive defense

The Proactive Defense module's interface deals with the application activity analysis and system registry monitoring. Dangerous activity is identified based on all of a program's activity rather than its individual actions. Kaspersky Internet Security 7.0 empowers a powerful heuristic analyzer that is a perfect addition to the usual virus scanning based on signatures. Sometimes the threats can attack your computer before the proper signatures are created and deployed, so heuristics come in to the play. To cut things short, the proactive defense analyzes active applications and, for instance, if their payload contains suspicious activities such as copying to network resources, adding its roots into registry and startup folder it flags the program as a potential threat.



Setting up parts of the Proactive Defense

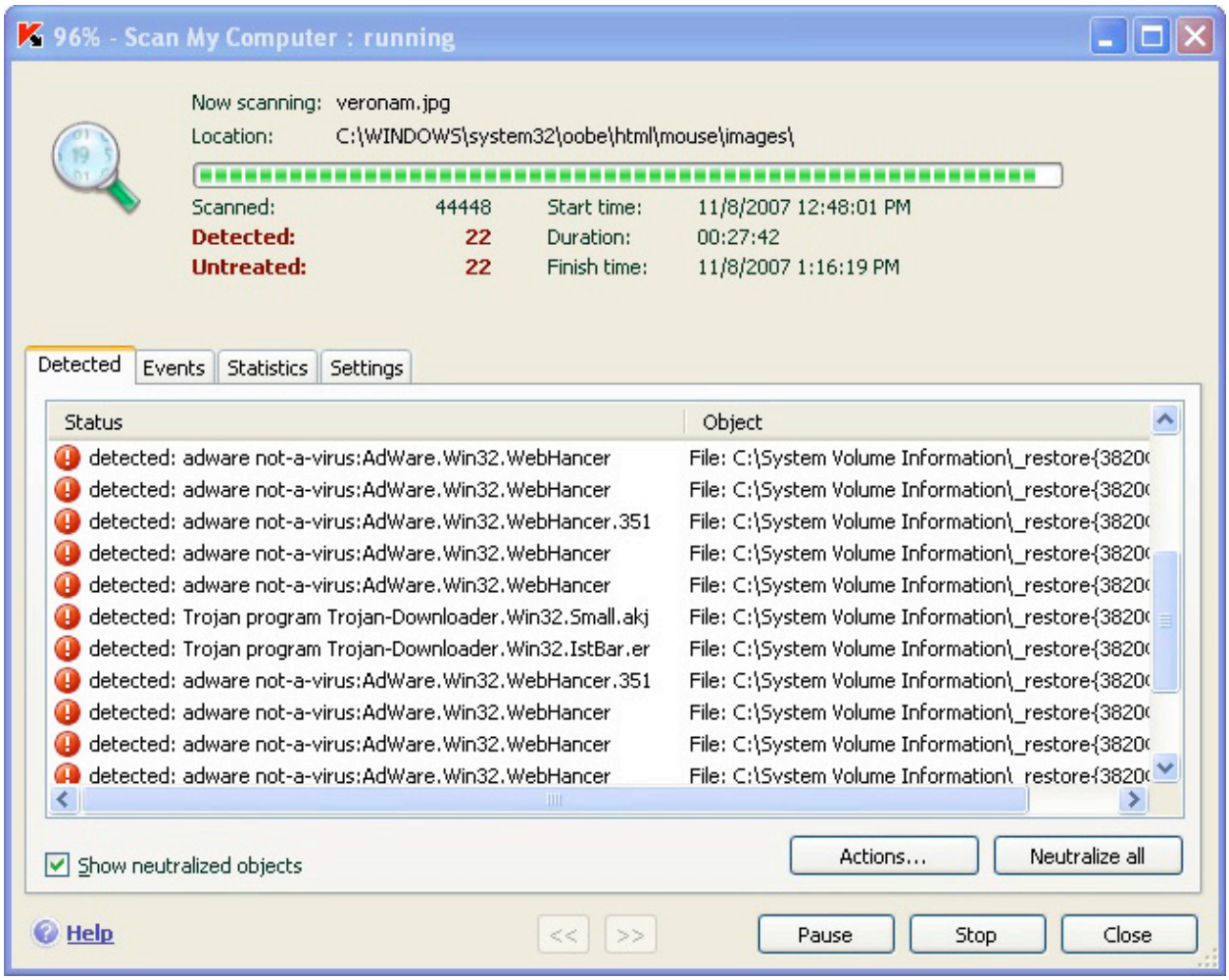
The good thing about this analyzer is that it uses a sandbox technique so Kaspersky software starts the application in an emulated environment which doesn't endanger the state of your computer security. After dangerous activity is detected on the system, the module can roll back any changes to the uninfected state.



Proactive defense alert window

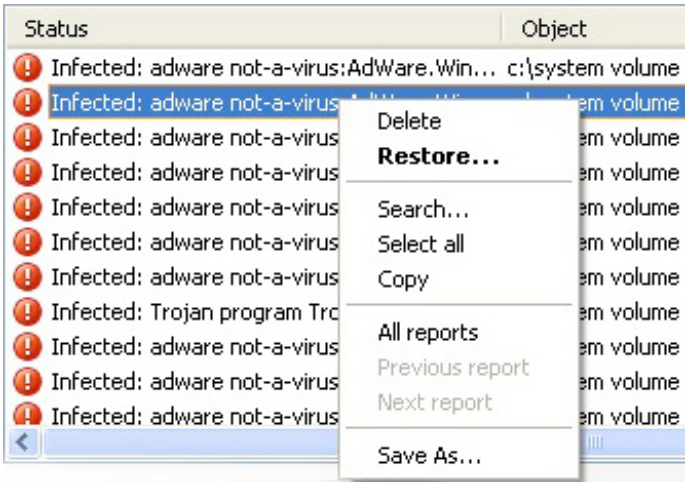
Local antivirus

Antivirus is the most typical component of personal computer security bundles, so there are not any ingenious new things I can mention. The scanning of my test computer with around 45,000 files took about 30 minutes.



Scanning for viruses on a local computer

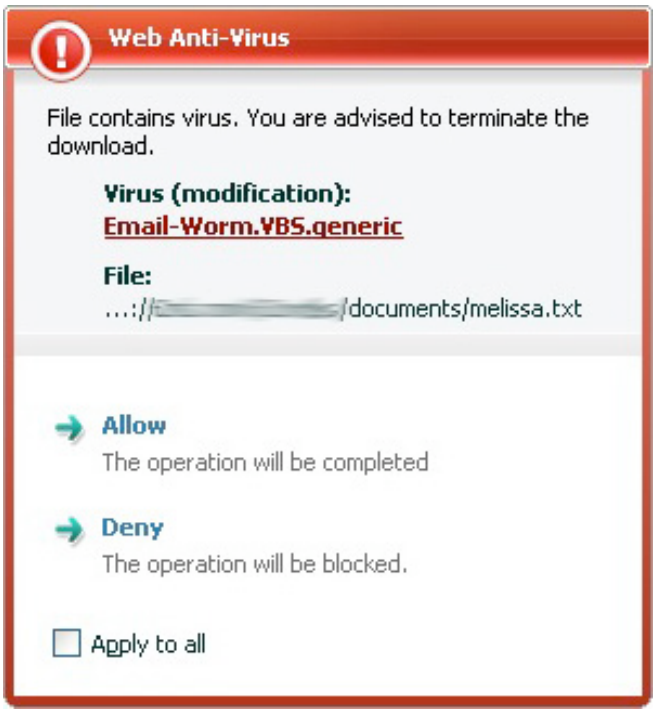
When malicious files are discovered the software will try to disinfect them. If this cannot be done, you can either move them to quarantine or delete them. All deleted files are also added to a local backup, so if in any case you want some of them restored, you can do it with a click of a mouse.



Quarantined infected files

Web antivirus

Majority of new threats are Internet-borne, so virus scanning interaction with browsing is a way to go. Kaspersky Internet Security integrates into your web browser (in my case Internet Explorer) and it sits there waiting for malicious files.

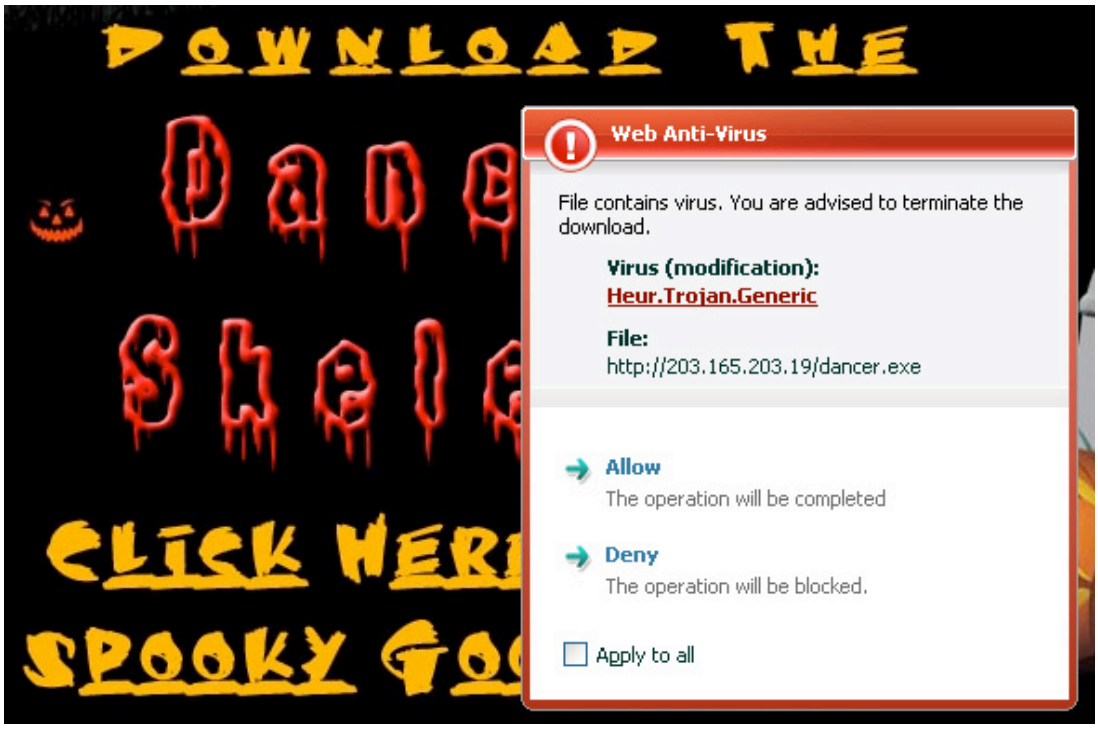


Alert saying the active download contains a VBS worm

If your browsing brings you to an infected web site - of course infected meaning that a malicious file is either available or pushed for download - the system will alert you with a pop-up accompanying a rather noisy squeaking sound.

Blocked access to the file containing Javascript malware

Besides the alert pop-up, the browser won't open the real file, but a changed HTML file giving you more details on the infected file.

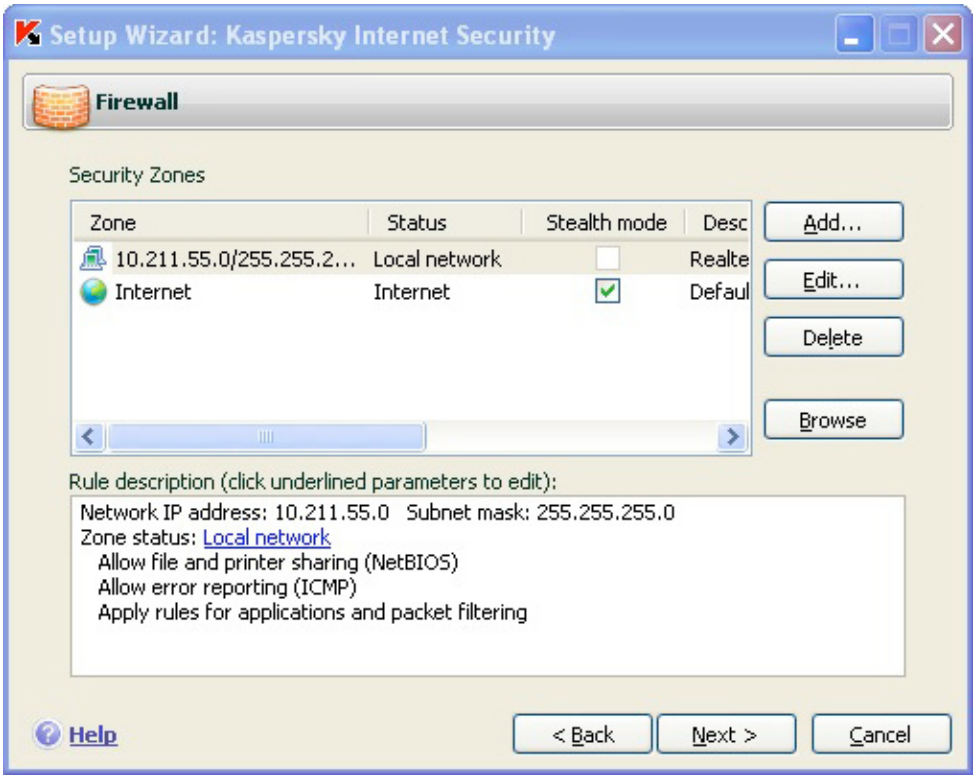


Trojan found in a Halloween dancing skeleton screensaver

Firewall

From my experience, looking from the home user or even SOHO point of view, firewalling the inbound connections is a thing from the past. Ten years ago personal firewalls were a valuable help from different type of attacks, but now days the biggest problem is to prevent things generating from your own computers. These problems include zombified distributed denial of service attacks, snooping software that reports to someone, as well as different type of malware that has its own secret agenda.

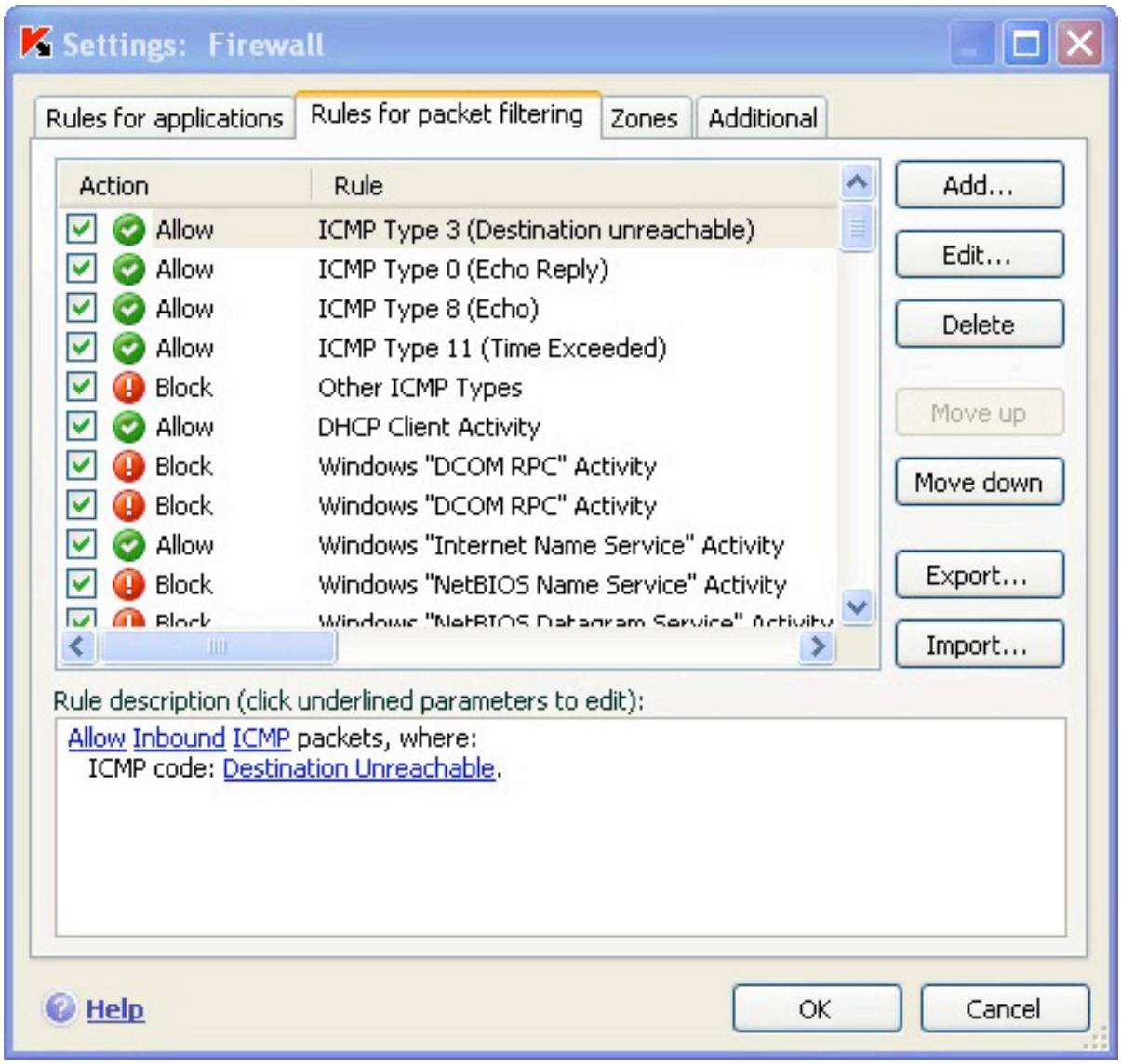
This module's functionality isn't of extreme importance, but when you combine it with different personal security modules, it provides an integrated solution that is a must have for home/SOHO users.



Security zones related to network connections

When configuring the built in firewall, the software automatically detects your network settings and sets up different security zones for the local network, as well as the Internet.

The basic configuration contains a specific set of packet filtering rules, that provide to be optimal for the average computer user. More experienced users can edit the predefined ruleset, as well as add new rules. From the application point of view, the software detects all running applications and creates a rule for them.

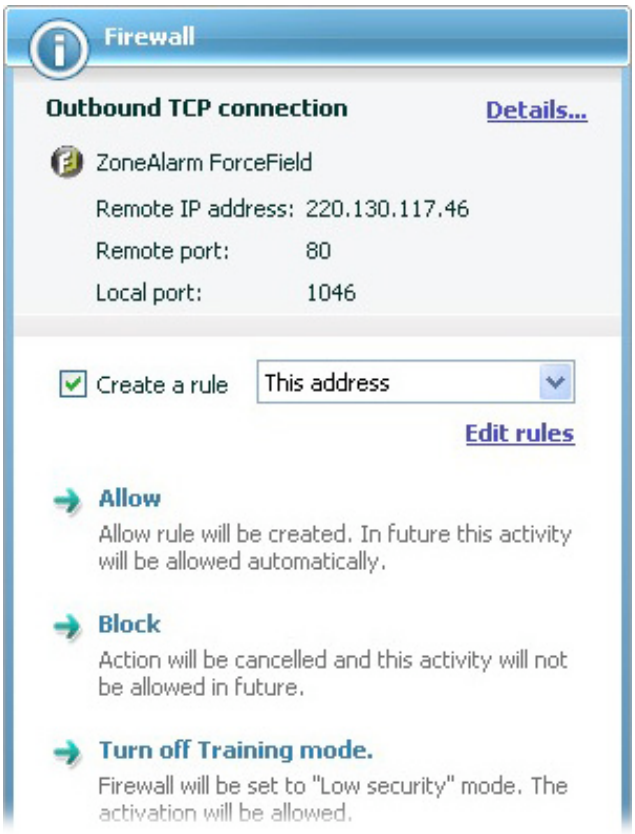


Setting up applications and packet filtering rules

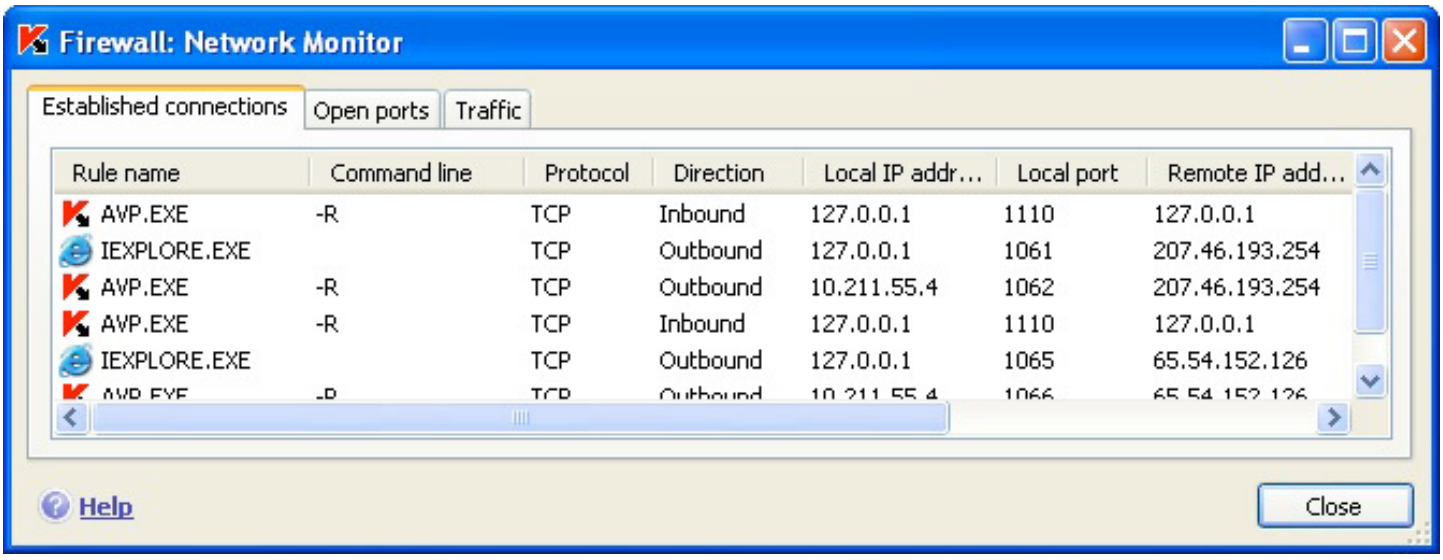
Kaspersky Internet Security has an adaptive firewall that will ask you a number of things when you actually start using your computer. Every software you manually open, or it is opened in the background will cause a pop-up alert where you can either allow or deny the connection.

