[IN]SECURE

OPEN. INFORMATIVE. TO THE POINT. Issue 7 - June 2006

SECURITY FROM DIFFERENT PERSPECTIVES

TABLE OF CONTENTS

Summer is approaching and the thought of working in a cubicle worried about the next possible attack on you network is less appealing by the day. Take this issue of (IN)SECURE and relax, there's plenty of interesting material.

The past few months have been very busy. Besides releasing a new version of Help Net Security (www.net-security.org) with a new identity, we also attended two major IT security conferences - InfoSec World in Orlando (Florida, USA) and Infosecurity 2006 in Lodon (UK). We've met interesting people and prepared some interviews and podcasts. You can find photos and news from both events in this issue.

Have a great summer and drop me a line with comments, they are always welcome.

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

McAfee Total Protection released

McAfee unveiled McAfee Total Protection. As the company says, it is the industry's first and only offering to combine and manage all the elements of a comprehensive system security solution through a single console and agent platform. McAfee Total Protection is a single concept with four distinct offerings for customers of all sizes and needs. For the first time, these customers can purchase a single solution that is tightly integrated into a single console. The end result is increased security, policy compliance and significant ongoing cost savings. McAfee Total Protection for enterprise includes anti-virus for all tiers of the network, anti-spyware, anti-spam, desktop firewall, host intrusion prevention and a complete network access control system—all managed by a single console. More information can be found at www.mcafeeasap.com

Secure Computing announces SafeWord PremierAccess 4.0

Secure Computing Corporation announced the availability of SafeWord PremierAccess 4.0 offering tight integration with Microsoft Active Directory and a perfect fit for companies who want to adopt identity and access management using their existing Microsoft Windows infrastructure. With tight integration to Microsoft Active Directory, SafeWord PremierAccess 4.0 is designed to work especially well in Windows environments. Companies can plug PremierAccess into their existing Active Directory infrastructure and instantly administer strong authentication using the Microsoft tools that they already use and know. This allows them to meet their obligations to provide secure access to data with the least impact on cost. More information can be found at www.securecomputing.com/

Test and crash beta Version of BitDefender 10 Internet Security

BitDefender is inviting the public to take their best shot at testing and crashing BitDefender 10 Internet Security Beta, the company's upcoming flagship suite of perimeter security products. Among the prizes to be awarded to the most thorough beta testers will be a fully-paid trip to Romania to meet BitDefender's development team, a laptop computer, 10 MP3 players, as well as 100 free copies and 1,000 discounts to the full version of BitDefender 10 Internet Security suite.

Available in the second half of 2006, the full version of BitDefender's award-winning Internet Security suite will offer many new enhancements and capabilities, including a powerful new rootkit detector, HTTP traffic scanning capabilities, and a privacy protection module for preventing sensitive information from being accessed and send without user consent. More information can be found at beta.bitdefender.com

Key trends for spam in first quarter 2006

Using SurfControl's Adaptive Threat Intelligence (ATI), SurfControl's Global Threat Experts have compiled threat trend data for the first quarter of 2006. In the first quarter of 2006, threat experts found that product and services-related spam has shown consistent growth of 16 percent month over month. The increase is partly attributable to Russian and Chinese coverage, where spam can be more generic, such as training courses, shopping and forum sites. This double-digit growth was also seen with phishing and fraud spam attacks. Additionally, there was a significant rise in the amount of pharmaceutical and finance-related spam, together representing 80 percent of spam volume. Stock tip embedded spam is still the most prevalent type of spam, claiming 40 percent of all financial spam, with 1,200,000 instances discovered in March 2006 alone. Embedded spam is defined as when the entire message is contained within a graphic, and has no extraneous text.

Non-conventional defence against phishing

IntelligenceFocus™
non-conventional intelligence solutions

IntelligenceFocus has released a new generation of security appliances able to convert traditional internet networks into phishing-immune networks. Proprietary DigiProbe appliances provide a unique combination of server-side intelligence analysis with network flows understanding and desktop compliance, analyzing digital contents and usage behaviours to prevent criminal activities and enforce regulatory compliance.