The best thing is to dedicate 10 minutes of your time and start all the applications you regularly use. On this way the ruleset will be created specifically by your demand and in the future it will be easier to detect new threats generating around your computer.

If you are not to keen in using command prompt for checking the status of your active connections, the software offers a Network monitor that will provide real time information on them. Besides this, with a click on a system tray icon, you can block all the network connections going from or coming to your computer.



User can act on every outbound TCP connection

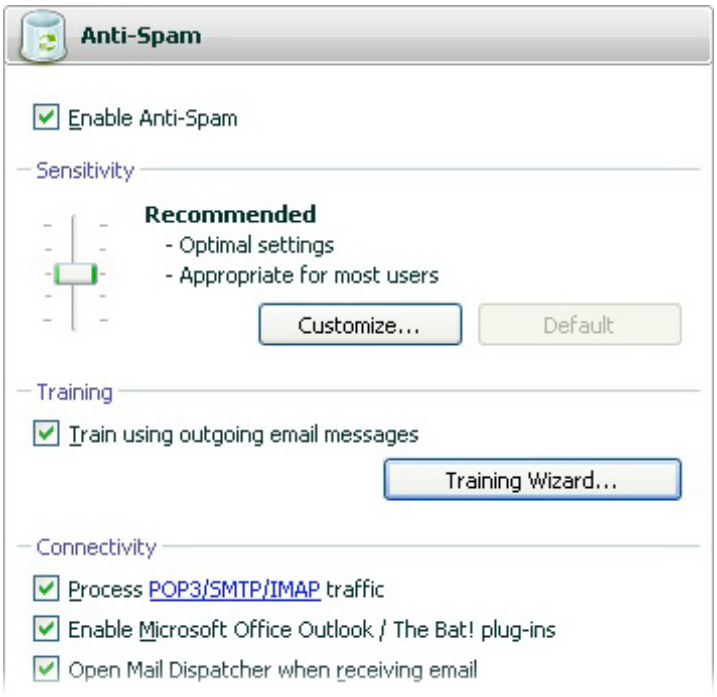


Kaspersky Net monitor showing the active connections

Anti spam

Spam is one of the key annoyances of the every day Internet use, so no security combo product of this kind shouldn't come without dedicated anti spam protection. This module works with a couple of popular Windows based mail solutions including Microsoft Office Outlook, Microsoft Outlook Express and The Bat!. Besides the plugins for the mentioned products, Kaspersky Internet Security can intercept and process all POP3/IMAP/SMTP traffic and therefore take care of unwanted e-mail. The technique used is based on Bayesian algorithms and works quite efficient.

One of the things I often find useful with anti spam products is the training mode, which is nicely incorporated into this product. You can manually chose a folder location of your e-mail (if you are Outlook/The Bat user) and the software will process all e-mails and start an interactive procedure where its "artificial intelligence" is pumped with details about the spam status of your received e-mails.



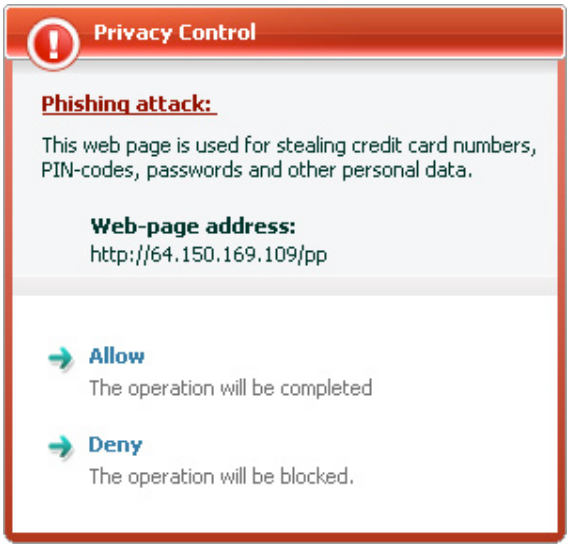
Anti spam module configuration zone

Spam filters can be configured as according to a couple of security levels provided with the software by default. Besides the usual Allow all and Block all options that work with your predefined whitelist, you can select High and Low levels which are sure to generate either too many false positives, or let the spam to enter your inbox. Recommended option is the one set up by default, as it proved to be most efficient.

If in any case you have some time on your hand, you can always use built-in Mail Dispatcher which gives your the possibility of manually checking the mail headers on your remote POP3 accounts. With the level of e-mail (both valid and spam) people are getting, this doesn't seem like an option someone would use, but nevertheless it is here.

Anti phishing

Kaspersky' security suite features a privacy control center that features anti dialer, anti phishing and confidential data protection. In the past, dialers proved to be a quite big problem for the average dial-up Internet user. As majority of us doesn't use dial-ups any more and we don't have (at least in the wild) dialers that use our computer's VoIP services I didn't play with this option at all. I was more interested in mangling the phishing threats by using the inbuilt protector.



Blocked phishing URL

The software hosts a database with fake URLs commonly found in phishing links. Therefor when a user mistakenly opens a fake PayPal or bank web site, the software will automatically pop-up an alert window saying that a phishing site was accessed. Besides the list, the program can also detect some common phishing "signatures".

I tested more than 20 different phishing web sites and the product detected just half of them. Phishing sites don't have a long "time to live", so I was testing the sites detected by another security company in real time. Most probably the detection rate was connected with the constant evolution of phishing sites, but I had better expectations from this module.

I should also note that the anti spam function of Kaspersky Internet Security also uses the same phishing database to automatically intercept phishing e-mails.

Inspecting encrypted transfer on the phishing site

Conclusion

Kaspersky Internet Security 7.0 proves to be a robust security applications with a line of quality modules that complement each other perfectly. By using this application, you can really make sure that your computer has a full force defence system against a variety of harmful security attacks and online annoyances such as spam and phishing.

Mark Woodstone is a security consultant that works for a large Internet Presence Provider (IPP) that serves about 4000 clients from 30 countries worldwide.

Interview with Amol Sarwate, Manager, Vulnerability Research Lab, Qualys Inc.

By Mirko Zorz

Amol Sarwate heads Qualys' team of security researchers and engineers who manage vulnerability research. His team tracks emerging threats and develop new vulnerability signatures for Qualys' vulnerability management service.

Amol is a veteran of the security industry and has devoted his career to protecting, securing and educating the community from security threats. He presented his research at numerous security conferences, including RSA 2007, InfoSec Europe 2007 Press Conference, Homeland security Network HSNI 2006 and FS/ISAC 2006. He regularly contributes to the SANS Top 20 expert consensus identifying the most critical security vulnerabilities.

What do you see as the biggest online security threats today?

For the past year or so we've observed a trend of increased client-side attacks that make use of social engineering techniques to compromise victim computers. Malformed images, videos, and music files land-up on corporate desktops that can then take complete control of unsuspecting users.

Social engineering techniques such as phishing are the preferred attack method which can lead to viruses, Trojans, spyware and other type of malware.

Web application vulnerabilities also pose a big risk as they can lead to consequences ranging from identity theft to fraudulent credit-card charges. These are all very big threats with potent consequences.

What do you see your clients most worried about?

I can't point to a single concern among clients, but issues that are often raised are in the areas of perimeter security, patch management, asset management and complying with PCI and other compliance frameworks like SOX and HIPAA.

Many larger organizations that acquire or grow operations rapidly in different parts of the world have trouble managing their assets, meeting the various requirements, as well as enforcing security standards without breaking their established business model.

What do you think about the full disclosure of vulnerabilities?

I fully support responsible disclosure of security issues. I do not believe in putting customers at risk by releasing a PoC (proof-of-concept) or publishing exploit code that has detailed instructions on compromising a vulnerable product – especially when this is done before a patch or a workaround is made available. I believe that the person who discovers a vulnerability should get full credit for his/her hard work. This can all be accomplished very easily via responsible disclosure.

In your opinion, what is the biggest challenge in protecting sensitive information at the enterprise level?

I believe that enforcing enterprise wide security policies is the number one challenge in protecting sensitive data. Part of the difficulty is due to large enterprises having diverse technologies and being scattered in different countries. This often happens when enterprises merge or buy other companies.

How do you see the current security threats your products guard against evolving in 3-5 years?

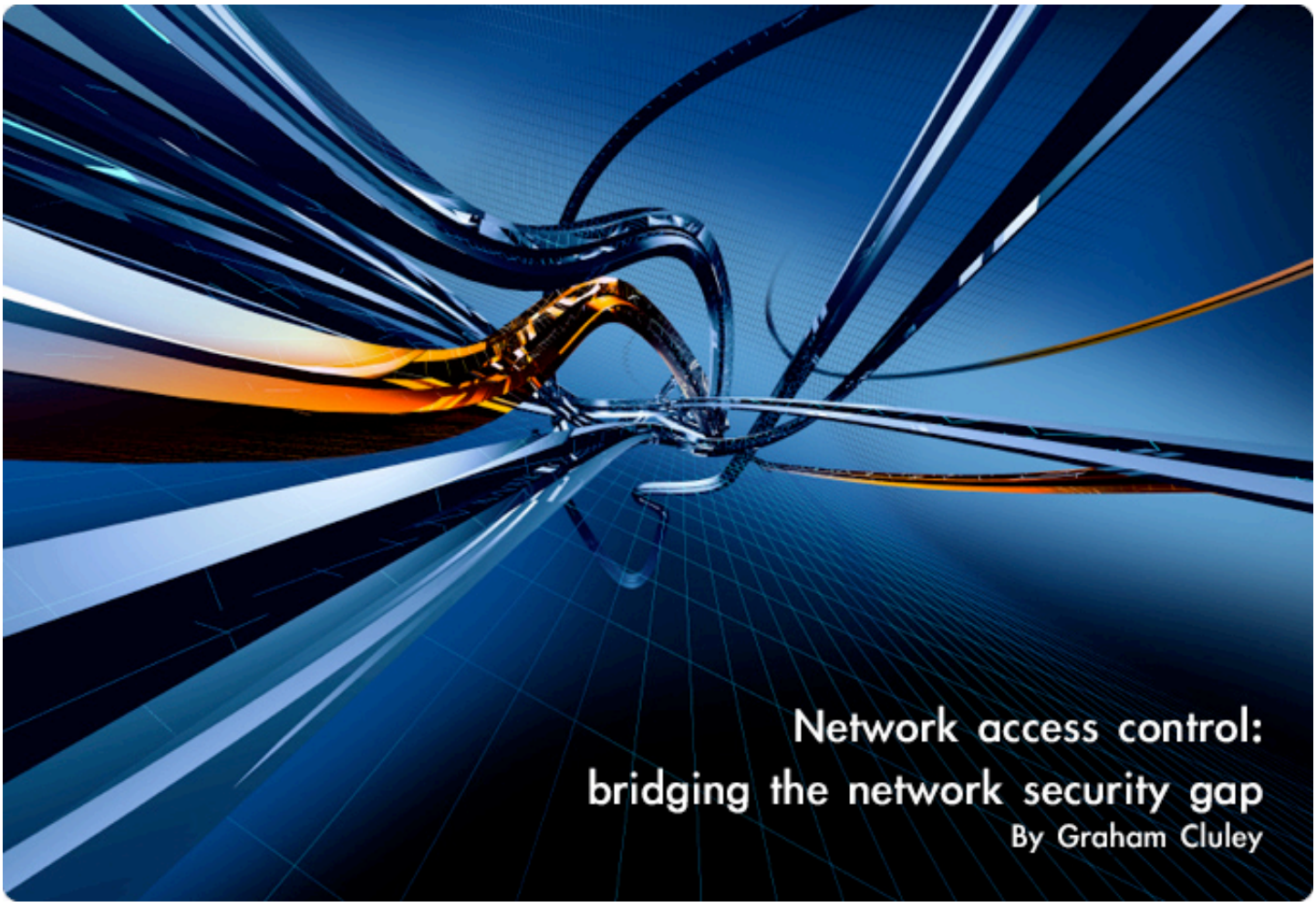
Currently Qualys' vulnerability management solutions can detect all remote and local vulnerabilities. Additionally, we have limited support for web application scanning. In the future, with advancements in newer protocols and applications we expect these types of threats to become more sophisticated. Therefore, new web application threats are almost guaranteed to come and Qualys is developing a comprehensive web application scanner that would scan remotely and optionally with web authentication.

In the future we will see vulnerabilities in the implementation of newer protocols like IPv6 as well as older, less targeted protocols like SIP. Control protocols like SCADA will also be targeted.

What are the future plans to extend your product offerings and capabilities?

To help customers comply with security frameworks like SOX, HIPAA, GLBA or internal policies, Qualys is developing a compliance platform that will leverage our existing scanning infrastructure to run compliance scans.

We're developing the next release of our PCI offering that will enable partners and customers to create their own certification program to audit vendors or external parties. As mentioned previously, we're also developing a specialized web application scanner for helping customers to identify and fix related threats.



The business work place has evolved significantly over the last ten years. Back then, networks were far more simplistic; the internet was not a critical business tool, there was far less legislation, and there were no applications for employees to launch in the workplace, except for a sly game of Solitaire. Now, a company's IT network is its central hub, an increasingly complex environment that offers dramatically enhanced efficiency, but also brings with it a convoluted set of problems for increasingly over-stretched IT departments.

Modern technologies have opened a Pandora's box of issues for companies trying to keep control of their networks. It is not unusual for a typical employee to launch instant messaging, log onto Facebook and start sharing videos with friends and colleagues. Not only might members of staff log on to the network from their desks, they might also log on from home, or from their laptop at a WiFi hotspot in a coffee shop or at the airport.

While the ubiquity of the new internet is predominantly positive for businesses, boosting employee up-time and therefore productivity, it has opened up a can of worms in terms of security, and adhering to an ever-escalating number of compliance regulations is becoming an increasingly difficult challenge for organizations. By their ability to puncture holes in corporate defenses, these new technologies are like candy to a baby for cybercriminals, who are exploiting these vulnerabilities to infect networks with malware, spyware and Trojan horses for their financial gain.

Organizations' ongoing drive for more flexible working practices also has a major impact on the overall security of corporate networks. Now, networks need to be opened up to third parties, such as contractors, customers and consultants, but these guests may not use the same security applications as the host network and may not have applied the most recent software upgrades or patches. Moreover, full-time employees are frequently granted administration rights that enable them to use their computers from outside the office, but this can compromise security, as it requires

that some critical security services are disabled.

Despite the risks involved in not keeping a tight rein on the comings and goings of network users, a surprising number of organizations have no enforcement mechanism in place to drive compliance or to report on results. This gap in corporate policy exposes the enterprise to a range of threats; not simply from malware and hack attacks, but also the loss or theft of intellectual property, and punishment from inadvertently flouting regulatory requirements.

Some forward thinking businesses are however cottoning on to the risks and have therefore begun to implement security policies which try to control employee use of corporate resources and the internet whilst at work. While such frameworks can go some way towards ensuring that employees toe the line, they can be difficult to implement and enforce.

Furthermore, policies alone do not present a watertight solution and they cannot stop all security breaches that are outside user control.

Policies alone do not present a watertight solution and they cannot stop all security breaches that are outside user control.

What are security companies doing to support customers?

The complexity of managing modern security applications, combined with a lack of control over employee and visitor computers attaching to the network, has driven many security vendors to incorporate compliance and enforcement capabilities as extensions to existing products. Indeed, some vendors have gone as far as to shift their position from promoting single endpoint security products to creating and endorsing entire suite of endpoint security solutions to give IT departments back the control they need to quash the growing threats to their networks. It has become starkly apparent that companies need support in managing all the various users and endpoints accessing their networks to ensure that security and compliance breaches do not take place.

Network Access Control (NAC) - helping companies to take control back

Organizations of all sizes are now considering NAC as part of a holistic security strategy. NAC not only gives businesses the power to simply and swiftly create and enforce security policies, it can also block or quarantine non-compliant or unauthorized computers that are seeking to gain network access. An effective solution can also determine whether all endpoints are compliant with the organization's security policies; not only prior to granting permission to access the network, but on an on-going basis once these users have been allowed to log on. In this way, companies can rest assured that if a user acts out of line with the security policy, they will be banned from the network until the matter has been dealt with. Furthermore, systems administrators can grant individual employees or guests specific levels of network access, which dictate which resources they can use. These levels are set by looking at a combination of factors, including the user's department, internal role and their level within the company, as well as the status of their endpoint's security solutions.

Replicating physical security measures online

The need to secure sensitive data on business networks, and the NAC method of achieving this, can be compared to the constraints many businesses put in place to ensure the physical security of their buildings. Let's take the example of a pharmaceutical company, which needs high levels of security in order to protect drugs patents worth billions of pounds, and to ensure compliance with strict legislative standards. In this kind of environment, a receptionist would meet all employees and visitors at the front desk. Once their reason for wanting to move forward has been established and the receptionist has accepted that it is in line with the company's security policies, they will then be either authorized or refused entry.

Those employees and visitors that have been approved, will be granted further access to specific areas of the building, depending on their requirements and position within the company. For example, while the managing director may have 'access all areas' clearance, a temp may only be able to access the parts of the office that they will directly be working in. By giving physical access to the right people in this way, the company has dramatically reduced the associated security risks. You would not let a masked man through business doors, but it's a bit more complicated to prevent them gaining access to the business network - without the right solution in place.

The risk of intelligent users

A common trap that many businesses fall into is only considering to implement NAC if they have remote and mobile workers and frequent visitors, but while these casual users certainly pose a significant threat to company networks, it is equally critical to protect their infrastructures from users within the corporate walls. Indeed, in a recent Sophos poll, which asked more than 200 companies who they thought exposed their networks to the greatest IT threats, 44 percent believe standard employees to be the most dangerous. Now that technology is so integral to so many people's lives, there are a growing number of expert users who have a potentially dangerous level of IT knowledge, enabling them to evade enforcement when accessing network resources, even if there is only the narrowest of gaps to slip through. Such a gap may arise from a number of scenarios, including the use of DHCP networks - enabling a device to have a different IP address every time it connects to the network - or where the rogue computer is using local, statically assigned IP addresses for network access.

Problems may also occur if a quarantine agent is not installed on the user's computer. Whilst many of these employees will simply be trying to play the system without malicious intent, they still pose a threat to networks because they are opening holes, giving cybercriminals a backdoor entrance into company infrastructures. This is one example of why companies should not rush headlong into purchasing the first NAC solution they find; unfortunately solutions do vary, and it is crucial to find the best system for the job.

Making NAC work for your company

There are a number of different ways to implement NAC; solutions can be hardware or software based, standalone or integrated into the internal network infrastructure. How do businesses decide what is right for them?

The appropriate solution for an organization is primarily dependent on its current network environment and it is therefore crucial to assess this fully before taking the plunge. Critical factors include, how homogenous the network is, what the main network access methods are, and of course, the budget available. For example, for small to mid-sized businesses, the most effective NAC solution is one that can assess the security level regardless of the specific solution in place as well as work seamlessly within existing IT infrastructures. When making their choices, enterprises should focus expenditure on the solutions and services that solve their biggest problems, choosing solutions that protect against vulnerabilities and provide a full security process instead of merely providing products. As a rule, the best option for organizations looking to introduce NAC to their security suite, is to find a solution that works with the existing network infrastructure and user management systems - and one that is truly vendor neutral. This will be least disruptive to implement and will produce the best return on investment.

It is also imperative that a NAC solution provides comprehensive support for the organization's security strategies, as well as having the ability to create and manage new policies in the future. It should also be flexible enough to meet new business strategies as they inevitably arise. A final critical factor is that the solution offers capabilities beyond standard network-based enforcement, identifying and providing protection against all classes of users trying to gain access to the network - both known and unknown.

The complete NAC solution

An all-encompassing NAC solution will alert network administrators of MAC and IP addresses, enabling them to take immediate

action when an unauthorized endpoint computer connects to the network. Its reporting capabilities should extend to include multiple reports for rogue endpoints, exempt computers and any new information that may prove critical - as events occur, in real time. The alerts should identify the rogue computer with pinpoint precision so that network administrators can simply and swiftly identify its network location and subsequently take the appropriate actions.

It is crucial that this constant monitoring does not interfere with normal network communications; for this reason, passive monitoring will provide the best results. The monitoring of low-level ARP (Address Resolution Protocol) a network layer protocol used to convert an IP address into a physical address, allows all IP communications to be detected, without exception. This means that even if a canny user evades DHCP network-based enforcement, their computer will not be able to communicate and spread infections throughout the network because ARP has to be used in order to slip through. By monitoring ARP, identifying which computers are attempting to make IP connections, and comparing the computer with the list of approved, compliant, and registered computers, systems administrators have a watertight way of spotting a rogue computer making advances on the network, enabling them to act fast and effectively.

This solution, while providing comprehensive reporting on users attempting to access the network, and the actions of those already logged on to the systems, should make systems administrators' lives easier, and that means that reporting should be simply decipherable and easy to action.

Maximizing flexibility and control for systems administrators

Implementing NAC solutions is all about giving companies control back over their networks. It is therefore crucial that the chosen solution gives systems administrators the optimum degree of flexibility and control. Because user groups in organizations are closely interwoven with the associated policies, determining which users are assessed for compliance against which policies, is a crucial step in reining in control. Groups can be defined according to department, function, individual hire dates, or a combination of these factors.

The best NAC solutions allow multiple policies to be created for various user groups, and for these to be shared between groups as necessary.

The crux of a truly flexible solution is ensuring that these policy-to-group relationships can be changed at the drop of a hat - including the addition of new users to existing groups - in line with the very real requirements of a constantly evolving workforce. This is particularly critical if administrators want to mandate specific security applications for new users. This degree of control is essential when mergers and acquisitions take place for example, when companies face the daunting task of imposing their corporate security policies on large numbers of new users.

Without an effective NAC solution in place, successful migration for new employees can be a logistical nightmare.

Conclusion

Controlling employee and visitor access to increasingly complicated business networks should not be seen as an expendable add-on to security suites, but as an integral part of ensuring compliance in an ever-more regulatory world, and fending off cyber attack in an ever-more dangerous network environment.

By implementing a flexible and comprehensive NAC solution, organizations are able to effectively combat today's threats, while being fully equipped to mitigate against tomorrow's.

Graham Cluley is one of the world's leading experts in IT security and control, and works as senior technology consultant and head of corporate communications at Sophos. He has given talks around the world at events such as EICAR, ICSA, Virus Bulletin and the European Internet Security Forum on the virus threat.

F-Secure Antivirus Research Weblog (www.f-secure.com/weblog/)

When you think about a company blog, you may expect boring marketing material. F-Secure decided to go the other route and offer visitors up-to-date malware information with informative videos, trend analysis and predictions.

Windows Incident Response (windowsir.blogspot.com)

The author of "Windows Forensics and Incident Recovery" writes about incident response and forensics on Windows systems and covers a very technical topic that will certainly find its audience.

SecuriTeam (blogs.securiteam.com)

SecuriTeam focuses on a variety of security-related issues and offers insight into current news and vulnerability research.

A Day in the Life of an Information Security Investigator
(blogs.ittoolbox.com/security/investigator)

An anonymous security professional writes about everything related to his field. The blog is rich with real-world examples and answers to diverse reader questions.

Change and configuration solutions aid PCI auditors

By Matt Clark

To the casual observer of the Payment Card Industry (PCI) standard, it might seem that the standard deals exclusively with the servers and point-of-sale terminals that house cardholder data. This is an understandable assumption, given the origin and subject matter of the PCI requirements. However, a careful read of the PCI Data Security Standards (DSS) reveals that almost half of the specifications are aimed at the network infrastructure that transmits the cardholder data.

Managers responsible for IT compliance need to understand that credit card companies hold merchants accountable for not only protecting stored consumer data, but also securing the network transport layer and on-going processes to validate compliance. Due to the never-ending amount of network device change and configurations, it is nearly impossible to determine exactly when a device actually becomes non-complaint. PCI auditors are not only on the lookout for non-compliant devices, but also for a well thought-out security process that is currently implemented, tracked and well documented. This is where an automated change and configuration management system can really assist.

The PCI DSS requirements pertain not just to retailers, but to any credit card accepting organization from university book stores to pay-at-the-pump gas stations. Let's face it, retail payment systems were not designed with security in mind, they were designed to add convenience to consumers' shopping experiences. However, hackers have caught on to this oversight and are finding new ways to exploit the weakest network links for their profitability — and they are getting really good at it.

Consider several well-published network data breaches over the last few years:

- February 15, 2005 - ChoicePoint - ID thieves accessed 145,000 accounts.
- April 12, 2005 - LexisNexis - 280,000 passwords compromised.
- November 2006 - UCLA – 800,000 current and former student Social Security Numbers stolen by computer hacker.
- July 2005 through January 2007 – TJX – 45.7 million credit and debit card numbers stolen.
- July 3, 2007 Fidelity National Information Services (Jacksonville, FL) 8.5 Million Records lost due to data breach.

To illustrate the depth of this situation, Privacy Rights Clearinghouse has chronicled data security breaches since January 10, 2005, and has estimated that 167,493,672 records containing personal data have been stolen.

Further underscoring the gravity of the situation, notice the amount of records stolen is rapidly increasing every year. Not only does this equate to bad publicity, but it also lends itself to increasing consumer costs. Hence, the quagmire merchants find themselves in: Do I assume status quo will repel hackers – and PCI auditors or, do I make an investment to help ensure a secure network? In the end, protecting consumer data is less costly than dealing with a security breach and precisely why the PCI Council was formed.

The PCI DSS specifies security requirements across many domains, from documentation and physical security to network encryption and software design, all designed to ensure the safe storage, transmission, and use of sensitive cardholder information.

As defined by the PCI Data Security Standard V1.1, "*These security requirements apply to all 'system components.' System components are defined as any network component, server, or application that is included in or connected to the cardholder data environment. The cardholder data environment is that part of the network that processes cardholder data or sensitive authentication data.*"

THE PCI DSS SPECIFIES SECURITY REQUIREMENTS ACROSS MANY DOMAINS.

This definition has indeed caused some heartburn among merchants, as they refer to these standards as too broad in scope — or too narrow in some instances — to actually comply with. In essence, there are 12 requirements and approximately 178 sub requirements to deal with.

Furthermore, organizations are required by credit card companies to comply with all these security requirements or face stiff penalties. Case-in-point: Under the new penalties issued by VISA last year, acquirers will be fined between $5,000 and $25,000 a month for each Level 1 or Level 2 merchant that is not validated PCI compliant by September 30, 2007, and December. 31, 2007, respectively.

However to add a twist, there is also an interesting caveat to the all-or-nothing approach PCI mandate, found in Appendix B of the PCI Data Security Standard v1.1 requirements called Compensating Controls. According to PCI Security Council's Glossary, "*Compensating controls may be considered when an entity cannot meet a requirement as explicitly stated, due to legitimate technical or documented business constraints, but has sufficiently mitigated the risk associated with the requirement [3.4] through implementation of other controls.*"

Requirement 3.4 deals with the Primary Account Number (PAN), or the payment card number that identifies the issuer and the particular cardholder account. The compensating controls may consist of either a device or combination of devices, applications and controls that meet all of the following conditions:

1. Provide additional segmentation
2. Provide ability to restrict access to cardholder data based on:
    a. IP/MAC Address
    b. Application Service
    c. User Accounts/Groups
    d. Data Type
3. Restrict logical access to the database
4. Prevent/detect common application or database attacks.

Given all the routine daily tasks that must be performed by the IT personnel, no wonder it's a seemingly impossible task to interrupt and implement PCI DSS. It stands to reason why VISA recently reported that only 40% of Level 1 and one-third of Level 2 merchants have validated PCI compliance.

With so much riding on PCI compliance, network managers are increasingly turning to software to automate specific steps in the compliance process.

Automation, if done correctly, helps facilitate the planning, management, review and documentation processes as well as assist with creation, implementation and enforcement of a PCI compliant security policy across the entire network infrastructure.

Network change and control helps demonstrate PCI DSS requirements

The PCI Security Council recognizes that network security is not a destination but a process, and that the ability to reliably control the security of the network is dependent upon the establishment of solid change control processes. Network change policies should be clearly documented, easily accessible to users responsible for daily management of the network, and regularly reviewed and approved by management.

Change processes should include validity checks and management approval for all outgoing changes, and change verification and compliance checks after a change has been made. It's not enough for an auditor to see that a device has been configured correctly, or even that a set of written procedures exists. To verify that an appropriate change control process is in place, the auditor will want to see evidence that the documented process has been followed on a daily basis.

Beyond describing the change control processes that must be in place, PCI also requires the existence of specific network device configurations such as access-lists and strong encryption. Border routers and firewalls should be configured with explicit access-lists allowing communication only across standard ports which serve a valid business purpose.

Network managers must employ regular password rotation and ensure that no device is ever deployed on the network with vendor-supplied default passwords in place. Any network path that facilitates the transmission of cardholder information must be secured with strong encryption or start to face those aforementioned $5,000 to $25,000 fines.
With 12 chapters and more than 170 individual requirements, planning for compliance with the DSS requirements is a challenge. Automating the change control and configuration process eases the burden of the network manager by providing a structured approach to implementation of the DSS. It should offer advice and best practices documentation in the context of the individual DSS requirements, making it easy for managers to determine which steps need to be taken to ensure compliance with the standard.

Change control processes should be documented and stored so that engineers and managers can access the process documentation on a daily basis. An automated, change control solution can facilitate this, providing the network manager with the ability to include the company's established policies alongside the individual PCI requirements and vendor best practice documentation.

For example, qualified personal should have the means to easily access the current – not static – status, and supporting documentation, of PCI DSS requirements in one consolidated view. This view should contain:

- PCI DSS Requirement Definition
    - o 2.1 - Always change vendor supply defaults before installing a system on the network.
- Reports and Links
    - o Credential and Usage Reports
    - o Communication Mechanism Reports
- Each Compliance Item and Status:
    - o Default Password
        - Cisco Routers
            - 3,772 compliant
            - 43 non compliant
- Review Comments
    - o 05/30/07 – Matt Clark, Updated default passwords policy to include PWs from latest IOS.

With easy access to this content, network engineers looking for direction or confirmation will find it easy to access and review the documentation, ensuring higher adherence to the established processes. Network engineers will be more likely to follow the process when it is widely published than if it is stored in a binder on the shelf of the compliance manager. Auditors will request network managers to demonstrate how the processes are distributed to engineers, and the central repository in the PCI compliance solution will meet the requirement.

One of the largest cost savings provided by having a PCI solution based on automated change and compliance control is the assistance in reducing the scope of the audit. Qualified security assessors (QSAs) are required to set the scope of the audit to the devices that protect, hold, or transmit cardholder data. While it's incumbent upon network engineers to design the network so that it is properly segmented, a PCI solution can assist in proving this segmentation to the auditor.

The solution should provide logical containers to manage each network domain, and change and compliance reporting should highlight the association between the PCI-compliant processes and the in-scope devices to the auditor. In order to keep up with the changing demands of the business, enterprise networks can absorb multiple changes per day. Engineers were once able to accomplish change management with a battery of scripts and FTP servers, but with today's heterogeneous networks and heavier audit requirements, this method does not scale to meet current challenges. Full change and compliance control cannot be achieved without a high degree of automation, which is perhaps the largest benefit of a PCI compliance solution.

ONE OF THE LARGEST COST SAVINGS PROVIDED BY HAVING A PCI SOLUTION BASED ON AUTOMATED CHANGE AND COMPLIANCE CONTROL IS THE ASSISTANCE IN REDUCING THE SCOPE OF THE AUDIT.

Automated change control will ensure that every change going into the network, whether through the change control application or not, is detected and stored. The PCI compliance solution must not only be aware of every change on the network, but must provide an auditable history (who, what, when, and why for each change) so that auditors can review the history. For example, PCI DSS Requirement #6, Develop and Maintain Secure Systems and Applications, specifically 6.4, Follow change control procedures for all system and software configuration changes. The procedures must include the following:

- Documentation of Impact
- Management Sign-off by Appropriate Parties
- Testing of Operational Functionality
- Back-Out Procedures.

The granular access controls and documentation that are inherent to an automated change control solution can enforce this.

Another PCI DSS requirement states that network managers must be able to build structure compliance tests detailed enough to validate individual configuration lines, but can also be aggregated to form comprehensive compliance policies automatically enforced upon change detection. In order to ensure that any lapses in compliance are immediately identified and remediated, network engineers must have flexible reporting and dashboard capabilities available to them, and any PCI compliance solution must provide this in order to be of significant use.

PCI DSS requirement 1.3.1 requires that firewall policies are established that restrict "*…inbound Internet traffic to internet protocol (IP) addresses within the DMZ (ingress filters)*." In essence, block access between publicly accessible servers and any system component storing cardholder data. Using compliance tests and policies within the automated change control solution, network managers can ensure that the specific access-list lines needed are in place at all times.

Using automated software, network engineers can assemble a dashboard that shows all pending changes, a list of changes in the past 24 hours, any changes flagged as non-compliant by the compliance engine, and a graph illustrating the overall compliance percentage across the network. If compliance violations do appear on the dashboard, the network engineer can immediately drill into details as to which devices failed compliance, what the offending configuration lines are, and who made the change. With automated change control in place, the network engineer can then rollback the access-list on the device and re-run compliance, resting once the dashboard shows "0" compliance failures.

PCI requires that security policies be reviewed no less than on a quarterly basis, and annually auditors will want proof that these reviews have taken place. A PCI compliant change configuration solution provides network managers with the ability to review current procedures and compliance policies in the context of the DSS requirements. Updates to the policies should be recorded in an auditable history, so that auditors can easily verify the ongoing management of the policies and procedures.

The PCI compliant change configuration solution should provide both current state and trending information on compliance to the established policies, so that network managers can make informed decisions about the direction they give the engineering resources. In addition, both sets of reports are useful to the auditor, since they demonstrate that a high level of compliance has been maintained all year, including the time of the audit.

Preparing for a PCI audit can be a costly endeavor, with tier 3 and 4 merchants spending $250,000-$300,000 on audit preparation. Most of this cost is spent trying to analyze PCI requirements and construct meaningful reports for the auditor.

Costs can skyrocket when an auditor spends billable time either wading through network details which haven't properly been summarized, or when prepared reports were deemed inadequate by the auditor, forcing a scramble to locate new information for a wide variety of resources.

Any PCI compliant change configuration solution needs to provide a well thought-out and easily accessible hierarchy of reports that can be printed out for any auditor to clearly acknowledge adherence to PCI DSS requirements.

When selecting a PCI compliance solution, network managers should keep the following criteria in mind:

• Automation – The solution must provide a high degree of automation, especially as it pertains to change control and compliance verification.

• Embedded PCI Knowledge – Look for evidence that the vendor has analyzed the PCI specification, and understands what is required to demonstrate to an auditor, showing compliance has been achieved.

• Change Control - The solution must work in a heterogeneous (multi-vendor) environment, must facilitate a structured approval process, and must contain strong audit capabilities.

• Compliance Enforcement – Structured compliance policies must be detailed enough to validate individual configuration attributes, and must provide automated compliance checking of all detected changes. Extra cost-savings can be achieved when the compliance engine supports automated remediation, staging changes for managers who must only review and approve the remediations.

• Reporting and Dashboards – Dashboards should be flexible enough for an engineer to monitor change and compliance information from a single screen. The product should facilitate the audit preparation by providing a structured and well thought-out list of reports for the auditor.

Achieving PCI compliance is not about where your network is today, but about how you can ensure where it will be tomorrow. An automated, PCI compliant change configuration solution can assist in all phases of preparation for PCI, and carries the additional benefit of cost savings through automation.

Matt Clark is the Director of Compliance Reporting at Voyence (www.voyence.com), where his responsibility is developing Voyence's automated compliance engine. Matt has held several roles during his six-year career at Voyence, from software development and quality assurance to project management for the implementation of Voyence's flagship offering - VoyenceControl - for major service providers. He welcomes your comments at mclark@voyence.com.

Uncontrolled use of USB sticks, MP3 players and PDAs opens up your network to data theft and viruses

Only $ 925 for 50 users!

Control user access to all devices connected to your network with GFI EndPointSecurity

GFI EndPointSecurity

TMC LABS INNOVATION AWARD 2006

Window Security.com Gold Award ★★★★

You have invested in network anti-virus software, firewalls, email and web content security to protect against external threats. Yet any user can come into the office, plug in a USB stick and take in/out over 32 GB of data. Users can take confidential data or they can unknowingly introduce viruses, trojans, illegal software and more – actions that can affect your network and company severely. Yet, as an administrator you had no way to control this until now!

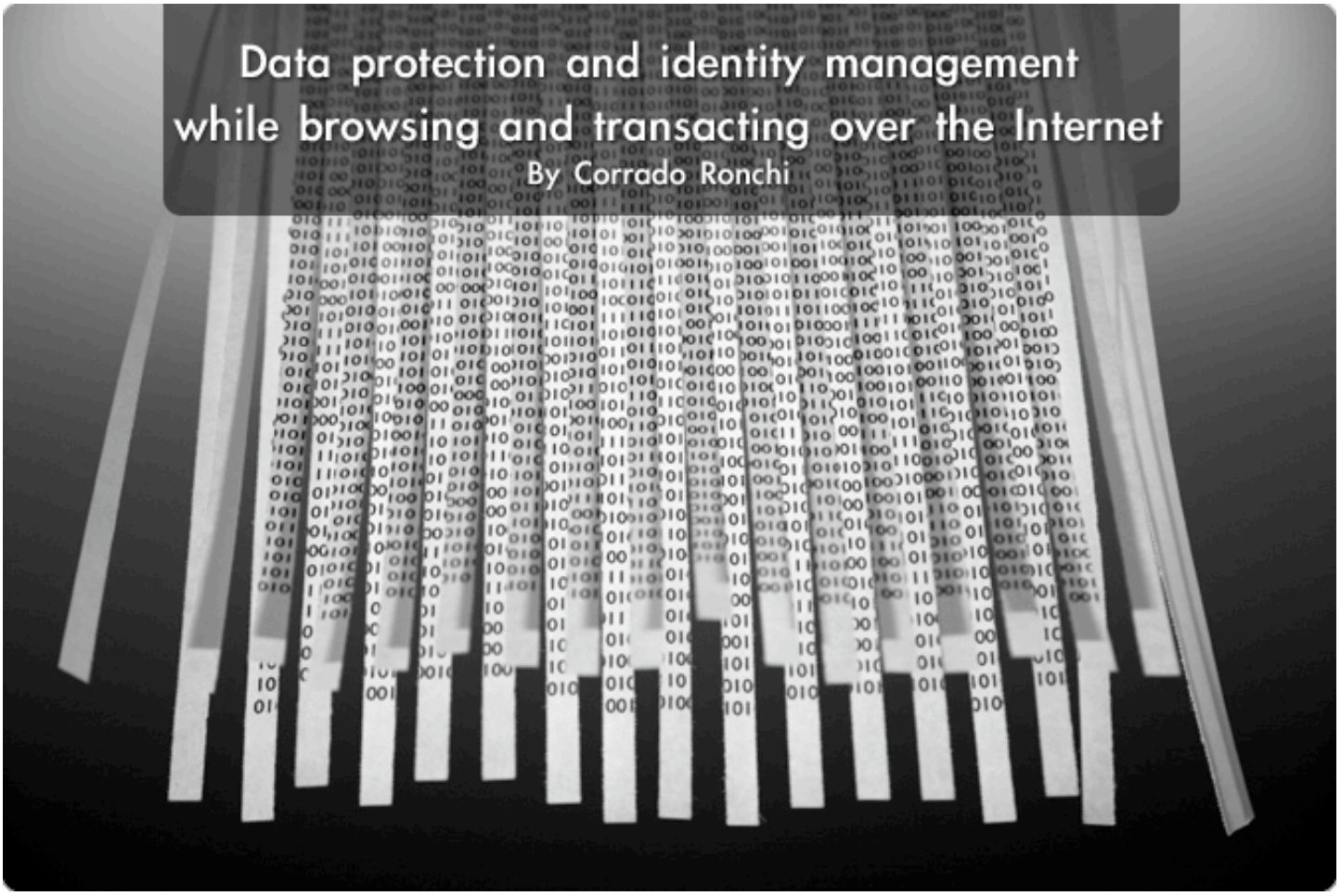
GFI EndPointSecurity allows administrators to centrally manage user access to devices such as iPods, USB sticks, PDAs, laptops and more. Controlling user access to such connectable devices allows you to:

- Protect your network by ensuring users don't introduce viruses and other malware
- Stop the alarming rate of insider data theft
- Increase employee productivity by preventing them from bringing other work, games or personal projects to their workplace
- Prevent users from introducing illegal or unauthorized software on their machines.

Download your FREE trial version from www.gfi.com/esecin/

GFI NETWORK SECURITY CONTENT SECURITY MESSAGING

tel: +1 888 243 4329 / +1 919 379 3397 | email: sales@gfi.com | url: www.gfi.com/esecin/



Data protection and identity management while browsing and transacting over the Internet

By Corrado Ronchi

Notwithstanding personal choices based on preferences for feature sets, usability, performance or interface design, all Web browsers share the same basic architectural building blocks among which, it is fair to say, data and identity security is not one of the cornerstones.

The reasons for this apparent lack of concern for security in the browsers' blueprints are in part historical (security threats have greatly evolved and expanded since the first appearance of the Internet), in part technical (security features require careful and more expensive a priori design) and in part legal/political (embedding strong encryption and privacy tools may first require social acceptance and proper legal framing). Be that as it may, the reality for today's Internet users is still that of an uphill battle against a multitude of threats to the privacy of their surfing data and of their online identities.

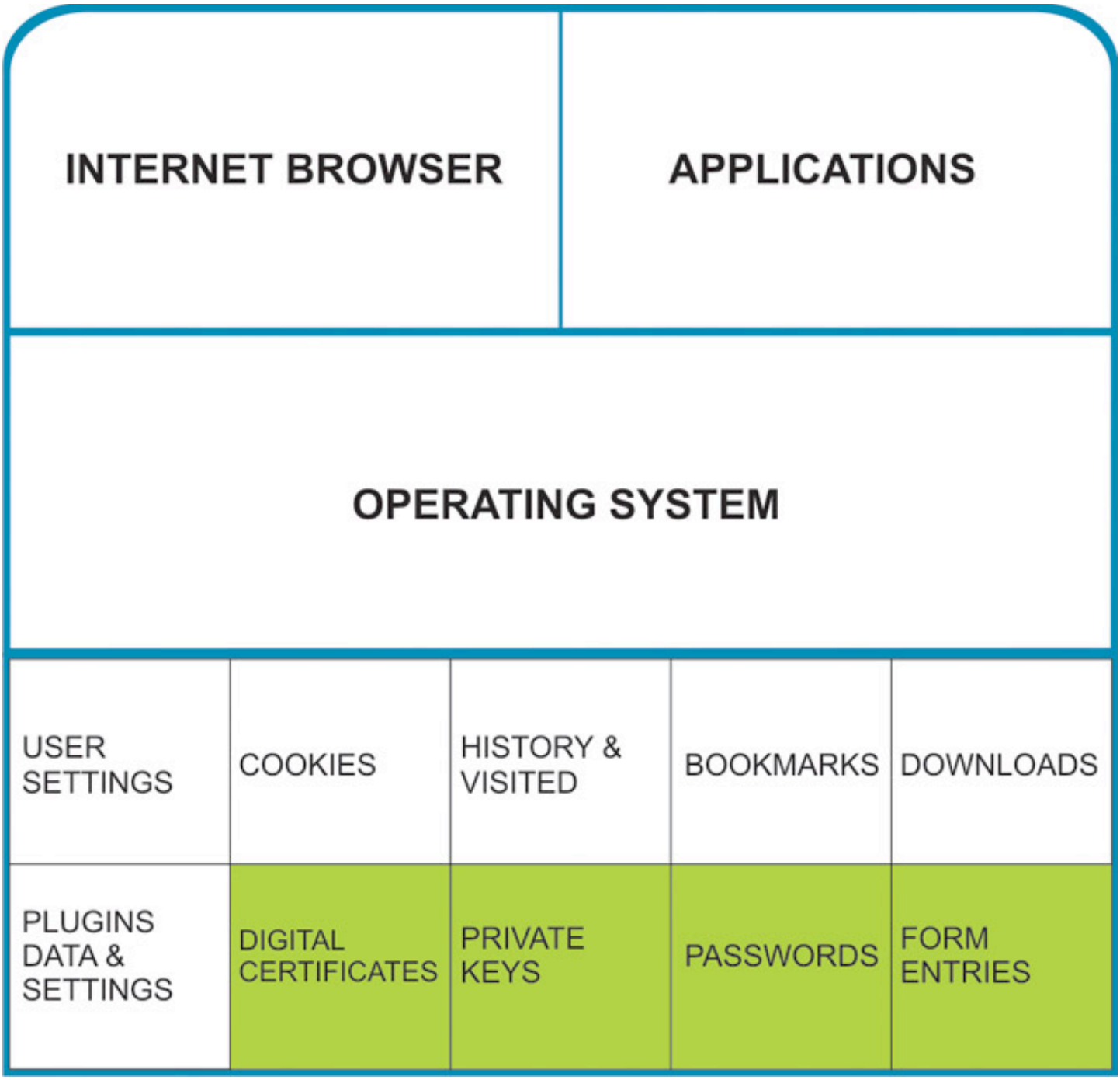
At the risk of oversimplifying such a multifaceted issue, let us first focus on two of the main security concerns for Internet users: local storage and network identity. The main assumption is that no information on Internet activity and/or online identity should be disclosed without the user's prior authorization and knowledge.