A first prototype infrastructure was deployed at a major European financial institution, where it successfully intercepted and blocked all phishing campaigns – and generated no false alarms. DigiProbe was implemented in a cross-continent back-end infrastructure, stressed with more than 2,000 historical phishing campaigns, simulating the defence of thousands of web users and over 300 companies, including more than 100 banks and other financial and e-commerce institutions with global presence. This resulted in an extreme fine-tuning of DigiProbe appliances on real-life cases and tremendous anti-phishing performance, close to 99% fraud detection and prevention. More information at www.intelligencefocus.com

First secure LAN Switch announced

ConSentry Networks, a leading provider of secure LAN solutions announced the LANShield Switch, an enterprise-class switch that integrates the security features needed to secure every user and every port on the LAN. With this announcement, ConSentry is leading the migration of security from an overlay to an embedded technology in the LAN. By delivering its LANShield silicon architecture and security software initially in the LANShield Controller (formerly the Secure LAN Controller), ConSentry was able to focus on refining the security functions and to prove out the LANShield architecture in a platform that integrates easily into customers existing infrastructure. The Network Admission Control (NAC), visibility, user access control, and threat control capabilities of the LANShield silicon constitute the foundation of the LANShield product family. More information can be found at www.consentry.com

Web based risk and compliance management service released

RiskComp Ltd. announced the launch of the World's first fully managed Web based Risk and Compliance Management Service. This Service provides the ability for Organizations of all sectors and sizes to introduce an Information Security Risk Management programme across their entire Organization without the need to install, support and maintain any software on the desktop, or employ expensive Consultants to "re-invent the wheel". The RiskComp Managed Service uses an Expertise based questionnaire driven approach, and is launching with an Information Risk Management Expertise, and an ISO 17799 Compliance Management Expertise. These provide everything necessary to both assess AND manage the Information Security and Operational risks of an Organization, and assess compliance against the ISO/IEC 17799:2005 Code of Practice for Information Security. More information can be found at www.riskcomp.com

NetContinuum launches NC-1100 Web application firewall and gateway

NetContinuum introduced the next generation NC-1100 Web Application Firewall (NC-1100 AF) and the Application Gateway (NC-1100 AG). The NC-1100 product line aims to establish the application proxy as an architectural best practice in the data center with 10X the performance and 10X the ease of deployment and management of previous generation application proxies. Application proxies provide comprehensive application assurance services to data center teams: securing the web applications from professional hackers and their methods, accelerating the user experience through caching, compression and connection pooling, and increasing application availability through load balancing and application health checks. The comprehensive application assurance feature set is delivered from a single point of control. The NC-1100's GUI offers up a very simple but comprehensive "Application Dashboard" that provides a single console view on all aspects of application assurance: application availability, application performance, and application security. The NC-1100 makes management even easier by providing a unique "Front-End health-check" capability to failover from one system to the other at the application level with application persistence. More information can be found at www.netcontinuum.com

SSH port forwarding: security from two perspectives, part one

By Andrew J. Bennieston and Liam A. Fishwick

SSH is the Secure Shell, a suite of applications which replace the UNIX rsh (remote shell) and, in many cases, telnet, offering security and many more features. SSH operates with a client-server architecture; that is, an SSH client connects into an SSH server on a remote system in order to achieve some goal, usually presenting the client user with a UNIX shell, through which they may interact with the remote (server) system.

Often, a single system will contain both an SSH client and an SSH server, allowing full two-way connections. That is, if you're sitting at computer A you can connect via SSH ("ssh into") computer B, which is running an SSH server. On the other hand, if an SSH server is also running on computer A, and you're sitting at computer B, you can ssh into A and run commands on that system. Clearly, this makes network server and workstation administration easy, as you can simply connect remotely into the computer you need to work on, and run commands through the SSH session.

But SSH provides far more than this. SSH is a protocol which establishes a secure (encrypted, authenticated and integrity-checked) connection between two computers. This connection may have multiple channels, and each channel may be used to route network traffic of any kind. This is known as tunnelling, and is an incredibly powerful feature of SSH.

Indeed, most SSH products include programs for a particular use of the SSH connection: for example, the scp and sftp clients, both of which copy files across a network by tunnelling their data transfers through SSH. scp is equivalent to the UNIX cp command, but allows the source or destination (or both!) to refer to a remote computer. The sftp program is an alternative to scp, with an FTP-like interface. sftp generally uses scp internally, however, rather than implementing the full FTP protocol over SSH.

This article looks at some of the more complex port-forwarding applications of SSH, and discusses these applications from the perspectives of flexibility and security. With flexibility, of course, comes a degree of insecurity. In this article we attempt to show that the flexibility of SSH should not be sacrificed entirely, but that SSH servers on internal, secure, networks should be running configurations which have been locked down, and that outbound SSH access should be tightly controlled on such secure networks.

Basic Port Forwarding

The basic port forwarding provided by SSH is to forward local ports to a remote destination. This means that ssh (the SSH client) listens on a local port and forwards (tunnels) connections on this port to a remote server, via the SSH connection. The remote endpoint can be on the computer running the SSH server (sshd) or can be any system reachable from that computer. Note, however, that the encrypted part of the connection only goes as far as the computer running the sshd into which you are connected. Furthermore, it is possible to configure the client to act as a gateway, accepting connections from any host that has access to it, thus creating a 4-point connection (Figure 2.1).