It is interesting to note that participants in focus groups on Internet usage often find such requirements too strong or even unnecessary until they are presented with the list of Web pages, form entries and passwords gathered during their previous navigation session.

When the harsh reality of privacy infringement hits the soft spot of one's own personal sphere, people tend to think again about the need for an adequate protection of their Internet activity.

Where is my Internet surfing data?

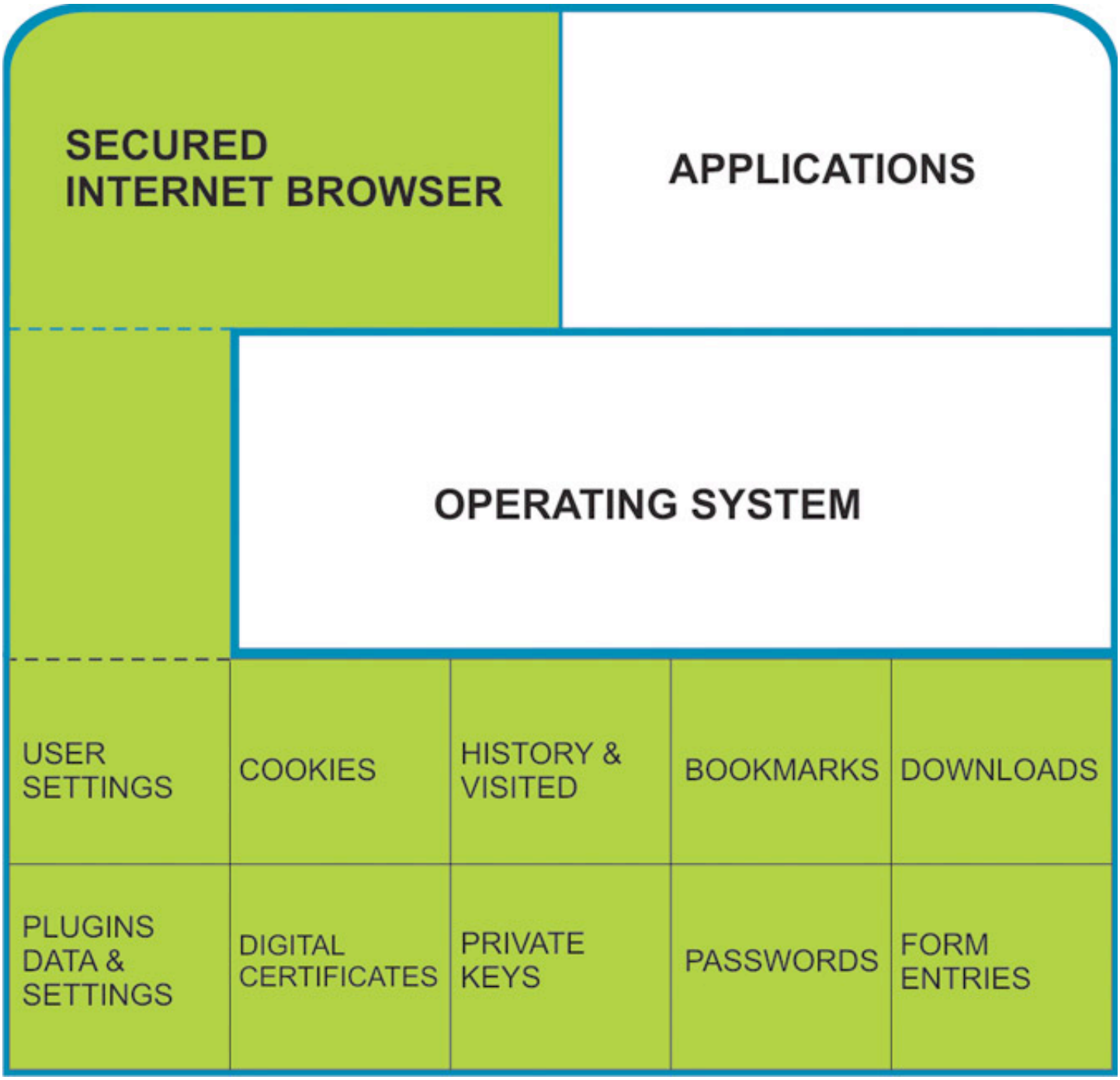
Navigating with any of the five mainstream Internet browsers mentioned above leaves a trail of data behind, stored in clear format inside well-known folders, readable by anyone who has access to the PC and by malicious codes (e.g. Trojans) silently executing in the background.



Sensitive data—browsing history, visited links, bookmarks, site cookies and, in some cases, digital certificates, Web form entries and passwords—are constantly in danger of being copied, captured or disclosed to others without the user's knowledge.

Most Internet browsers do provide some means for clearing navigation data, or cache, by periodically erasing the application files where such data are stored. This resembles more of a Catch-22 situation rather than true protection, however. In fact, one is really never sure of the right time to perform the deletion (before, during or after browsing?) and will always be tempted to postpone it, since the operation also erases useful links and data that one may need at a later time. On the other hand, access to the browsing applications is generally not controlled and no form of authentication is required to launch them. This implies that gaining access to someone's PC log-in account also grants the freebee of unrestricted access to the user's Internet environment. All these facts are well known to security professionals and to a growing segment of the user population—typically those who have learned the hard way about the standard browsers' vulnerabilities.

There is no doubt that current technologies, both at the hardware and at the software levels, can provide a much stronger level of security to the average Internet user.



Therefore, it should be possible to implement user authentication and strong encryption of all browsing data and thereby mitigate or even remove the majority of the security threats mentioned above.

There is still limited activity in this direction, however, compared to the dimension of the issue and the size of the affected population of end users. The few known initiatives for securing Internet browsers are not sponsored by global software multinationals, but by smaller companies with focused expertise aimed at occupying a specialized niche in the security market. Part of the reason for Microsoft's disinclination to include local security measures into Internet Explorer 7.0 may lie in the strong coupling of its software to the PC operating system and to the application environment and its components, which still suffer from equally damaging security vulnerabilities. On the other hand, the general availability of encryption tools for protecting Internet surfing data may fuel fears of misuse and hinder the work of law enforcement officials against criminals and terrorists. A recent initiative from Germany's Interior Minister Wolfgang Schäuble may help shed some light on the potential relevance of this concern. The ministry is advocating for the development of means to secretly install government Trojans (loaded with so-called "Remote Forensic Software") onto the computers of crime suspects.

Needless to say, privacy advocates are concerned about such measures, pointing to the blurriness of the boundary separating a priori a crime suspect from an innocent citizen. The German supreme court recently determined that such "legal hacking" techniques cannot be used because no legal framework exists at present. This ruling, however, leaves room for further debate as Mr. Schäuble will reportedly push for the constitutional changes needed to allow the police to perform activities defined as "online house searches." This case should not be considered an exception but rather an indication of a global reality that has been in constant development during the past decade, albeit subject to the general public's low awareness and scrutiny.

According to The Economist, "These days, data about people's whereabouts, purchases, behavior and personal lives are gathered, stored and shared on a scale that no dictator of the old school ever thought possible. Most of the time, there is nothing obviously malign about this. Governments say they need to gather data to ward off terrorism or protect public health; corporations say they do it to deliver goods and services more efficiently. But the ubiquity of electronic data-gathering and processing —and above all, its acceptance by the public— is still astonishing, even compared with a decade ago. Nor is it confined to one region or political system.

Who cares about My IP address?

The second dimension of Internet users' privacy is that of anonymity and online identity management. It is a well-known fact that simple analysis of the data header packets generated by Internet traffic can disclose the source (IP address), destination, size, timing and possibly even the content of the surfing activity. Similar to the issue of securing the local surfing data, no integrated solution is currently offered for protecting Internet users against traffic analysis, and thus their traffic privacy is de facto left totally exposed. However, the question often asked is: why should the average user care about disclosing his source IP when browsing over the Internet?

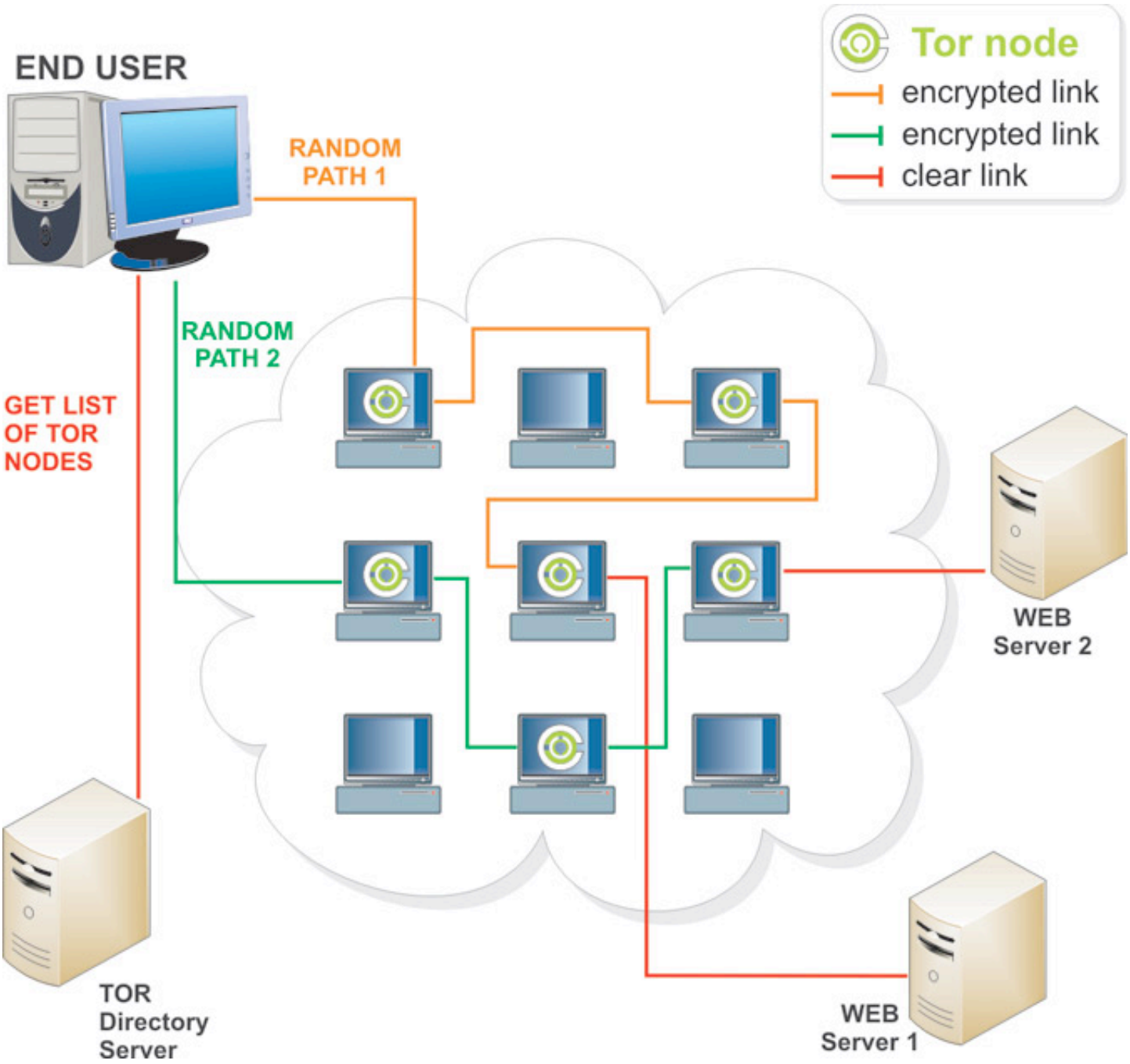
Knowing the origin and destination of Internet traffic allows any third party to track a user's online behavior and interests. Most frequently, the monitoring party is also the Web content provider, interested in profiling visitors' geographical location, browsing activity, subject preferences and social status.

The data collected can be later used and sold to allow targeted advertising or to enforce price and even service level discrimination. In other cases, traffic analysis can allow foreign government authorities to scan Internet visitors based on their countries of origin, thereby facilitating subtle forms of censorship using preferential routing and keyword filtering. Protecting network anonymity can also safeguard against prejudice during socially sensitive communications, such as those occurring in chat rooms and Web forums for political dissidents, rape and abuse survivors or people with severe and disabling illnesses.

Companies are also systematically gathering data about their employees and online customers, who typically are totally unaware of the information they are handing over during their transactions and of the subsequent use made of such information.

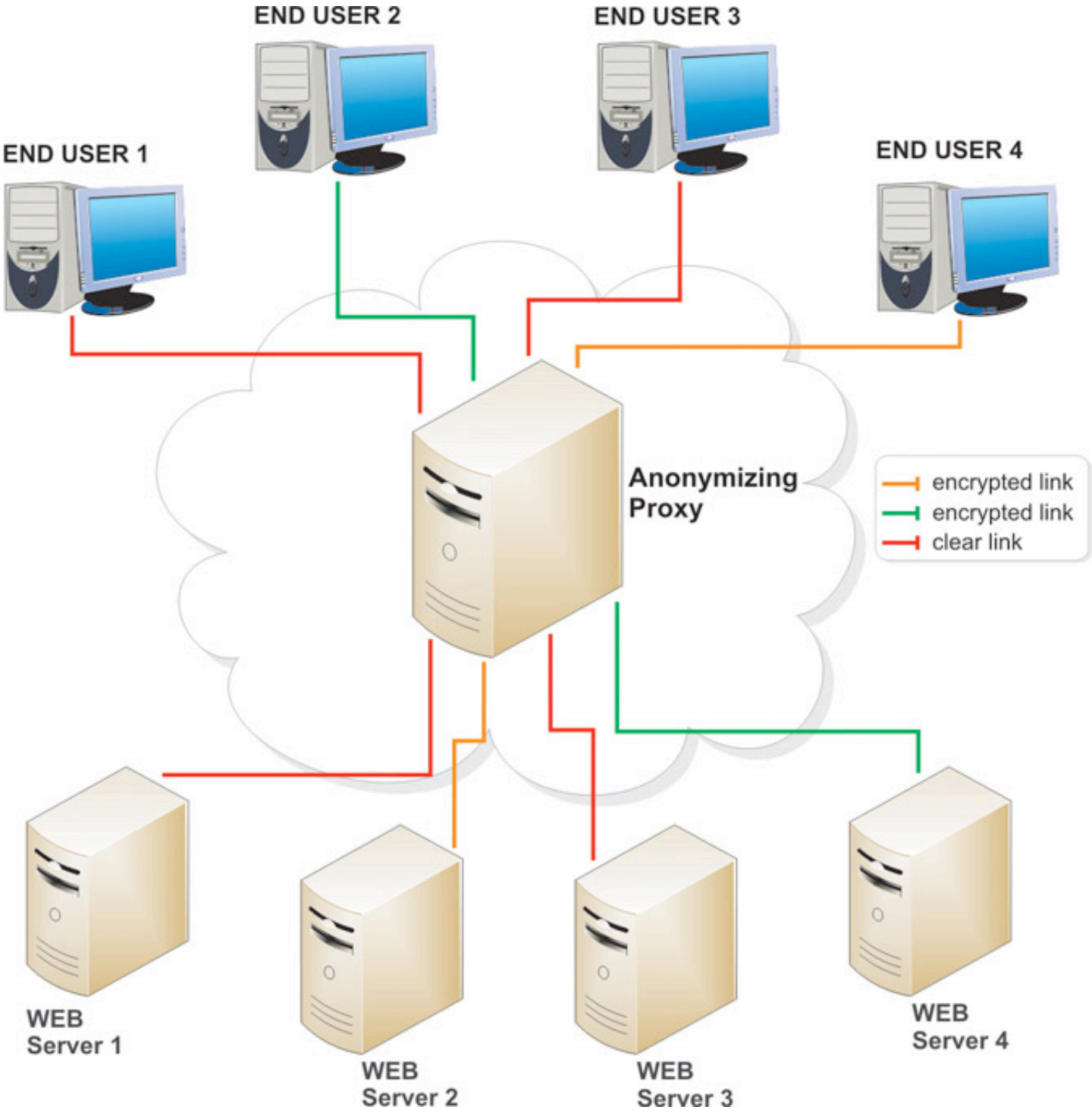
On the other hand, security concerns have resulted in legislation concerning the surveillance and monitoring of Internet use in several countries. Although distinct from filtering, these have many parallels in their potential impact upon online freedom of expression and access to information. Recent and controversial EU legislation is aimed at regulating the surveillance of traffic data and its retention. The European Data Retention Directive, which will become effective for Internet traffic by March 2009, requires ISPs in the various nations to retain data pertaining to Internet access, e-mail and telephony for a minimum period of six months but not exceeding two years. Through the formal establishment of common procedures for data retention, this directive should facilitate the tracing of illegal content and to identify those who use the electronic communications networks for terrorist activities and organized crime. Privacy groups across all the member states, however, are voicing their concerns about the rights of ISPs, search engines and Web companies to retain data and monitor people's online habits for up to twenty-four months, which seems like an unjustifiable length of time.

These examples help us better understand the growing demand for tools to counteract traffic analysis and to allow end users to choose if and when to disclose their Internet identities. A popular resource is the Electronic Frontier Foundation's Tor toolset, which employs Onion routing, a technique for pseudonymous (or anonymous) communication over a computer network, developed by David Goldschlag, Michael Reed and Paul Syverson. The basic idea behind Onion routing is to distribute the connections randomly over several Internet nodes, so that no single node can recover the complete path (including the origin and destination) that a data packet has followed.



Before each hop along the circuit, the end user's client negotiates a separate set of encryption keys to ensure that a node cannot trace the connections passing through it. Because of the distributed and encrypted nature of Tor paths, using this technology for anonymous surfing may (and in most cases will) substantially degrade the Web browsing speed with respect to clear direct connections. Onion routing, however, is also implemented in private networks owned by companies selling anonymity services to customers who are willing to pay a premium for a large bandwidth guarantee. In such cases, the service providers look at their private Onion network of virtual tunnels both as the technical means for

ensuring anonymity and as the legal means for avoiding legal liabilities for the end users' online activity. In fact, the nature of Onion routing complicates noticeably the task of packet tracing even when all network nodes are controlled by the same entity. It is also worth mentioning that the Onion routing approach provides better anonymity protection than the "anonymizing proxy" approach shown in the picture below, where all communications appear to come from a proxy server and not from the true originator:



This technique has the advantage of a simpler architecture, focusing traffic through one server that screens the identities of all the originating locations. A more careful analysis, however, also reveals that the "anonymizing proxy" approach suffers from the main disadvantage of requiring the users to place all their trust on one single entity. This "trusted entity" is de facto a single point of failure, where a compromise or successful attack is enough to reveal the identities of all the users. The Tor public service, on the other hand, suffers from a known vulnerability that can be easily spotted by looking at the routing diagram: the

last node through which traffic passes in the network has to decrypt the communication before delivering it to its final destination. In other words, the entity operating that node sees the communication passing through it in the clear. This vulnerability points to the difference between protecting anonymity and assuring confidentiality or integrity, something that, unfortunately, Tor users don't yet seem to fully appreciate.

Recently, Dan Egerstad, a Swedish computer security consultant, posted online the user names and passwords for 100 e-mail accounts intercepted by hosting five Tor exit nodes placed in different locations on the Internet as a research project. This was a dramatic demonstration of how an opportunistic attacker could exploit a Tor exit node to view and manipulate the traffic of a large numbers of users—which in this case also included people from embassies belonging to Australia, Japan, Iran, India and Russia—without the need to compromise key parts of the Internet infrastructure. Naturally, the use of end-to-end encryption (e.g. via SSL connectivity) would force the traffic to leave the Tor exit node still encrypted, thereby preserving the integrity and confidentiality of the communication.

The lack of ubiquitous cryptography in network communication protocols, however, leaves the unaware Tor end-user often exposed to this form of attack to the privacy of his anonymous Web sessions.

Platforms for ultra-secure Web transactions

Some of the points touched on above also apply to enterprises wishing to provide their employees and/or customers with strong security means for accessing the corporate domain or for transacting over the Web. The slow penetration of online banking compared to other Internet activities is a clear indication that both the financial institutions and the end users are aware of the high vulnerability of the current Internet browsing platforms when it comes to carrying out sensitive transactions.

Recent FFIEC regulations requiring two-factor authentication in financial business are aimed at mitigating the risks associated with the use of Internet-based applications and services. The rise in the variety and sophistication of cyber fraud and identity theft points to the strong need to provide protection well beyond the simple perimeter level.

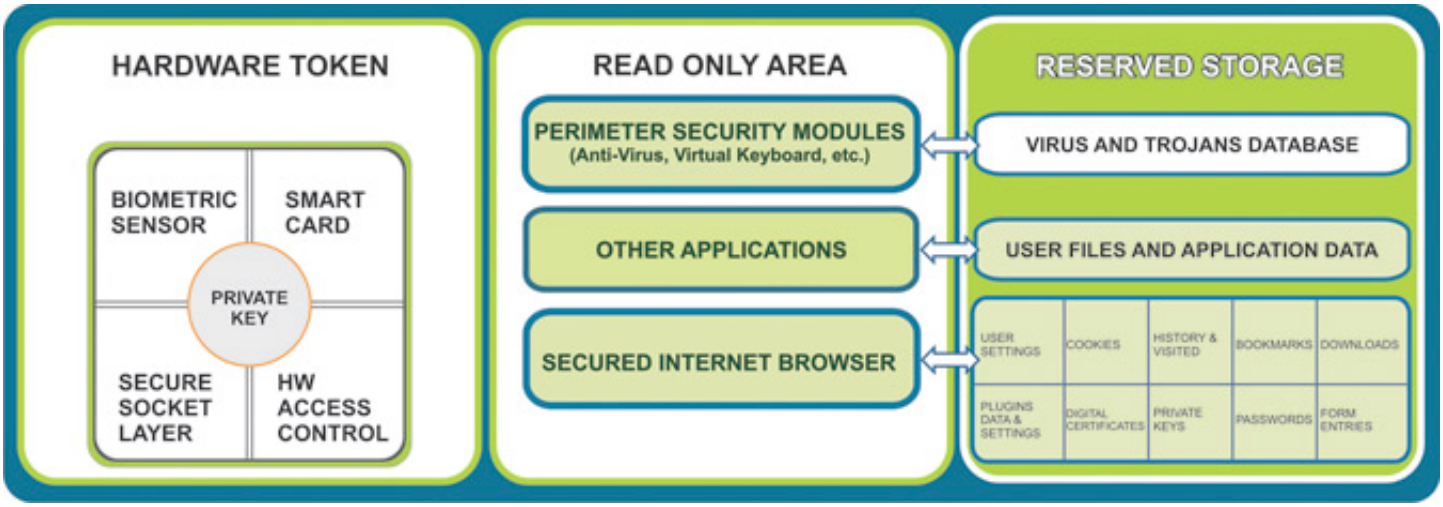
Here we wish to report on the slow but steady emergence in the industry of ultra-secure products for Web transactions. These products offer the combined features of a smart-card-enabled hardware token, a mass storage device for data encryption and a secure application platform. As shown in the figure below, this new family of products exploits standard smart-card technology to deliver PKI-compliant two-factor authentication, on-the-fly hardware encryption and digital signatures of both data and transactions. The on-board SSL engine allows seamless enforcement of mutual client-server authentication as definitive protection against phishing or man-in-the-middle attacks.

At the same time, a second, read-only layer holds embedded zero-footprint applications such as anti-keystroke-loggers, anti-virus, biometric sensors and Web transaction engines that enable users to be identified and to securely access and operate online without the need to rely on PC resources.

A final, third security layer is dedicated to the safe storage of personal and financial data, which can be kept permanently encrypted and managed without fear of exposure to the PC operating system and its vulnerabilities.

The usability advantages of this new generation of products for end users are obvious, especially when presented as an easy-to-use device such as a familiar USB stick and with no major learning curve to master. Furthermore, the flexible on-board flash memory allows remote updating of the applications' databases and security components in order to oppose new threats without having to physically replace the units.

The possibility of loading such devices with a variety of pre-installed and pre-configured security applications opens the road to targeted offerings and functionalities specifically designed for the online needs of vertical markets.



Finally lifting the security concerns of financial institutions and corporations without overburdening the end users with complex and unfriendly procedures will undoubtedly increase the number of online bankers, e-commerce and Web transaction clients, ultimately transforming them from passive users to active customers.

Corrado Ronchi (CISSP) is the co-founder and CEO of EISST Ltd., a multinational company focusing on software architecture, applied cryptography and mobile storage technologies. Corrado has conducted academic and applied industrial research for 20+ years, consulting with major European and USA corporations on strategic issues concerning information security technologies applied to Internet-based business models, regulatory compliance and business-critical applications. Originally from Brazil, Corrado holds a Master's degree in theoretical astrophysics from "La Sapienza" University of Rome and a Ph.D. in applied physics from Cornell University. Prior to his current occupation, he worked for leading global corporations, including Telecom Italia, AT&T and Cisco Systems. The author can be reached by email: cronchi@eisst.com.

Securing moving targets

By Caroline Ikomi

Newton's first law of motion states that a moving body will want to keep moving. The same law also seems to apply to business data, and the problem is trying to stop that mobile data moving further than you want it to.

It's an issue that has caught out a number of very high-profile organizations, from the UK financial institution, the Nationwide Building Society, to MI5, the British security service. Both have suffered embarrassing losses of laptops, with the potential for damaging data leaks from those devices.

What's more, the problem is growing. In the 2006 FBI security survey in America, theft of laptops and mobile devices was second only to viruses as the most common type of attack detected over the previous year. Nearly 50% of those responding to the survey had suffered, with an average loss per respondent of over $30,000 USD – up from under $20,000 the previous year.

So how should mobile data security be addressed? Broadly, this means looking at three key issues. The first issue is hard disk encryption of laptops, and smart devices such as PDAs, mobile phones and USB devices. Second is the requirement to audit and control data transfer and access to removable media, for example USB keys or iPods. The final issue is control of the security policy running on the user's endpoint device – irrespective of type of device.

Let's now look at each of these issues separately – and how security administrators can best control the use of mobile technologies to give the widest access to corporate resources while maintaining control to the organization's security policy.

Disk Encryption: full-disk or file?

Once you have decided it is necessary to protect your mobile devices then you will need to decide on whether to implement full-disk encryption (FDE) or file-based encryption.

The latter is tempting, because Windows XP comes with file-based encryption built in – in common with Linux, and the Macintosh operating system. While these methods mean that anything stored in specific folders or directories is encrypted automatically, there is a significant security flaw. They rely on users putting files in the encrypted folders themselves.

That's fine in theory, but as an IT professional do you want to rely on users to know what is sensitive information and two to place it into the appropriate folder. Even for the sharpest end-users the issue is further complicated by popular applications such as Outlook and Web browsers, which scatter attachments across file systems, often in obscure places. Folder-level encryption helps only if the IT department can tightly control all files and applications.

File encryption is only as good as your end-users' level of interest or knowledge. Simply put would you leave updating the corporate AV software, or software patching to your users?

The key advantage of full disk encryption is that it automates the process and secures the entire disk, so mobile users don't have to worry about it – and also cannot interfere with it.

Enterprise data encryption solutions also offer central management with tools for resetting passwords when the user forgets or leaves so the corporate data remains a corporate asset. Let's look at some of the factors it is worth considering with a full disc encryption product.

The key advantage of full disk encryption is that it automates the process and secures the entire disk, so mobile users don't have to worry about it – and also cannot interfere with it.

Performance and standards

Increasingly, compliance emphasis is being placed on encryption that meets the Federal Information Processing Standard (FIPS) developed by the United States Federal government. This entails the use of either Triple DES (Data Encryption Standard) or 256-bit AES (Advanced Encryption Standard) as the encryption algorithm.

Encryption performance is also a factor to consider. A common criticism leveled at FDE techniques is that they slow down the PC's performance, with the user experiencing delays while data is encrypted and decrypted on the fly.

To a certain extent this is true, but misleading. A typical business-oriented machine from a corporate fleet of laptops, built in the last 2 to 3 years, will have the processing power and memory capacity to make any difference in running performance barely noticeable.

In fact, the only times that FDE truly impacts on performance is on boot-up or going into hibernation – but this is a very modest trade-off for security.

It's essential that the FDE solution you choose is operative during these wake-up and shut down periods, to avoid security vulnerabilities.

Busy users often don't shut down their laptops at the end of a session: they put them into sleep or hibernate mode, so they can start again quickly. It is vital to ensure the FDE solution you choose can encrypt the contents of the laptop's memory during the process of it being written to the drive. If the solution does not do this, a thief can remove the disk drive from a stolen laptop that's in sleep mode, mount it in another machine, and recall and read the data written from the memory. Support for laptops' sleep and hibernation modes is critical.

For similar reasons, it's important to choose an FDE solution that encrypts data before the laptop operating system loads, on boot. The FDE solution should take control while the computer's BIOS looks for a master boot record to load, to prompt for the users for their login credentials. This ensures that only authenticated users boot the OS, and minimizes the opportunities for manipulating data.

Security in hand

While the examples given so far relate to laptop PCs, the same concerns are just as valid for PDAs and smart phones which are also platforms for corporate data. Because these devices vary in operating system – from Symbian, Pocket PC and Windows Mobile to Palm – and architecture, an easy security solution is harder to define than for an Intel PC platform.

Key concerns for handheld security include a rigorous audit of all the devices being used within the enterprise, and then a single encryption solution to cover as many of the platforms as possible. If the handheld device is not authorized, the default approach should be to not allow connection to the corporate network or storage of sensitive data. And as with full disk encryption on laptops, the solution chosen should encrypt data automatically with no user intervention, giving ease of use with control and enforceability.

In terms of encryption strength for handheld devices, this is typically not as strong as for a fully specified laptop, but look for 128-bit AES for data stored on the devices as a minimum.

However, this is only the first part of the security picture. Full-disk encryption is not a magical shield against all types of security threat to portable devices. While it will protect data on the hard drive from compromise if the device is stolen or lost, the hard drive is only one storage medium in use on a typical laptop. This brings us to the second area for endpoint security: the management and control of data leakage.

Key concerns for handheld security include a rigorous audit of all the devices being used within the enterprise, and then a single encryption solution to cover as many of the platforms as possible.

Data leakage: audit and control of removable media

Endpoint security should ensure that the organization is able to avoid data leaks onto peripheral devices such as USB drives and portable storage media – such as MP3 players and digital cameras.

The starting point for protection against leaks via these USB devices is to include them in the business acceptable usage policy (AUP) and to educate users on the importance of following policy – which will include the business risks of breaching policies.

However, policies alone are not enough. How should they be backed up and enforced? This is the role of port control solutions, which can automatically block a USB device that does not comply with the corporate security policy or prevent the transfer of certain files or file types.

An example of a corporate security policy could include allowing encrypted USB devices – but not an iPod or mobile phone – from an authorized user. Again the ability to manage the security policy centrally will be a key requirement to the Security Department as in a large environment it would not be unusual to have 1000s of USB devices. Once the data is encrypted on an authorized device it must be accessible to the organization if required through central administration of the system.

At the end(point)

This leads us to the third area of endpoint security. How do we protect the data on the machine from software threats such as application-level attacks or malicious code?

The starting point for an effective endpoint security strategy is for every machine to run a firewall and antivirus protection with up-to-date signatures before it is granted a connection to the corporate network. This client should also ensure that the laptop is running the appropriate software patches and include a VPN client for secure transfer of corporate information back to the corporate infrastructure. As with all endpoint security it is important that this is managed centrally.

Other key points that should form part of the endpoint security plan are:

• Client lockdown, to prevent mobile users and attackers from disabling endpoint security or enforcement of network access policy. The ability to deliver comprehensive, assured endpoint security and policy compliance across the enterprise enables threats to be defeated.

• Inbound threats: laptop PC ports should only be opened for authorized network traffic and should block network intrusion attempts; port stealthing hides endpoint PCs from port scans.

• Preventing unauthorized applications and malicious code from capturing and sending enterprise data outbound to hackers.

• Email protection: this includes quarantining suspicious email attachments and inappropriate email – whether by network-based software or an in-the-cloud service – to help prevent address book hijacking.

With endpoint security, each time we touch the remote device it is a cost to the organization so the ability to centrally manage the security policy of the remote security solution will be a key factor in deciding on a solution.

Management matters

With endpoint security, each time we touch the remote device it is a cost to the organization so the ability to centrally manage the security policy of the remote security solution will be a key factor in deciding on a solution. Security without easy, central control by IT administrators leads to holes in defenses – holes which will eventually be exploited. Don't underestimate the importance of management.

Looking specifically at the management issues around full disk encryption, ensure the solution you choose to deploy lets IT staff easily perform day-to-day functions, such as resetting users' and administrators' passwords and PINs.

Make no mistake, many users will forget or lose their authentication details, so reallocating these needs to be simple and secure. Furthermore, IT staff will regularly need access to users' machines for routine upkeep tasks such as software patches and updates – so administrator access similarly needs to be secure and easy to manage.

For broader management of all endpoints, desirable management capabilities include the ability to exclude users or allocate specific user permissions; to create user groups; automatically push updates; integrate with existing LDAP or Active Directory infrastructures; and set configuration essentials such as user passwords, password lengths and strengths, retry attempts, lockout times and user recovery options.

The other essential management issue is quick access to comprehensive audit and event logs, which give an audit trail on user and network events such as when users are changing passwords, if there were failed attempts to log in, or errors occurring. This visibility is essential from both a management and compliance standpoint.

Load and lock

In conclusion, some industry observers question the need to have any sensitive data on mobile computing devices. It's an interesting point – but the data is already out there, and now that it has started to move, it's going to keep on moving.

Therefore, the only effective solution is to ensure that data loaded onto mobile devices is kept locked up.

Caroline Ikomi (CISSP) has worked in IT for 15 years, and has specialised in IT security since 1997 when she was security engineer for the utility company, London Electricity. She joined Check Point in 2000, and is now UK technical manager.

The need for a new security approach

By Mairtin O'Sullivan

Historically the goal of security for most companies was nice and simple - keep the bad guys out. And it was easy to classify who the bad guys were. The bad guys were everyone outside the company on untrusted external networks.

This approach worked pretty well until a number of reports emerged starting that internal threats accounted for around 50 to 60 percent of the total security threats to a company. Now the bad guys were more difficult to classify. This revelation required a new approach to security that revolved around keeping the bad guys out, even if they were inside the network. Companies ensured they had all their systems patched and "hardened" so that no attacker would be able to break in. This approach too has lasted a number of years and been very successful.

Recently, however there's been a marked move towards a new security approach. This approach revolves around securing the data itself as opposed to just the systems and networks that hold the data.

Why the somewhat radical shift in focus and need for a new approach? There are a multitude of reasons but the primary drivers are the increased awareness of the value of data and the failure of the existing security approaches to secure the data.

Companies now more than ever are realizing that their confidential data is in many cases the lifeblood of their business and loss or theft of the data could be critical

A simple example would be the prior approach to dealing with lost laptops. Previously a laptop left in the back of a taxi would have been written off as just the replacement cost of the laptop. The total cost to the business would be €500 maybe. Now however companies realize that the data stored on the laptop may be worth a whole lot more. How much would that laptop be worth if it currently held all your customer records? While it's hard to determine you can guarantee it's a lot more than €500, especially if you hadn't backups of the data!

Of course this is just one example of how former security controls don't adequately secure the data. Another major source of new risks to data is the fact that companies now want to share and integrate more with their customers and suppliers than ever before. Integration is no longer a competitive advantage, it's a requirement. This often involves giving external users access to internal systems and applications, many of which were previously hidden from public view by layers of firewalls. This increased requirement to expose internal applications to the public has emerged in conjunction with the explosion in web application security research. The problem here is that many of the vulnerabilities within web applications are exploited through the normal functionality of the application of which firewalls and traditional security measures have no visibility.

So what does this shift in approach actually entail for the average security manager? One of the most significant shifts is that the security manager must now interact more with the data owners. Previously if a new financial application was being introduced the security team would harden the server and then restrict access to it using a firewall. At that point their job was often done. The finance team would administer the application and that would be the end of it. Under the new data security approach however, the security team would also have to speak with the finance team to determine what kind of data will be stored in the new system, how sensitive that data will be, who will require access and where will the data flow both within and outside of the application.

Essentially the main elements of data security revolve around data classification, data encryption, data integrity and data access control.

Data classification is a key element in the data security model because unless you know how sensitive the data is you can't assign adequate security controls to its protection. For example, if you have two file servers on your network; one which stores all your companies intellectual property, and one which stores employee personal photos, which are you going to prioritize and assign greater levels of controls to? When stated like that it seems obvious but how many people really know what's stored on their file servers? And if you don't know what's there, you're either going to end up over-spending on protecting data that isn't sensitive or you'll under spend and leave sensitive data exposed.

Data encryption is a rapidly growing area of security. While security managers have been very familiar with the use of encryption for securing data in transit over public network such as the Internet, encrypting data at rest on file servers or in databases is a relatively new concept.

If data encryption is a new concept for many data integrity is an even stranger concept again. Data integrity boils down to a simple question, but one that often is unanswerable, how do you know the data hasn't been changed since you entered it? There are many examples where data integrity is even more important than data encryption. For example, if your company produced medicine, would you know if someone altered the formula just prior to a new batch being produced?

Data access control may seem like an area that's already addressed by existing access control controls but can you restrict access to the data throughout it's life? You may only allow the finance department access the budget files, how do you restrict access to the budget file once it's been copied to a USB key or emails to an anonymous email account? Technologies such as DRM allow you to ensure that only the members of your finance department can open the file so that if the file is sent outside the organization is will be useless to anyone else.

Each of the new controls bring with them many obstacles to overcome such as locating data, educating employees on classification, key management and supporting mobile workers. This are the challenges of the future. The next time you think about security, don't just think about how to keep the bad guys out, think about how to keep the data secure.

Mairtin O'Sullivan is a Senior Security Consultant at Espion (www.espion.ie)

NEW THREATS. NEW SOLUTIONS.

BLACK HAT STYLE.

The stakes are high for today's network defenders.

New security threats to governments and businesses emerge hourly, from sophisticated wireless attacks to remotely organized Bot armies.

Black Hat DC brings together the best minds in security to define tomorrow's information security landscape.

Featuring many new tracks, new training sessions and a special emphasis on wireless security and attack analysis, DC 2008 is a whole new Black Hat.

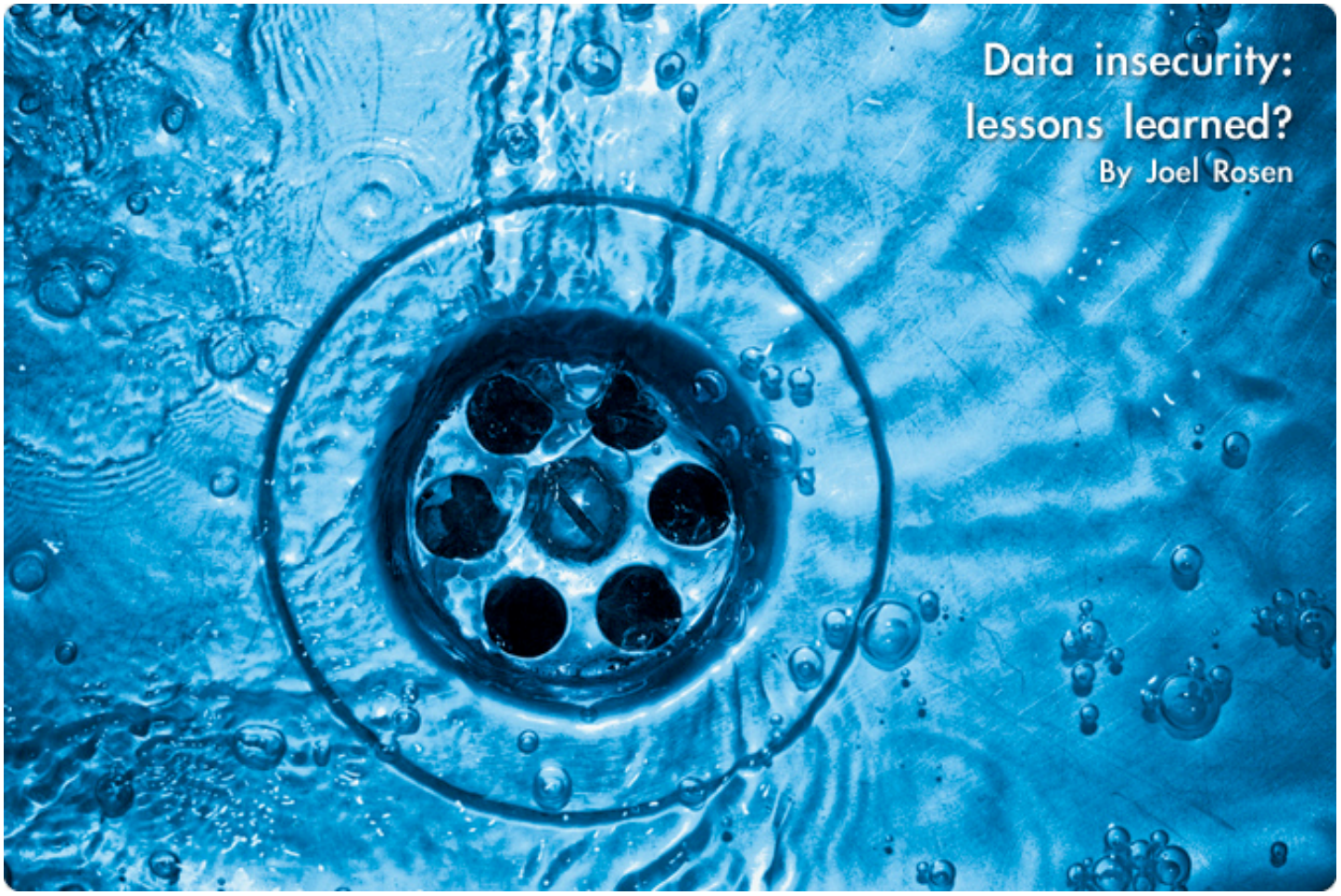
Join us February 18-21 in Washington DC and see for yourself.

Black Hat
BRIEFINGS AND TRAINING

FEBRUARY 18-21, 2008
WESTIN DC CITY CENTER

Diamond Sponsor
Microsoft

Gold Sponsors
IOActive
NORMAN
SAINT



Data insecurity: lessons learned?

By Joel Rosen

One of the things that we take pride in as intelligent human-beings is our ability to learn from our mistakes. And for the most part, we do. But this ability to adjust our actions when things go wrong seems to fly in the face of the data insecurity problem that's been dogging corporations for quite some time.

Since 2005, according to Privacy Rights Clearinghouse, 155,233,309 records containing personal information have been compromised. A recent Ponemon Research Study (The Business Impact of Data Breach, 2007) points out that the question isn't if a company will suffer a data breach but rather when. The same study reveals that the overwhelming majority of the US companies surveyed have experienced a data breach, and half of those respondents have no incident response plan in place. Scratch head and read on.

Data breaches are (obviously) an enormous problem. The fallout from mass data breaches includes: fines, law suits, loss of customer and partner trust, brand damage, loss of business and dropping share prices. What could possibly cause companies to ignore the data risk problem? The answer is that they're not ignoring it. According to the same Ponemon study, organizations that suffer data breaches actually employ substantially more data security measures than organizations that haven't suffered a breach.

What makes the data breach problem so hard to solve?

Security has always been a game of cat and mouse. The good guys lock up the valuables, then the bad guys figure out how to pick the lock, and the good guys add a new obstacle to keep the bad guys away. But before the cat and mouse cycle begins, an object has to be worth stealing. This is what is happening to electronic data.