In this example the encrypted traffic is only between 10.0.0.6 and 192.168.0.5 even though the data itself does not originate at these machines.

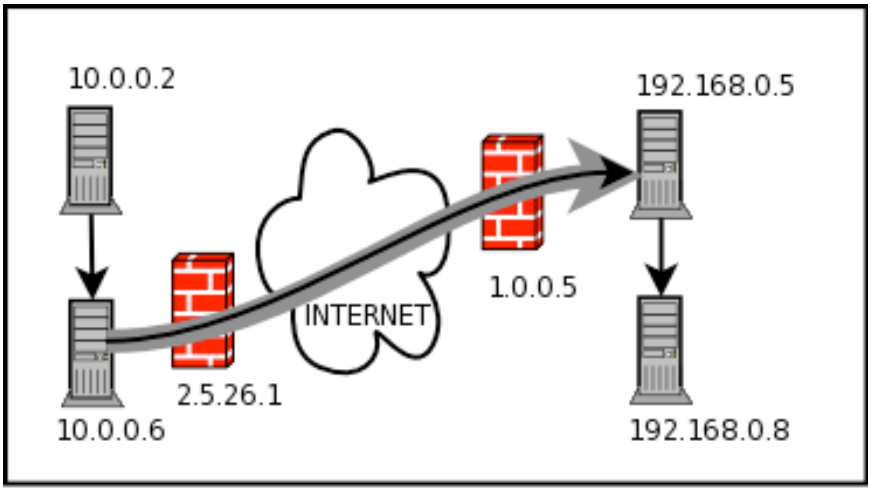


Fig. 2.1

In this scenario, we have a network with a public IP address of 2.5.26.1, and a network with a public IP address of 1.0.0.5 (We are using 1.X.X.X and 2.X.X.X as these are reserved ranges and so should not be in live use on the real Internet). Each network has computers behind a firewall performing NAT (Network Address Translation), numbered using the private IP address ranges 10.0.0.0/8 and 192.168.0.0/16, respectively.

For this discussion, we'll assume that an SSH server is running on host 192.168.0.5, that port 22 (SSH) is forwarded through the firewall at 1.0.0.5 to this host, and that outbound connections to port 22 are allowed through the firewall at 2.5.26.1.

As an illustration of the SSH forwarding capabilities, we will assume that a user on 10.0.0.6 ran the following command from a bash shell.

```
ssh -g -L 6667:192.168.0.8:6667 user@1.0.0.5
```

This logs the user into the SSH server at 1.0.0.5, which is actually forwarded by the firewall to host 192.168.0.5. The -L part specifies that the ssh client should listen on port 6667 on 10.0.0.6 for connections, and forward those to 192.168.0.8 on port 6667. Port 6667 is commonly used for IRC (Internet Relay Chat). The address 192.168.0.8 is not accessible to 10.0.0.6, as it is not on the same network, and is not routable over the Internet, but this does not matter as the resolution of the remote endpoint for the tunnel is performed on the system running the SSH server, not the client. The server is on the same network as 192.168.0.8, and so this connection succeeds. The -g tells ssh to allow connections from remote hosts (by default, an ssh client listening on a local port will only accept connections from the local host). The grey arrow in figure 2.1 shows the SSH connection between the client and the server.

Using this setup, a user on 10.0.0.2 may point their IRC client to 10.0.0.6 port 6667, and their connection will be forwarded through the encrypted SSH tunnel to the remote IRC server on 192.168.0.8.

The firewalls at both sites do not need changing to allow this to happen, neither site need allow any traffic at all on port 6667 through their firewall, as the entire IRC connection is tunnelled through the SSH connection - which normally is on port 22, meaning that only port 22 will need to be allowed through from each host. This connects with encryption, authentication and integrity checking performed by SSH between the client and server. The encryption occurs only through the SSH tunnel, however. The connections between 10.0.0.2 and 10.0.0.6, and between 192.168.0.5 and 192.168.0.8 are not encrypted as they are beyond the endpoints of the SSH tunnel.

In this way, it is possible to operate a network which limits incoming traffic to established connections, and inbound connection requests to SSH, without limiting connectivity for remote users. For instance, if you have an internal mail server, but wish to allow traveling users to connect into it, you do not need to open ports on your firewall to allow mail connections, you can simply have the user set up an SSH tunnel, via the SSH server, and connect using that. This has the added benefit of only allowing those with a valid SSH username and password to connect inside the network.