Companies have used sensitive electronic data for quite some time; only in the last few years has data become such a valuable commodity that it's being targeted by a vast and growing community of data thieves. Only in the last decade has the nature of business called for electronic data, especially sensitive data, to be accessible to so many different

users. As the need for industries to provide data access to more stockholders grew, industries and governments imposed dozens upon dozens of regulatory requirements--including thirty five state and numerous federal regulations--on the care and handling of sensitive data. The state regulations bring with them the added challenge of notification (they mandate that any individual who resides in that state who is at risk from a breach be notified). Compliance with these regulatory requirements, although inspired by the need to protect and/or guarantee the integrity of data, became the primary focus of many companies.

In some respects, the regulations helped to clarify and in others they have complicated the data protection issue. The Payment Card Industry Data Security Standard (PCI DSS) has done a better job than most regulations of laying out the action needed to achieve compliance. The standard clearly calls for encryption to be used for the protection of cardholder data but unfortunately many companies read this as "encryption is the silver bullet for PCI compliance"—which it is not.

Adding to the data protection challenge is the fact that most organizations store data in multiple locations and in many different types of servers, and that data is accessible to thousands of computers on corporate networks and even larger numbers of people (maybe tens of thousands or millions) via the Internet. Data is portable and easier to hide than most valuables and harder to track. So, to sum it up, in order for businesses to achieve and/or maintain competitive advantage, many, many people must have access to data; data is at greater risk than ever before, but you can't lock data away or you will hurt your business; and, your company is likely to fall under a dozen or more regulations mandating that you know what is happening to the data in your care and be able to prove that you know what's going on with it. This adds up to a very difficult problem to solve.

DESPITE THE FACT THAT COMPANIES ARE EMPLOYING MORE SECURITY THAN EVER BEFORE, THE SECURITY METHODS THAT THEY'RE USING APPEAR TO BE LESS EFFECTIVE THAN EVER BEFORE.

This difficulty of securing sensitive/regulated data is evidenced by the fact that data breaches have become such a common occurrence that we are no longer surprised when data belonging to thousands of people is compromised (outraged maybe, but not surprised). Despite the fact that companies are employing more security than ever before, the security methods that they're using appear to be less effective than ever before. Data security is a moving target and we're in a phase where the bad guys seem to have momentarily pulled out in front—security needs to catch up. But, as the old saying goes, "we have the technology."

Where do you start?

Business practices are a good starting place when reformulating the way a company views their data assets and handles data security. There is another old saying that a fish rots from the head down. This is a colorful way of expressing the sentiment that a company's attitude (about data and anything else of critical importance) is passed down from top management. Data Governance is the term that many companies have adopted to describe their company's overarching plan for how data is to be handled by stake-holders. The more strategic companies start with a Data Governance plan and build programs from there. This is likely to be the way that many companies will formulate data protection strategy in the future.

In the present, however, companies tend to start from the immediate problem and work from there. They may be under the gun to pass a compliance audit (where non-compliance will result in stiff penalties) or have suffered a data breach that forces them to totally rethink their data security policies and activities. The question is, "what should a company consider when they're looking to update or overhaul data protection/governance practices?"

Searching the internet you can find statistics claiming that anywhere from 50% to 80% of data threats come from insiders. Whether these statistics are accurate or somewhat exaggerated, this is still a good starting place when it comes to rethinking data protection. Insiders are not just a company's employees, outsourcers or partners, but they are any users with credentials—this includes masqueraders pretending to be authorized users. These users have the keys to the kingdom. In other words, traditional security will not work. Catching insiders or outsiders masquerading as insiders, requires a new way of looking at things. If traditional security is "Outside In" thinking companies need to adopt "Inside Out" thinking. What this means is that instead of constructing obstacles from the perimeter inward toward the data, companies need to start from the inside—at the core data servers where data is stored.

What we've learned from recent breaches is that enterprises employing only data security architectures, designed to slow or stop attacks, cannot stop mass data breaches—where someone with credentials accesses a database or file server containing large amounts of valuable data assets.

Companies using only this type of "perimeter" security are subjected to data breaches that go unnoticed for many months (or years). There are many recent examples of data breaches that were detected long after the fact including a major retailer, a credit card processor and several well-respected universities –just to name a few. These organizations did not have insight into what was happening with the data stored in their data centers. They were not tracking user activity with sensitive data assets. Since no break-in alarms were sounded, no firewall of IAM system breached, the breaches were impossible to detect in time to mitigate damage.

Interestingly enough, at the core of almost all compliance regulations is the requirement that companies track who accessed which regulated data when and report on these actions in detail. These are essentially the same actions needed to prevent data theft from inside data centers.

CATCHING INSIDERS OR OUTSIDERS MASQUERADING AS INSIDERS, REQUIRES A NEW WAY OF LOOKING AT THINGS.

Rethinking data security

The Inside Out data protection model addresses insider data risk as well as compliance requirements. It also enables wide access to data because it is based on having insight into exactly what is happening with data—as it happens—without locking the data away.

The Inside Out model is based on four steps:

1. Discovery – Knowing where high value data is located and classifying it.

2. Monitoring – Capturing detailed information on the access to data as it is being accessed.

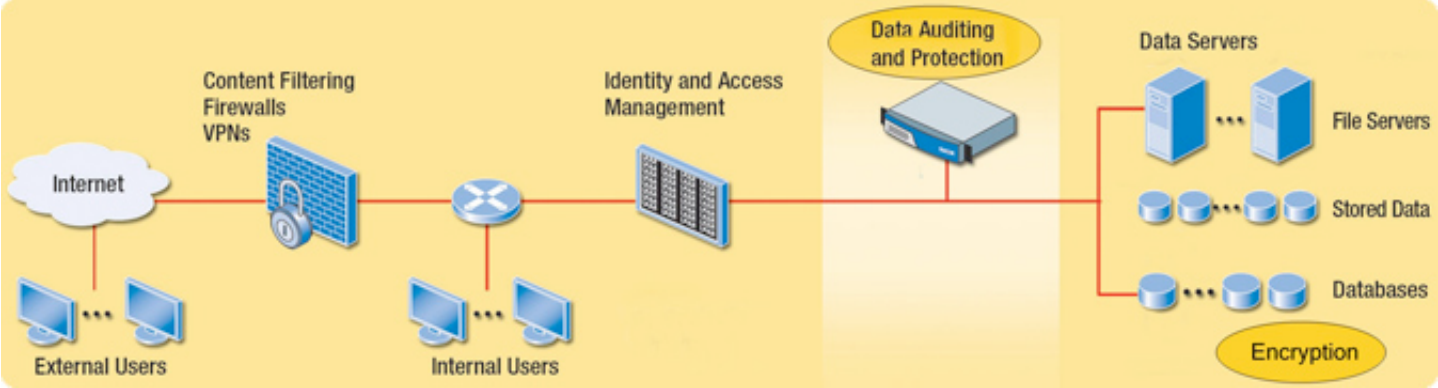
3. Theft Alerting – Using analytics that can detect theft accurately in real-time and alert on it (theft has to be differentiated from legitimate access - analytics are critical).

4. Automated Risk Mitigation – Alerting capable of sending data to response centers immediately, as a breach/data compromise is detected. This should be designed so that actions can fit the exact situation.

To illustrate the way Inside-Out security thinking works, it might be useful to visualize a security camera in Fort Knox that is being monitored by guards who know exactly who should be in what part of the building and who is allowed access to the contents of the vaults--right down to which blocks of gold they can touch. If they make it past the locks and the badge readers, the guard can see what they're up to, and if they overstep their bounds he can remediate based on the action they take.

This is an oversimplified analogy but it identifies the hole in data security that has allowed mass data breaches affecting databases to continue.

That hole is the inability to “see” what is going on inside data centers. Traditional best practices have emphasized the integrity of server-resident data assets. They have relied on layered defenses that include user authentication, access control, encryption and content inspection for data in motion. These methods are still extremely important for data security but they make up only part of the solution because they can’t tell the difference between an authorized user who is conducting legitimate business and a malicious insider who is stealing valuable data assets from a database.



What have we learned?

The current atmosphere of breach mania is a clear signal that beefing up existing methods is not the answer. To stay on top of the latest threats requires us to step back and rethink what security looks like. Insider threats pose some of the greatest risk to data and it will take more than traditional layered defenses to mitigate it. This is particularly true when it comes to privileged insiders who have direct access to systems and data and are capable of covering their tracks.

Compliance regulations are the motivators for much of the data security/data integrity action that is being taken by companies. They are a reaction to the fact that we’re not doing a good job of protecting data from being compromised. If we get data governance and protection right, compliance will fall in step behind it.

Getting it right is not a simple checklist exercise. Enterprises are complicated entities with diverse policies, data access needs, technology infrastructures and resources. That said, the answer is relatively simple---make sure you know what is going on with sensitive/regulated data at all times and make sure that you can prove that you know what is going on.

Inside Out data security with monitoring and behavioral analytics in an active role (to help companies know what is really going on with data and applications) is a necessary component of sound data governance and security. This is an intuitive leap--watch what is actually happening to data, don’t simply trust that the locks are secure—that will turn recent data security mistakes into both a security and bottom line business advantage.

As president and CEO, Joel Rosen drives the business strategy and day-to-day operations of Tizor. Previously, Joel served as president and CEO of NaviSite, a managed services infrastructure provider, where he led the company through a successful initial public offering and grew revenue tenfold to $100 million. Tizor Systems Inc., Maynard, MA, provides the world’s largest companies with the only data auditing and protection solutions that can monitor and report on all critical data activity across the enterprise – including databases, file servers, and mainframe applications – for compliance assurance, data protection and theft detection. Joel can be reached at 978-243-3231 or via e-mail at joel.rosen@tizor.com. Visit Tizor’s Web site at www.tizor.com.

NetStumbler
http://www.net-security.org/software.php?id=160

NetStumbler is a tool for Windows that allows you to detect Wireless Local Area Networks.

Kismet
http://www.net-security.org/software.php?id=218

Kismet is a wireless network sniffer. It is capable of sniffing using almost any wireless card supported in Linux.

WifiScanner
http://www.net-security.org/software.php?id=381

WifiScanner is an analyzer and detector of 802.11b stations and access points. It can listen alternatively on all the 14 channels, write packet information in real time, can search access points and associated client stations, and can generate a graphic of the architecture using GraphViz.

KisMAC
http://www.net-security.org/software.php?id=625

KisMAC is a free stumbler application for MacOS X, that puts your card into the monitor mode. Unlike most other applications for OS X it has the ability to run completely invisible and send no probe requests.

Wireless technologies, including Wi-Fi, are subject to security issues because data is transmitted through the air. Because encryption methods are not utilized on hotspot networks, everyone within range can "listen in" or capture potentially sensitive data.

One of the main benefits of networking in general is the ability to share files among other network users. However, this is not such a desired feature on public networks, because the users probably do not want others browsing through their files. This article addresses these issues and more, enabling you to provide a safer and more secure hotspot experience for your users.

Understanding everyone's responsibilities

Everyone has certain responsibilities when it comes to the safety and security of your Wi-Fi hotspot, as Table 1 below illustrates.

Hotspot Administrator/Owner	The User
Inform users of the risks when using a hotspot or unsecured wireless network.	Beware of the risks when using a hotspot or unsecured wireless network.
Give users safety and security tips.	Follow the safety and security tips.
Enable VPN1 Passthrough.	Use VPN connections.
Isolate clients.	Disable file sharing.
Filter hotspot content.	Use personal firewall software.
Secure user information.	Keep an eye on valuables.

Hotspot administrator/owner responsibilities

You as the hotspot administrator or owner have the obligation to do many things to help ensure your hotspot users have a safe and secure experience.

Inform users of the risks

One of the most important responsibilities that you have as a hotspot administrator or owner is to ensure that your users understand the risks associated with using an unsecured wireless network, such as your hotspot. Following are three such risks:

• Internet activity can be monitored.
• Login information from unsecured Internet services and websites can be intercepted.
• Any shared files are open for others.

People who have the right tools can capture the data that is flying through the air. Because hotspots do not use encryption, all the information that is sent over the wireless network can be captured. This includes the usernames and passwords when logging into web-based applications, such as websites (that do not use SSL with a HTTPS address), e-mail accounts, FTP connections, and other services that do not use encryption or other security methods.

Give users safety and security tips

After informing the users of the risks associated with using your Wi-Fi hotspot, you should provide solutions or methods that will help limit or eliminate these risks and issues. These solutions, as shown in the following list and discussed later, summarize the steps that users can take to ensure a safe experience while using public hotspots:

• Use VPN connections.
• Use secure (SSL) websites.
• Disable file sharing.
• Use personal firewall software.

Enable VPN Passthrough

Users can use VPN connections to secure their information that is being passed through the public wireless network. In most cases, VPN Passthrough is enabled by default (and should not be disabled) on wireless networking equipment, such as routers, access points, or hotspot gateways. This Passthrough feature opens the ports that VPN connections use. You can find the Passthrough settings in the Miscellaneous or Security section of your wireless device configuration utility.

Isolate clients

Some wireless devices, such as routers, access points, or hotspot gateways, have a client isolation feature. It is a simple and inexpensive version of the VLAN feature that is available on enterprise equipment. Client isolation blocks the traffic between the users on the network. Therefore, users cannot access each other's shared files. This benefits the people who forget to disable file sharing on their computer while using the hotspot.

NOTE: Keep in mind that if your Wi-Fi hotspot uses multiple access points (APs), you should enable the client isolation feature for each AP. This is because the isolation feature can be implemented only on an AP-to-AP basis.

Filter hotspot content

You can use a few filtering methods to help keep your users safer while using your Wi-Fi hotspot:

• Filter web content (to block pornography, foul language, and so on).
• Block certain Internet ports (to prevent the use of file-sharing programs, POP3 e-mail, and so on).
• Block specific websites.
• Block websites based on keywords.

The filtering and blocking features of particular wireless routers and hotspot gateways vary greatly.

Web content filtering solutions allow you to easily block illegal or inappropriate websites. This solution is great for hotspots that might serve a majority of youngsters; however, it typically is not feasible for general hotspots. Actively filtering the websites that users visit typically requires the use of hardware, such as a proxy server, and is too expensive and time-consuming for most hotspot owners.

Many wireless routers and gateways allow you to block users from using certain Internet ports. These ports are associated with certain applications and services, such as port 80 for web browsing.

Following are some ports you might want to block:

• 21 - FTP (prevent large transfers)
• 25 - SMTP Server (disable sending of POP3 e-mail to help prevent spam from originating at your hotspot)
• 1214 - Kazaa (online file-sharing program)
• 3689 - Network Jukebox protocol
• 6667 - Universal Internet Relay Chat (IRCU)

Many wireless routers and gateways, allow you to block users from visiting specific websites or those that contain keywords you define. For example, if teens are spending hours on a certain website, and it is causing problems, you can add that website address to the list. This prohibits the teens from accessing the website.

Using these methods can also help protect you, as the hotspot owner, from users who are performing illegal activities through the Internet access you are providing.

Secure user information

You should keep your user's information secure when it is traveling over the wireless hotspot and in any databases where sensitive information is stored.

Because hotspots are for public access, they usually do not use encryption methods—such as Wired Equivalent Privacy (WEP) or Wi-Fi Protected Access (WPA)—such as used in private networks at homes and businesses.

Therefore, all the information that is passed through the wireless network is unsecured, and others can easily decipher the data. However, data that is sent to and from a website that uses SSL encryption, indicated by the padlock in the lower-right corner of the web browser and a web address of https, is safe and secure.

User responsibilities

Even though you can take precautions to make your hotspot safer and more secure, it is up to the users to ensure their security.

Beware of the risks

The saying "Ignorance is bliss" might come back to haunt people who ignore the risks and issues of using unsecured wireless networks such as hotspots. Even if users do not follow all the advice to limit or eliminate the risks, they should at least educate themselves. Therefore, when it comes to the safety and security of using Wi-Fi hotspots, the main responsibility of users is to be aware of the issues, so that they can properly protect themselves.

Follow the safety and security tips

Hotspot users should follow any safety and security tips that you or others give them:

• Use VPN connections.
• Use secure (SSL) websites.
• Disable file sharing.
• Use personal firewall software.
• Keep an eye on valuables.

These items are discussed in the following sections.

Therefore, to protect your user's information, use SSL encryption on all applicable web pages, which secures the login or payment information. Most hotspot gateways have this feature.

In addition, if you are using a RADIUS server or a hosted solution, you should look into and understand the security measures taken to keep the user information safe.

Use VPN connections

If users are conducting sensitive business, such as checking unsecured POP3 e-mail accounts via hotspots, they should use VPN connections to encrypt the information. Many businesses provide this service to their employees to access the corporate network while away from the office.

Typically, VPNs securely connect remote networks or give people secure connections to a remote network. However, typical consumers can also use VPN connections to secure their hotspot experience. Even if your users do not intend to connect to remote networks, they might use VPNs because the information passed through the VPN tunnel is encrypted and secured from end to end.

Use secure (SSL) websites

When hotspot users are viewing sensitive information, such as web-based e-mail and banking information, they should ensure that the website is implementing SSL encryption on the website login page and during the entire sensitive session on the site. As discussed in a previous section, others cannot see the login and other information when SSL is in use.

Disable file sharing

Before people use public hotspots, they should ensure that their PC has no actively shared files, folders, or other services. The sharing features that operating systems provide today are useful when using private networks; however, this is not the case when on public networks.

Use a personal firewall

When using Internet connections, at home or on a public hotspot, users should use personal firewalls. Firewalls help prevent people from accessing your PC through the Internet. You can use operating systems, such as Windows XP, that have built-in firewall capabilities, or you can purchase software that provides the protection. Some hotspot-specific software solutions provide firewall features. You can also look into consumer software titles, such as ZoneAlarm from Zone Labs or Kerio's Personal Firewall.

Keep an eye on valuables

Users should keep an eye on their valuables while using public hotspots, or others will. Users should keep items such as their laptop, PDA, or briefcase with them at all times.

Summary

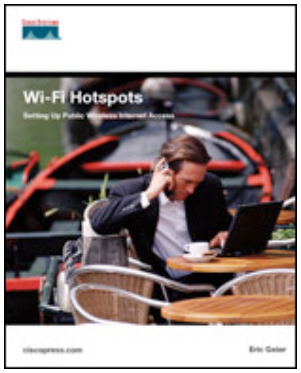
Given that Wi-Fi hotspots use the airwaves to transmit data and that they are used by the public creates many security issues. This article discussed ways to prevent and overcome many safety and security issues with public Wi-Fi hotspots.

Keep in mind the main concerns:

• Public Wi-Fi hotspots are inherently not secure. People who have the right tools can intercept the information that users send over the airwaves. However, users can take certain measures to protect themselves.
• Inform users of risks, and give them tips to stay safe and secure while using your public Wi-Fi hotspot.
• Enable features such as VPN Passthrough, client isolation, and web filtering to give users and yourself a safer hotspot experience.

Eric Geier is a computing and wireless networking author and consultant. He is a certified wireless network administrator (CWNA). He is an author of and contributor to several books and eLearning (CBT) courses.

This article is an excerpt from the Cisco Press book "Wi-Fi Hotspots: Setting Up Public Wireless Internet Access" and you can find out more about it at www.tinyurl.com/yt5kqo



WIRELESS SECURITY

6 CTOs, 10 burning questions!

Read the advice by experts from:

* AirDefense
* AirMagnet
* Aruba Networks
* AirTight Networks
* Fortress Technologies
* Trapeze Networks

Dr. Amit Sinha specializes in wireless communications and network security. Prior to joining AirDefense, he held various research positions at MIT, HP Laboratories, Intel and Texas Instruments. He is also the author of 15 patents dealing with different inventions in 802.11 infrastructure and wireless security. Amit received his S.M. and Ph.D. degrees in Electrical Engineering and Computer Science from MIT.

People use wireless networks on a daily basis and are growing concerned about the possible threats. What advice would you give to mobile users so that they could make and keep their laptops secure on any network?

Taking the following precautions significantly mitigates security risks associated with mobile wireless access:

1. Install a firewall.

2. Use hotspots only for internet surfing.

3. Enter passwords only into websites that include an SSL key on the bottom right.

4. Disable/remove the wireless card if you are not actively using the hotspot.

5. Ensure that your laptop is updated with the latest security patches.

6. Avoid hotspots where it is difficult to tell who's connected (hotels, airport clubs, conferences).

7. If the hotspot is not working properly, assume your password has been compromised, report to hotspot service provider and change your password at the next immediate opportunity.

8. Read all pop-up windows in their entirety.

9. Do not use insecure applications such as non-encrypted email or instant messaging while at hotspots.

10. Explicitly disable municipal Wi-Fi access from within the enterprise.

Despite the insecurities of 802.11, the number of wireless networks is growing rapidly. What should be done in order to raise awareness of wireless security problems?

There is significant user indifference to wireless security especially given the fact that radio frequency connections are not "visible". Enterprises should define and enforce explicit wireless access policies. Organizations should manage and enforce customized WLAN policies based on the desired security and acceptable uses for each WLAN device. In addition, on going user IT training should include wireless security sessions where users are exposed to the dangers of insecure wireless access, rogue devices, etc.

Security auditors can raise awareness by requiring strict compliance with emerging regulations such as the Payment Card Industry's Data Security Standard which is quite specific about wireless security requirements. Similarly strict adherence to other regulations such as HIPAA and SOX will also result in increased wireless security awareness. Further, enterprises should conduct frequent vulnerability assessments using wireless experts that comprehensively test wireless weaknesses and misconfiguration issues.

A significant part in the process of developing wireless networks is ensuring that the data located on wireless-enabled devices is secure. What do you see as the most prevalent threats to that security?

Today's mobile workforce is extending the edge of the enterprise network. Hotels, hotspots and other public access wireless networks are prime locations where hackers exploit wireless vulnerabilities to gain access into unprotected laptops. Following are some of the most prevalent threats:

1. Evil Twins & Wireless Phishing - An Evil Twin is an AP offering a wireless connection to the Internet pretending to be a trusted wireless network. The unsuspecting user sees the Evil Twin hotspot which looks identical to the legitimate public network the user logs on to every day. By presenting the user with a familiar scenario, such as a login page to a hotspot, the user will readily provide his or her username and password.

2. Automatic Networking - In addition to tricking an unsuspecting user into connecting to their laptop, hackers have the benefit of taking advantage of the increasingly wireless-friendly nature of the Windows XP and MAC OS X operating systems. Due to the self-deploying nature of wireless, a wireless laptop will continue to "probe" for APs it has been connected to in the past. These probes are easily picked up in the air by freely available wireless monitoring tools and tools such as Karma allow the hacker to become the exact network a user's laptop is looking for.

3. Wireless Driver Exploits - Several new Wi-Fi client driver based vulnerabilities have been revealed. These vulnerabilities typically exploit malformed management frames to run remote code on client machines.

4. Man-In-The-Middle Attacks - A man-in-the-middle attack is a type of attack where the user gets between the sender and receiver of information and sniffs any information being sent. In some cases users may be sending unencrypted data which means the man-in-the-middle can easily obtain any unencrypted information. In other cases, the attack could be used to break the encryption key.

5. Malware Injection - AirDefense has also identified several instances where unsuspecting wireless users received a fake web page with a mouse-activated web overlay. Any click of the user's mouse would trigger a download of harmful content, such as a virus or Trojan.

6. P2P Wireless - Ad-Hoc mode connections allow one wireless device to directly connect to another device. Default ad-hoc mode usually does not require authentication or encryption. This allows hackers to easily connect to an enterprise laptop without going through the more involved Evil Twin setup. Often mobile users leave their wireless card on when connecting to the enterprise wired network. This can result in an easy access wireless "bridge" into the wired network that circumvents firewalls and traditional wired perimeter security.

What are the biggest challenges related to the implementation of wireless LAN security policies for mobile users in the enterprise?

The biggest challenges related to the implementation of wireless LAN security policies are:

1. Flexibility – To accommodate enterprise specific policies. E.g., some enterprise want to enforce a no wireless policy while others might want to guarantee that all authorized users use WPA2. Some enterprises might want to allow access to certain hotspot and home networks only if the VPN is enabled. Having the ability to define and administer fine grained and enterprise specific policies is hard.

2. Scalability – WLAN monitoring and policy enforcement gets challenging when dealing with large organizations with hundreds of thousands of users and global presence.

3. Manageability – Many organizations feel overwhelmed by too much information and false positives that entail monitoring for policy compliance.

Passive discovery of wireless networks using wardriving tools may be unsettling but it is not technically illegal.

What's your take on wardrivers? Some say they're harmless while other label them as criminals.

Passive discovery of wireless networks using wardriving tools may be unsettling but it is not technically illegal. This would be similar to listening to someone standing at a street corner and shouting out random personal information. Trying to decrypt encrypted transmissions or intentionally interfering with someone else's WLAN is illegal. The act of wardriving per se is relatively harmless from an enterprise's perspective. However, it should serve as an early warning for them to beef up wireless security. If someone is doing a persistent wireless reconnaissance scan chances are they want to discover vulnerabilities and potentially exploit.

With the growing number of wireless users living outside urban areas, the last few years have seen a growth in the number of WiMAX deployments. What are the possible security risks associated with the deployment and usage of WiMAX technology?

The 802.16 standard is definitely more "carrier grade" than the original 802.11 standard and has a better security infrastructure. However, as with all standards, there exists vulnerabilities in 802.16. Several popular vulnerabilities of 802.11 (Wi-Fi) networks exist albeit to a lesser extent in WiMAX.

1. Rogue Base Station - This scenario is very similar to rogue/evil-twin Wi-Fi APs that broadcast credentials (MAC address, SSID, etc.) of a trusted or preferred network in an attempt to lure users into connecting to them. In WiMAX, every Subscriber Station (SS) requires strong authentication using X.509 digital certificates. This was done to prevent theft of service by unauthorized users. However, there is no such requirement for Base Stations (BS). This asymmetric treatment of BS and SS is very similar to many Wi-Fi implementations. The 802.16 standard makes no mention of BS authentication. As such, it would be easy to setup a rogue BS and trap authorized users to connect and reveal confidential information. It could also be used for DoS attacks where a SS shows strong signal strength and connection but no network access because it is connected to a rogue BS.

2. Denial of Service - All RF protocols are fundamentally vulnerable to DoS. With a strong enough jammer most wireless communications can be disrupted. While WiMAX uses sophisticated forward error correction codes and modulation techniques that are robust to interference, an intelligent jammer can disrupt a specific session without the need to brute force jam the whole medium.

The 802.16 MAC is contention free and uses scheduled transmissions. The BS broadcasts a UL-MAP frame that is available to all stations (authenticated or not) that determines who transmits when. An attacker can use the schedule information to inject valid frames (e.g. replayed frames) to disrupt a stations communication slot. Since the interference is completely "in-band" it is much more effective.

3. Management Frame Spoofing - The lack of authentication of powerful management frames in 802.11 resulted in popular DoS attacks such as de-authentication/dis-assocations attacks. Such attacks disrupt a wireless session between two nodes by injecting spoofed de-authentication/-dis-assocations messages by a third party pretending to be one of the communicating nodes. The 802.16 MAC has similar management frames (e.g. Reset and De/Re-register) that can force a subscriber station to disconnect and re-initialize. Unlike 802.11, these frames have cryptographic protections from spoofed identity. Authentication is achieved using a SHA-1 in the form of an HMAC digest computed using the message and a secret key. While the HMAC provides management frame protection, several MAC frames remain vulnerable to simple "replay" attacks. In a re-play attack, a valid frame transmission is captured and replayed. The presence of an HMAC requires that the message be replayed without any modification. Typically, frames use transient information such as serial number or a time-stamp to thwart replay attacks. IEEE 802.16 remains somewhat vulnerable to interference from brute force replay DoS attacks, because there is no mechanism in place to specifically detect and discard repeated packets. An attacker could repeat many messages (whether valid or not) in an attempt to interfere with the proper operation of the network. There are several ways in which the victim network might respond, depending on the exact content and timing of the replayed message.

4. Privacy and Key Management Issues - Several weaknesses in the PKM of 802.16 have also been revealed. All key negotiation and data encryption key generation rely on the Authorization Key's (AK) secret. The AK is generated by the BS. However, the standard has not described the AK's generation. Traffic Encryption Key (TEK) related problems have also been revealed. The TEK generated from the AK has only a 2-bit identifier space, which is insufficient during the AK lifetime. Further the TEK does not have any freshness assurance. The standard used DES-CBC for encryption. However, 56-bit DES is proved to be vulnerable.

Wireless hot spots, and especially rogue access points setup as hot spots to trick users, raise unique concerns for the mobile warrior. What can be done in order to mitigate the risks associated with their usage?

Wi-Phishing is the act of covertly setting up a wireless-enabled laptop or AP (such as an Evil Twin) but for the sole purpose of getting wireless laptops to associate and track keystrokes, allowing the hacker to capture passwords and credit card information. This concept is very similar to the email phishing scams, where a message is sent to users tricking them to enter confidential information, such as bank account information or other sensitive username and password combinations. The process of tricking someone to voluntarily provide confidential information has been used for years in a variety of forms and is generally referred to as “social engineering”.

Both WEP and WPA have its problems. Is it time to introduce a new wireless network security standard? If yes, what features should it have?

WEP is broken. WPA is better than WEP. However, WPA Pre-Shared Key can be cracked if you use small dictionary based passwords. WPA2-Enterprise based on IEEE 802.11i is secure. The current problems in WPA2 lie mostly around misconfigurations and implementation issues. WPA2 also does not currently address management and control frame authentication that is the basis of several types of masquerade and DoS attacks. Protection of some management frames is being addressed in IEEE 802.11w. However, rogue APs continue to be a big security gap not addressed by 802.11w. Further, 802.11w does not address control frames that can still be exploited for denial of service attacks. The problem with Wi-Fi security is that security was not designed into the original

standard. Standards based security patching will never completely solve the Wi-Fi security problem given backwards compatibility requirements and the proliferation of legacy networks.

Based on your experience, what advice would you give to organizations that are considering deploying wireless networks and increasing their mobile workforce?

Organizations planning wireless LAN rollouts should focus on each of the following 3 aspects:

1. Plan – Proper RF coverage and capacity planning using accurate simulation tools that factor in expected usage patterns and applications, propagation characteristics of building materials and future growth plans are important in maximizing the subsequent ROI from WLAN. Poor planning invariably results in recurring management and support costs.

2. Secure – Once APs are deployed, security configurations should be checked and properly applied. Usage policies for employees should be outlined and duely communicated.

3. Monitor – Once WLANs have been rolled out, monitoring the network 24x7 for security, policy compliance and WLAN health is required.

What are your predictions for the future when it comes to wireless security?

As we have seen in several high-profile recent data breaches, wireless is often the Achilles heel when it comes to network security. Wireless threats and attacks will continue to rise as hacking tools get more sophisticated and easy to use. As wireless networking proliferates, more and more data breaches and malware delivery will occur over the air. Organizations will realized that traditional wired security paradigms such as Firewalls and VPNs are not enough and a layered approach to security that incorporates wireless authentication and encryption along with wireless monitoring and intrusion prevention is critical for overall network security.

Prior to co-founding AirMagnet, Mr. Kuan was the first software engineer at Precept Software, where he developed IP multicast and IP video streaming technologies. His prior experience includes engineering design at Empirical Tools and Technologies and systems architecture at The Wollongong Group. Mr. Kuan holds a Bachelor of Science in Information Engineering from National Taiwan University and a Masters in Computer Science from Stanford University.

People use wireless networks on a daily basis and are growing concerned about the possible threats. What advice would you give to mobile users so that they could make and keep their laptops secure on any network?

Wireless users should be suspicious at all times, especially regarding those too-good-to-be-true service offerings. Here are a few good habits that might keep users out of trouble:

1. Turn on Personal Firewall or Windows Firewall in the Wireless Network Connection Properties. This will prevent unauthorized incoming connection attempts.

2. Turn off Internet Connection Sharing. If a mobile device's wireless security is compromised, this setting will limit the damage to the mobile device itself without spreading to the connected wire network.

3. Use 'on demand' instead of 'automatic' connection method for those wireless connection profiles without mutual authentication mechanism. Typically, those profiles are for hot spots (no encryption) or home usage (static WEP).

4. Never use 'ANY' as the SSID for any wireless connection profile. Mobile users should only connect to the SSID he or she knows is legit.

5. Never connect to known wireless network especially ad-hoc (peer-to-peer) networks.

6. Use wireless service with WPA2-Enterprise (802.1x) security whenever possible. Use WPA2-PSK at home where the 802.1x server is likely not available.

7. When using hot spot wireless services, avoid sending confidential information such as personal financials or company proprietary documents unless a VPN is used.

Despite the insecurities of 802.11, the number of wireless networks is growing rapidly. What should be done in order to raise awareness of wireless security problems?

As is often the case, education is key to raising awareness. However, industry wireless vendors and OS vendors hold the key to educating the masses about wireless security and best practices. Often times, security best practices are compromised in the name of ease-of-use or plug-and-play propaganda. People need to be informed of the risk they take when they cut corner or do not protect their wireless networks. Vendors need to take a leadership roll in ensuring that information is available. In addition, vendors need to provide solutions that are easier for the general public to deploy and use. It can be done with proper engineering.

A significant part in the process of developing wireless networks is ensuring that the data located on wireless-enabled devices is secure. What do you see as the most prevalent threats to that security?

Wireless devices are typically mobile devices such as laptop, voice handset, scanners, and etc. The most prevalent threat is the loss of those wireless mobile devices, which contain the credentials to join the wireless network and ultimately into the wired network. It is critical to ensure the security of the wired network threatened by the loss of wireless devices with credentials to enter the wired network. Such credentials stored on the wireless device allow the perpetrators to enter the wired network, and potentially even enterprise servers/ domains, without physically attaching to the wired network or even being on premise.

What are the biggest challenges related to the implementation of wireless LAN security policies for mobile users in the enterprise?

The biggest challenge resides in the natural paradox between information security policies and mobile user's wireless freedom and convenience.

Software products exist today to help enforce mobile user wireless policies, so implementation of security policies can be managed reasonably well.

The challenge however remains in the policies themselves. The most secure policy may call for wireless connection to the enterprise wireless network only, and nothing else. Such policy prohibits wireless connection to mobile user home wireless nets, hot spots, hospitality suites, etc. Obviously, this is not the most flexible and mobile user-friendly policy. Should enterprises compromise? The real world practice lies somewhere in between a strict and lax policy.

What's your take on wardrivers? Some say they're harmless while other label them as criminals.

Considering the percentage of insecure wireless networks (totally unencrypted, not even static WEP), wardrivers are the least of the problem. They do not make the already terrible security situation much worse at all. A hacker can already easily gather similar information with very primitive tools such as Netstumbler.

Why blame wardrivers? I see them as the messengers who are delivering the bad news. The wireless world would not be a more secure wireless world without wardrivers.

With the growing number of wireless users living outside urban areas, the last few years have seen a growth in the number of WiMAX deployments. What are the possible security risks associated with the deployment and usage of WiMAX technology?

Leveraging WiFi security standards and technologies, WiMAX started out with a much better security framework and authentication/ encryption algorithms.

A security flaw such as the static WEP in the WiFi world is not expected to take place in WiMAX any time soon. Secondly, WiMAX infrastructure and base stations are expected to be set up by WISP unlike Wi-Fi deployments, where less security-aware consumers and SMBs are heavily involved. Thirdly, WiMAX sniffing technologies has only been available to lab environments due to the extreme cost. Ordinary hackers are not likely to have access to such tool.

So, what are the security risks for WiMAX? Physical layer denial-of-service attack using RF jamming devices is the simplest one to conduct. There are also theoretical MAC (layer 2) denial-of-service attacks using unencrypted management frames. As WiMAX deployment takes place and CPE becomes more available, more risks may unfold.

Wireless hot spots, and especially rougue access points setup as hot spots to trick users, raise unique concerns for the mobile warrior. What can be done in order to mitigate the risks associated with their usage?

First of all, wireless connection profiles for hot spots on a mobile device should not be set to 'automatic' connect. Instead, use the 'on demand' option, which will prompt mobile user to confirm the wireless connection. The extra step may be a little inconvenient but may be the most effective to spot foul play. For example, a red flag should be raised immediately if the SSID for your home wireless network suddenly becomes available to you in your hotel room.

Road warrior should always be suspicious and cautious. Wireless phishing attacks, which impersonate wireless services and web sites, are difficult at times for mobile users to spot. As a general practice, mobile users should never send confidential information over unencrypted wireless networks.

Both WEP and WPA have its problems. Is it time to introduce a new wireless network security standard? If yes, what features should it have?

WPA2 addresses the problems in WEP and WPA. WPA2 is secure to the best of our knowledge. Security from a network security standard point of view, the next step is protected management frames. 802.11 today transmits management frames (AP beacons, client association requests, etc.) unencrypted. By spoofing management frames, wireless services can be easily interrupted, for example fake AP attack, de-authentication attacks, disassociation attacks, and etc. A new standard to authenticate and encrypt management frames will reduce the risk of such attacks.

Based on your experience, what advice would you give to organizations that are considering deploying wireless networks and increasing their mobile workforce?

First of all, use the highest security level possible. WPA2-enterprise (using 802.1x authentication server instead of pre-shared key) with AES encryption is the way to go. Secondly, define a secure, practical, and enforceable wireless policy for the wireless infrastructure and mobile devices. Lastly, monitor on wireless network according to the pre-defined policy on all possible aspects from security to performance and from layer 1 (RF spectrum) to layer 7 (voice application for example).

What are your predictions for the future when it comes to wireless security?

Wireless security standards and vendor products have caught up with the known vulnerabilities. It is true that low tech denial-of-service attacks such as RF jamming are still easy to conduct, but data security and wireless network penetration risks have been addressed by the IEEE standards and vendor products. This is by no means to say that wireless security is home free.

In the near future, the obvious security challenge is practically deploying these security technologies properly and timely. The economic impact of upgrading to the latest security technologies and the lack of IT expertise to implement the upgrade remain to be resolved. Further in the future, vulnerabilities against the current security and authentication/encryption algorithms may still be discovered by on-going research and the black hat community. That cat and mouse game will not stop in the wireless security arena.

Merwyn and members of the Office of the CTO drive Aruba's IPR, Standards, Federal, Security Vulnerability Assessment, Rapid Prototyping and long term technology strategy. Merv is an active and voting member of the IEEE 802.11 working groups. He has issued and filed numerous patents on wireless, security and high availability networking. Prior to Aruba, Mr. Andrade was a Wireless LAN technical leader at Cisco Systems. Mr. Andrade is an industrial electronics engineer from Bombay, India.

People use wireless networks on a daily basis and are growing concerned about the possible threats. What advice would you give to mobile users so that they could make and keep their laptops secure on any network?

With more focus on exploiting client-side wireless vulnerabilities, I tell customers and prospects to assume that anyone can connect to their workstations directly.

Attacks such as AP impersonation (so-called "evil twin") are difficult to mitigate with mobile users; the lack of lower-layer defenses (e.g. open networks) mandates stronger upper-layer security precautions.

Despite the insecurities of 802.11, the number of wireless networks is growing rapidly. What should be done in order to raise awareness of wireless security problems?

Educating security professionals as to the risks associated with different wireless networks is a significant contributor to helping people recognize and mitigate inherent wireless risks.

Projects such as the Wireless Vulnerabilities and Exploits (www.wve.org) database allow organizations to remain informed about wireless threats while supplying a reference source for wireless intrusion detection and vulnerability assessment tools.

A significant part in the process of developing wireless networks is ensuring that the data located on wireless-enabled devices is secure. What do you see as the most prevalent threats to that security?

The most prevalent threat to mobile devices is not high-tech or elite; it is simply lost or stolen devices. I was working with an organization recently who had deployed a handheld credit card processing system, using strong encryption for wireless traffic, but with a simple pre-shared key mirrored on all devices for authentication. With a handheld loss rate between 5 and 10%, each lost handheld network threatened all customer payment card data. Another emerging threat is Wireless telephony devices including dual-mode smart phones with saved pre-shared keys and/or credentials that allow unmitigated access to enterprise resources and significantly increase risk when lost or stolen.

Can handheld devices be exploited using zero-day and innovative techniques? Of course, we've seen that almost globally across devices with IEEE 802.11, Bluetooth and WiMax as potential attack surfaces. However, the more universal attack of theft with weak local data storage mechanisms represents a much more practical target.

My primary concern with WiMAX technology is that it was designed with the service provider's security interests as a priority.

What are the biggest challenges related to the implementation of wireless LAN security policies for mobile users in the enterprise?

The ubiquity of wireless networks is one of the biggest attractors to the adoption of the technology, but it is also one of the biggest security challenges. Organizations can take steps to protect their enterprise networks, but for many users, mobility extends beyond the organization's walls. Wireless access in hotspot locations, hotels and often home environments are inherently risky since the only network admission control is physical presence or payment for service. These challenges can be mitigated by secure wireless overlays that uniformly enforce and create "principle of least privilege" isolation via in-built firewalls, centralized device and user to poilcy enforcement point encryption and defense in depth through tightly integrated wireless intrusion prevention all whilst ensuring seamless mobility.

What's your take on wardrivers? Some say they're harmless while other label them as criminals.

I strongly believe that wardriving has significantly contributed to the steady growth in strong encryption and authentication methods needed to protect wireless networks. Kismet, while once a wardriving tool, has matured to the point where it is an indispensable part of a wireless toolkit for system administrators, auditors and pen-testers. Were it not for wardrivers, I believe more wireless networks would remain vulnerable today.

With the growing number of wireless users living outside urban areas, the last few years have seen a growth in the number of WiMAX deployments. What are the possible security risks associated with the deployment and usage of WiMAX technology?

My primary concern with WiMAX technology is that it was designed with the service provider's security interests as a priority. This is exemplified in the WiMAX Privacy Key Management (PKM) protocol, where significant expense is assumed to protect WiMAX providers from theft of service, but leaves consumers vulnerable to man-in-the-middle and base station impersonation attacks. While the IEEE 802.16e specification for WiMAX includes support for the Extensible Authentication Protocol (EAP), it is not a mandatory portion of the specification, and it is yet unclear as to how vendors will deploy WiMAX technology. This is especially disappointing, since the lack of mutual authentication was one of the early security lessons learned in IEEE 802.11 network evolution, but repeated with the development of WiMAX.

Wireless hot spots, and especially rogue access points setup as hot spots to trick users, raise unique concerns for the mobile warrior. What can be done in order to mitigate the risks associated with their usage?

When mobile users leverage open or even encrypted networks at hotspot locations, they need to remember that they are sharing the network with anyone else within range of their location.

A raised sense of awareness is necessary here, leveraging secure upper-layer protocols such as SSL/TLS, with careful attention to suspicious activity such as browser certificate warnings or the lack of SSL for web page authentication requests.

IPSec tunneling can be a useful countermeasure against the threats in hotspot locations. By initiating an IPSec tunneled connection to a corporate server with split-tunneling disabled, users can mitigate many common attacks.

Both WEP and WPA have its problems. Is it time to introduce a new wireless network security standard? If yes, what features should it have?

The known flaws in WPA/WPA2 have been limited to denial of service vulnerabilities, or weaknesses in authentication mechanisms meant for consumer networks. Both WPA and WPA2 represent significant improvements over the security provided by WEP, with WPA2 using CCMP representing the "gold standard" for strong encryption in wireless networks. Combined with a strong authentication mechanism, WPA and WPA2 are a formidable mechanism to protect wireless networks. I don't believe a replacement for WPA/WPA2 is warranted, since it solves the problem it was designed to solve.

Other vulnerabilities in wireless networks remain, which will require very different solutions. It is important however to not just rely on one technique to tighten wireless security since the end-points will naturally be very diverse and need multiple defense-in-depth techniques discussed earlier to offer compensating controls. A WPA2 EAP-TLS authenticating Laptop that forces you to perform multi-factor authentication needs to be treated and firewalled differently by the network v/s a WPA2 EAP-TLS authenticating smart phone with credentials pre-saved for ease-of-use.

Based on your experience, what advice would you give to organizations that are considering deploying wireless networks and increasing their mobile workforce?

Before organizations deploy or significantly grow their wireless networks, they should become familiar with the risks and challenges associated with wireless security. For some organizations, the risks associated with wireless technology will surpass the potential benefits. Other organizations may be willing to accept the risks to gain the rewards and benefits associated with mobile computing. Deploying wireless networks without understanding the risks and challenges may unnecessarily expose organizations.

What are your predictions for the future when it comes to wireless security?

The exploit targets of the future are embedded platforms. As more organizations leverage patch management technology, publicly released exploits have a shorter lifetime. Advancements in mitigating exploit vectors make it more difficult to reliably exploit common Windows targets.

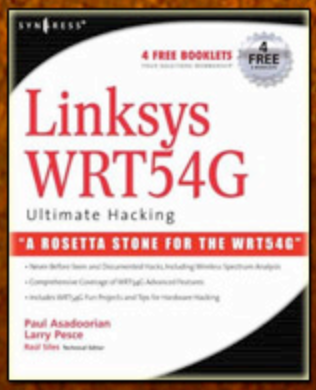
In contrast, embedded devices are often deployed without advanced security features, are seldom patched with any kind of regularity, and number in the billions of devices. Multiple vulnerabilities have been discovered on both access points and wireless client drivers ranging from denial of service conditions to full code execution attacks. With a widespread number a devices that can be exploited for network access and any traffic encryption keys, it seems likely this will be a new target for attackers.

Unfortunately, organizations cannot mitigate these vulnerabilities other than responding quickly to vendor security updates, and for selecting vendors who show expertise in a proactive security development life-cycle.

NO WIRES (IN)SECURE GIVEAWAY

// one grand prize, wireless hacking guaranteed! //

+



Linksys WRT54G
Wireless-G Router

Linksys WRT54G
Ultimate Hacking

Go to www.insecuremag.com/wireless to enter

The giveaway ends December 15th 2007.

Pravin is a wireless networking pioneer and an accomplished researcher with numerous patents to his credit. Recently he rolled-out a very large scale outdoor WLAN network connecting two cities in north India. He regularly serves on program committees of networking and wireless conferences. He is the Associate Editor of IEEE Transactions on Mobile Computing. Pravin has a B.Tech. in Computer Science from IIT Kanpur, India and an MS/PhD in computer science from the University of Maryland, College Park, USA.

People use wireless networks on a daily basis and are growing concerned about the possible threats. What advice would you give to mobile users so that they could make and keep their laptops secure on any network?

1. Use strong encryption and authentication protocols (such as WPA2) while using WiFi at work.

2. Exercise caution while using WiFi at public hotspots & home.

3. Use a VPN client – (highly recommended).

4. If you don't have a VPN client installed use SSL and avoid accessing valuable data over open (unencrypted) connections.

5. Avoid connecting to your preferred wireless network in locations where you don't expect it to be present. It could be a trap (or honey-pot) set up by a hacker. Communicating through a suspect wireless network is risky, unless you are using a VPN client to protect all communication.

6. Remove any peer to peer network connections from your wireless network connection profile.

7. Use strong password to protect access to your laptop. Don't keep sensitive data in shared folders.

8. Turn off your wireless card when not in use.

Despite the insecurities of 802.11, the number of wireless networks is growing rapidly. What should be done in order to raise awareness of wireless security problems?

• Perception that 802.11 is 'insecure' exists, but most users don't yet know how those 'insecurities' affect them. The extent of security exposure is also not fully understood.

• The nature and extent of wireless insecurity exposure is different at home, at work and at public hotspots. Likewise, threat scenarios are also different in each market segment (for example, retail, education, financial, government & Enterprise). More vertical market focused articles and presentations are needed so that end users can better appreciate how insecurities of 802.11 affect them directly.

• Ironically, a bad news often spreads faster. In the Internet space it took a couple of high profile breaches before everyone realized that a wired firewall was a necessity. The recent TJX wireless breach has already served as a wake-up call in PCI retail market segment. I sincerely hope that awareness spreads quickly before malicious users find new opportunities to make another news headline.

A significant part in the process of developing wireless networks is ensuring that the data located on wireless-enabled devices is secure. What do you see as the most prevalent threats to that security?

• Many wireless-enabled handhelds are still using WEP encryption to protect wireless transactions. Breaking WEP encryption is now considered a push-button exercise. Upgrading these devices to WPA or WPA2 is not always possible.

• Support for more secure protocols (for example, WPA & WPA2) is now available on laptops, yet many users continue to use WEP or no encryption at all at home and at work.

• Wireless medium offers an adversary direct layer 2 access to wireless-enabled devices. This level of access is often not possible in wired systems. The extent of exposure for the data stored on wireless-enabled devices is higher. Strong passwords must be used to protect data.

New means of detection and enforcement (such as Wireless IPS) are needed to implement wireless LAN security policies for mobile users. Yet, market acceptance has taken time.

What are the biggest challenges related to the implementation of wireless LAN security policies for mobile users in the enterprise?

New means of detection and enforcement (such as Wireless IPS) are needed to implement wireless LAN security policies for mobile users. Yet, market acceptance has taken time.

Myth #1: Personal firewalls, anti-virus and VPN clients can also protect mobile users from wireless threats. Most wireless attacks exploit vulnerabilities in wireless Layer 2. Neither firewalls, anti-virus nor VPN clients protect wireless Layer 2.

Myth #2: The existing wired side controls (firewalls, Network IDSs) are also adequate for monitoring wireless security policy violations and enforcing controls. In many scenarios traffic originating from and destined to mobile users does not even flow through the wired network. It is, therefore, not possible to enforce wireless LAN security policies using wired security systems.

The above two myths and the lack of wireless threat perception have been the two main barriers for implementation of wireless LAN security policies in the enterprise.

What's your take on wardrivers? Some say they're harmless while other label them as criminals.

Human eye can spot whether a physical door is locked or unlocked. Wireless is invisible and hence most users are unable to see whether their wireless doors are locked or unlocked.

Wardrivers are like people with night vision equipment. They are going around detecting which wireless doors are locked and which ones are unlocked. They are playing an important role in spreading awareness about wireless LAN security problems so that users can take necessary precautionary measures before any damage is done.

With the growing number of wireless users living outside urban areas, the last few years have seen a growth in the number of WiMAX deployments. What are the possible security risks associated with the deployment and usage of WiMAX technology?

On the client side threat scenarios for WiMAX will be somewhat similar to those for WiFi. A WiMAX client can act as a bridge between a public WiMAX network and a private enterprise network. It will be necessary to use a wireless connection manager agent on WiMAX clients to monitor and enforce policy decisions.

On the access point side, I expect a WiMAX base station to be owned, controlled and operated by a mobile carrier in licensed spectrum. Due to spectrum licensing issues, WiMAX base stations will grow in a controlled fashion. The threat of rogue WiMax base station may not be very high.

Wireless hot spots, and especially rogue access points setup as hot spots to trick users, raise unique concerns for the mobile warrior. What can be done in order to mitigate the risks associated with their usage?

There are two ways to solve this problem:

Client side solution
Freely downloadable wireless connection manager agents are available. These lightweight client agents can protect laptops users from rogue hotspot threats.

Infrastructure side solution
A hotspot provider can install a WIPS (wireless intrusion prevention system).

Deploying a wireless network is a more complex task than rolling out a wired network, yet the effort required is well worth it.

Both WEP and WPA have its problems. Is it time to introduce a new wireless network security standard? If yes, what features should it have?

Both WEP and WPA have its problems but WPA2 is relatively secure (there are no obvious flaws reported as yet). The industry does not need a yet another new standard for security. What is instead needed is more education on how to correctly configure and use WPA2.

Based on your experience, what advice would you give to organizations that are considering deploying wireless networks and increasing their mobile workforce?

Deploying a wireless network is a more complex task than rolling out a wired network, yet the effort required is well worth it. It has been proven beyond doubt that wireless access provides productivity growth and infrastructure cost reduction.

To maximize benefits, a wireless network must be properly planned, deployed, monitored and secured. The best results are achieved when a wireless infrastructure is rolled out in conjunction with an overlay wireless intrusion prevention system. Wi-Fi infrastructure provides 24x7 mobile access while WIPS ensure secure and uninterrupted access for all mobile users.

What are your predictions for the future when it comes to wireless security?

More and more security features will be embedded inside Wi-Fi infrastructure offerings, yet need for a dedicated wireless overlay security will continue in ‘high security’ market segments.

The complexity and cost of deploying, configuring and managing wireless security will continue to reduce. This will alleviate ‘insecurity’ fears and lead to ubiquitous deployment of wireless.

Prior to joining Fortress Technologies, Barsoum was a Principal Architect with EZchip Technologies and the Principal Systems Architect at Quarry Technologies. Barsoum has also held engineering positions working on DSLAMs at both US Robotics and 3Com. He holds a B.Sc. and M.S. from Worcester Polytechnic Institute, an MA from Brandeis University, and has earned credit towards the completion of a Ph.D. as a Guggenheim Fellow at California Institute of Technology.

People use wireless networks on a daily basis and are growing concerned about the possible threats. What advice would you give to mobile users so that they could make and keep their laptops secure on any network?

Wi-Fi security has come a long way since the days of WEP. For the road warrior, there is a multitude of threats that are independent such as rogue APs, physical loss of the device, and weak passwords. To keep the laptops secure, at a minimum, we recommend the use of a personal firewall combined with encryption of the hard drive contents and a VPN to access the corporate data. A personal wireless intrusion detection solution can also be beneficial. An additional concern is the use of Internet applications that send unencrypted data with POP and SMTP as the biggest culprits. Mobile users should only use SSL-secured versions of these applications.

Despite the insecurities of 802.11, the number of wireless networks is growing rapidly. What should be done in order to raise awareness of wireless security problems?

Both WEP and wardrivers have done a tremendous job improving the awareness levels of the user community. This level of awareness has brought tremendous pressure on the vendors and the standards committees to bring products to the market with a much higher level of security. We live in an open society where innovation fuels the efforts of security researchers and vendors.

A significant part in the process of developing wireless networks is ensuring that the data located on wireless-enabled devices is secure. What do you see as the most prevalent threats to that security?

There are two main threats for the wireless-enabled devices. These are rogue APs and loss of the device. With the physical size of mobile devices shrinking and their data capacity increasing rapidly, the impact of losing a device can be a real threat. We feel that encryption of the content stored on the wireless device is an absolute necessity. Decryption should require user authentication. In addition, the ability to disable the device from accessing the network and remotely *zeroizing* the contents is very important.

What are the biggest challenges related to the implementation of wireless LAN security policies for mobile users in the enterprise?

Not surprisingly, human factors are the biggest challenges to implementing a WLAN policy. Humans are typically, the weakest link in the chain. Humans select weak passwords, weak PSKs, and disable security software. The trick is to be realistic about defining the set of security threats and outlining a set of steps to defend against these threats. Under-defending clearly leaves ample room for vulnerabilities to be exploited. On the flip side, an over-zealous security policy alienates the user base which ends up avoiding or turning off these security mechanisms.

In general, a balanced approach to security works best. I like security tools that don't get in the way, that operate seamlessly and make it easier for the user to do the right thing vs. the wrong thing. For instance, in our products, we have a mechanism to generate a truly random number to be used for as a PSK, instead of relying on the user to come up with a random number. Another mechanism we use extensively is what we call a "device ID". This is an ID that is cryptographically tied to a particular device. If the device is ever lost or stolen, the administrator can simply disable the device's ability to access the network, even of the user's password is compromised. These kinds of mechanisms go a long way to creating an effective security policy.

Humans select weak passwords, weak PSKs, and disable security software.

What's your take on wardrivers? Some say they're harmless while other label them as criminals.

Wardrivers raise the level of awareness to the common problem of unprotected Wi-Fi access points. I think that in general they provide a service to the community. One needs to realize that the vulnerabilities are there. Wardrivers are just shining the light on them.

With the growing number of wireless users living outside urban areas, the last few years have seen a growth in the number of WiMAX deployments. What are the possible security risks associated with the deployment and usage of WiMAX technology?

The security model in WiMAX (802.16d) mirrors that that of DOCSIS Cable Model standard. Both of these models are protecting against theft of service primarily. WiMAX (802.16d) provides for only one way authentication (BS authenticates the SS) using a device-specific certificate. In general, this model is adequate for a broadband device sitting outside the firewall (where a cable modem sits today). There are some parts of the standard that are less than ideal. For instance, only the AP contributes randomness (via a nonce) to the key mixing process. This is not adequate in the case where a higher level of assurance is desired. Also, like Wi-Fi, the management messages are neither encrypted, nor authenticated. This presents a set of challenges mostly around protection against DOS type attacks. We think WiMAX (802.16d) security level is adequate for consumer broadband applications. For high assurance environments, there are serious shortcoming such as one-way-authentication (susceptibility to rogue APs), key mixing issues, and lack of user authentication. These present real challenges for our customers.

Wireless hot spots, and especially rogue access points setup as hot spots to trick users, raise unique concerns for the mobile warrior. What can be done in order to mitigate the risks associated with their usage?

Mitigating these risks requires a security implementation with multiple defense elements. These elements include personal firewalls, strong VPN security. The addition of a personal wireless intrusion detection system simplifies the implementation of a corporate policy for wireless network access.

Both WEP and WPA have its problems. Is it time to introduce a new wireless network security standard? If yes, what features should it have?

WEP obviously was a poorly designed implementation based on an OK (not great) cipher, namely RC4. WPA addresses some of these shortcomings within the limitations of RC4. WPA2 is built on AES and is much stronger. WPA2 comes in two flavors: personal and enterprise. Personal mode uses a pre-shared key, while enterprise mode relies on 802.1x authentication.

We believe WPA2 is secure. Whatever weaknesses that may exist are related to the actual implementation and choice of mode or EAP type. For instance, in PSK mode, the entire level of security hinges on the strength of the PSK used. Since most people, use fairly weak pass phrases, the resultant security level is, in most cases, much less that what AES offers. In Enterprise mode, WPA2 relies on the strength of the EAP type used. EAP-TLS provide a very high level of security. Unfortunately, EAP-TLS requires a PKI infrastructure which most enterprises are less than eager to invest in.

Separately from protecting the user data, it is also important to protect the management channel, which today is neither encrypted nor authenticated. 802.11w, when ratified will encrypt the management channel to provide protection against a number of attacks.

Based on your experience, what advice would you give to organizations that are considering deploying wireless networks and increasing their mobile workforce?

I believe the most important thing for an organization to do, is a proper threat analysis for the proposed usage model. We recommend strong AES-based encryption both on the WLAN as well as a WIDS solution. For the mobile handheld, we recommend an AES-based encryption for the both the WLAN and the VPN solutions. We also recommend hard drive (or flash) encryption as well as mechanism to erase the device or render it unusable if it is lost or stolen.

What are your predictions for the future when it comes to wireless security?

The use of AES and a solid cryptographic design has improved the security of Wi-Fi tremendously. This is leading to broad adoption of the technology. Over the next few years, the focus is likely to turn to securing the management channel of the various wireless technologies. This is starting to take shape already with 802.11w and we expect similar efforts for 802.16.

Before Trapeze, Dan Simone worked at several prominent companies. At Bay Networks (now Nortel Networks), he drove the development of hubs, switches and net management products. At Motorola, he headed up design, installation and management of the corporate LAN. Dan co-authored the point-to-point protocol over Ethernet (PPPoE) and holds several patents.

People use wireless networks on a daily basis and are growing concerned about the possible threats. What advice would you give to mobile users so that they could make and keep their laptops secure on any network?

As a mobile user, there are several things that can be done. First, use the personal firewall that is bundled with most current laptops. This will limit the traffic that makes it past your network adaptor to other services on your laptop. Second, always use some form of encryption when sending sensitive data. For most individuals, this means making sure there is secure link between their web browser and the site they are communicating with. You can usually tell this is the case when you see the "lock" symbol in your browser. Is it also a good idea to disable any services you are not using on your laptop that allow outside communications. These can invite trouble. For example, turn off your Wi-Fi radio in your laptop in a public place if you're not using it. Lastly, if you are a home wireless user, be sure to enable the encryption that came with your AP. Even if the only option available to you is static WEP, this is better encryption than none at all and often enough to make the casual hacker look elsewhere. Naturally, where possible, use WPA or WPA2 as that protection of far stronger than WEP, which does have technical flaws. Every device that has been Wi-Fi Certified since the fall of 2003 includes at least WPA.

Despite the insecurities of 802.11, the number of wireless networks is growing rapidly. What should be done in order to raise awareness of wireless security problems?

The biggest issue is simply a lack of knowledge of the various techniques that can be

used to protect wireless communications and perhaps more importantly, a willingness to be sure to use them at all times. Because this has been such a fundamental issue from day one, a lot of attention has been given to wireless security. Today, it is possible to build extremely secure wireless networks if the proper steps are taken. Unfortunately, users have been known to get lazy when it comes to security and don't expect that they may be the subject of an attack. In a business setting, professional IT staff should surely be aware that the Wi-Fi network needs to be secured. In a home environment, the end user needs to become aware that the product out of the box typically is in a mode with encryption off. They then need to proactively turn encryption on.

A significant part in the process of developing wireless networks is ensuring that the data located on wireless-enabled devices is secure. What do you see as the most prevalent threats to that security?

The most effective means of attack involve stolen or lost devices and/or social attacks. The threat of a lost laptop is by far a greater threat to corporate and personal security than over the air attacks. This is particularly true when the proper authentication and encryption is in place within the wireless infrastructure. A stolen laptop typically provides much useful data directly. If it doesn't, often passwords and usernames are stored within the system making access to the data far easier. Unfortunately, this is not really a wireless problem but a mobile computing problem in general that must be addressed through means that are independent of the network access method. Some examples of solutions in the marketplace that can help are strong laptop passwords, log on methods that include biometrics or tokens with changing PINs, and even hard drives that automatically encrypt themselves in the event they are removed from the laptop.

What are the biggest challenges related to the implementation of wireless LAN security policies for mobile users in the enterprise?

There are primarily two major roadblocks. The first and biggest is the availability of proper security protocol support by all the enterprise's client devices. For example, WPA2 and EAP-TLS are well known and widely supported encryption and authentication protocols. All enterprise class suppliers of wireless LANs support these protocols. However, many end user devices do not. For example, a retail store may have scanners that were purchased years ago and support static WEP at best and no strong authentication. This represents a major hole in any secure deployment. Enterprises must insist that all their client devices support the full 802.11i standard and are WPA2-Enterprise certified.

The second largest problem is authentication. The Enterprise must first select one or more protocols that are supported by its end devices, then create the appropriate database and possible PKI environment to support it. The creation and maintenance of this database is a necessary evil to deploying a world class secure WLAN. In addition, the various authentication protocols have support for various features such as key distribution, fast roaming, two-way vs. one-way authentication, etc. that can make the selection of a the proper protocols a difficult and potentially confusing tradeoff. However, standardizing on one of the strong methods backed by the Wi-Fi Alliance as part of WPA2 testing such as EAP-TLS, PEAP-GTC, or PEAP-MSCHAPv2 is a good start.

What's your take on wardrivers? Some say they're harmless while other label them as criminals.

Whenever a valuable service is being provided for free, it will attract a crowd! This should not be a surprise to anyone. The easiest way to stop wardrivers is to always make sure that your wireless network is secure.

Even some of the least expensive APs on the consumer market come with fairly simple and sophisticated ways to secure them, for example, WPA. Most wardrivers will move right on to the next AP once they see that the network is protected by WPA or WPA2. That said, even for a wide open network, connecting to a network that isn't yours is plain and simply theft of service. However, if those installing the wireless network are not taking any steps to indicate the network is private or any steps to secure the network, they have no one to blame but themselves for the theft.

*** With the growing number of wireless users living outside urban areas, the last few years have seen a growth in the number of WiMAX deployments. What are the possible security risks associated with the deployment and usage of WiMAX technology?**

Most of the early deployments of WiMAX have been as last mile replacement for cable modems, DSL, or T-1 lines. Security issues associated with this application of WiMAX are no different than any time you are sending sensitive data across the public internet. End to end encryption of some sort (e.g. SSL or IPSEC) must be used. As WiMAX applications continue to grow and we see increasing numbers of WiMAX client devices, all of the same issues for which Wi-Fi had to find solutions will exist. Luckily, solutions such as 802.1X, AES encryption, and other technologies are largely independent of the underlying MAC layer, e.g., 802.11 or 802.16 technology. WiMAX has the advantage of being able to learn from some of the early mistakes in the Wi-Fi market.

Wireless hot spots, and especially rogue access points setup as hot spots to trick users, raise unique concerns for the mobile warrior. What can be done in order to mitigate the risks associated with their usage?

Users of hot spots and mobile users in general should put pressure on their providers or corporations to deploy the necessary security features required to address this problem. Technical solutions, such as VPN's with mutual authentication, exist. Also, within the IEEE's 802.11 working groups, new extensions to the 802.11 standard are bring developed to secure over the air control and management messages. This will further help to identify and contain rogue devices.

Both WEP and WPA have its problems. Is it time to introduce a new wireless network security standard? If yes, what features should it have?

We already have a standard network security solution that is backed by the IEEE, National Institute of Standards and Technology (NIST) and the Department of Defense. It is call 802.11i. Within this standard, if users insist on 802.1X authentication with AES encryption, they can be assured they are running top commercial quality algorithms that have no known attacks. The Wi-Fi Alliance also certifies a version of this called WPA2. There are no documented hacks of properly configured WPA2 systems, or WPA systems for that matter. Customers should insist on WPA2-Enterprise capabilities in all their client devices as well as their wireless infrastructure if security is important to them.

Based on your experience, what advice would you give to organizations that are considering deploying wireless networks and increasing their mobile workforce?

Wireless networks have a tremendous ability to improve productivity, enable a whole new class of applications, and change the way organizations think about access to data. This is much like the change we experienced with the introduction of the Web. Organizations should insist on a wireless infrastructure that scales, has sophisticated yet easy to use centralized management, and adheres to all of the latest security standards. The industry made a significant change over the past several years moving away from standalone access points to APs that are "thin" or centrally controlled. More recently, this approach has been improved further with hybrid architectures that are centrally managed while still utilizing the AP for the heavy lifting of traffic forwarding and encryption. This has lead to more sophisticated services, more consistent services and security policies, and better scalability all while achieving lower cost of ownership. For organizations that expect to deploy more than even a few APs, this is the architecture of choice today among leading enterprises.

What are your predictions for the future when it comes to wireless security?

Mobility is one of the few services that end users have consistently been willing to pay for. The cellular phone is a great example. We willingly gave up a "5 9's" reliability and consistently clear communications for a higher priced service that could deliver neither. Why? Because it is mobile and we value mobility over everything else. In the future, if your applications, equipment, and infrastructure does not support wireless, it will be obsolete.

o3: magazine

Open Source / Enterprise
Free DIGITAL magazine

http://www.o3magazine.com