Of course, this security comes at the price of user convenience. It is much easier for a user to simply open a mail client than it is for them to set up an SSH tunnel and then configure their mail client to use this, instead of connecting directly to the remote mail server.

Remote Port Forwarding

Mirroring the local forwarding features discussed above, SSH provides remote port forwarding. In this case, the SSH server listens for connections on a port (on the server computer) and forwards connections on it to a designated local port (that is, a port on the client system). In this way, you can allow inbound access to services on a local host. In order to do this you would use the -R option, which has the same syntax as the -L option for local port forwarding, but the first port number specifies the port the server listens on, the address in the middle is resolved locally (and can be localhost, 127.0.0.1), and the final port is the port to connect to on the address specified.

For an example, we'll have an enterprising user who wishes to run a small personal web server on his office computer. Unfortunately for him, the company firewall blocks access to port 80, except to the main corporate web server, but outbound SSH connections are allowed anywhere.

This user has an account on an SSH server which is outside of the company firewall, so all he would need to do is run:

```
ssh -R 10080:127.0.0.1:80 user@host
```

All that remains is for our enterprising user to tell his friends to connect to host:10080 to access his webserver, and the connections will be forwarded back through the firewall (inside an encrypted SSH tunnel) to the system running the real web server.

The forwarding is transparent to web clients (though virtual hosting, and similar setups, on the web server may be broken as the client address is different to the server address).

It is, of course, possible to set up remote forwarding with an endpoint which is not localhost. This is similar in form to figure 2.1, but with the direction of the connections reversed! Note again, that in this situation the encryption, authentication and integrity-checking are performed only over the SSH connection, between the ssh client and the sshd server. The endpoint connections are not encrypted unless they are also tunnelled through SSH (or another technology such as SSL/TLS or IPSec is used!)

Dynamic Port Forwarding

In the previous situation, a single local port was forwarded to a single remote endpoint, through the encrypted SSH channel. This works for connections to a single service, and even works for connections to an individual website. But if you want to follow a link off that site, or connect to other services, you would need to add another static forwarding rule to the connection. As an example, we will look at the use of BitTorrent, a peer-to-peer file distribution protocol.

A BitTorrent client establishes a connection to a tracker; a system which keeps track of each peer serving a file. It then opens a connection to one or more of these peers to obtain the file. If the outbound firewall permits, the client will also report itself to the tracker so that other clients may download the file from it.

This mechanism requires several connections, with more than one endpoint. A BitTorrent client must connect to the tracker, and then connect to one or more peers to actually transfer the file. If we were to run this through SSH, for instance to encrypt BitTorrent traffic from a private tracker at the central office to a client at a remote workstation, we would need to create a static port forwarding channel for the tracker connection, and then create further channels for the individual peer connections. This is clearly difficult to achieve, especially if you do not know the IP addresses and port numbers of the peers in advance.

In situations such as this, and many more diverse cases, SSH provides a clean solution in the form of a SOCKS proxy. The SOCKS protocol is designed to allow clients to request a proxy connection (i.e. a connection through another system) to a remote endpoint of the clients choice. OpenSSH, and other SSH solutions, offer both SOCKS4 and SOCKS5 support. With SOCKS5, domain-name resolution is performed by the proxy server (i.e. the SSH server) rather than by the client. This feature is not available in SOCKS4, which means that domain names are looked up locally and may appear in DNS logs. If you are using dynamic port forwarding for security (or secrecy), ensuring SOCKS5 is used will ensure that your entire connection, including DNS resolution, is performed through the proxy. (Note, however, that some non-standards-compliant applications ignore the proxy settings and perform DNS resolution locally even if a SOCKS5 proxy has been specified.)

This approach also works when you wish to navigate websites which may link to, or draw content from, other websites. SOCKS based SSH proxying allows you to bypass any network-based restrictions on content and connections to remote services, provided outbound SSH is permitted and you have an account on an external SSH server. In order to set up SOCKS-based dynamic port forwarding, you run the ssh client (on UNIX) with the following command:

```
ssh -D 1080 user@host
```

The -D sets up dynamic forwarding. In this case, the number following the option specifies a local port to listen on as a SOCKS proxy. 1080 is the default SOCKS port, so this has been chosen here. You may use any port you wish, when running dynamic forwarding. Port 8080 is also a popular choice, as it is commonly used for web proxies.

With dynamic forwarding, you can specify to a program that you wish it to communicate via a proxy server on the local host, port 1080 (or whatever you specified after -D) and the traffic will be encrypted and forwarded to the host (SSH server), where it will be decrypted and sent on to its destination. As TCP streams are bi-directional, the reverse is also true; that is, incoming data on an outbound connection created on the local side of the proxy will be encrypted between your system and the host you are “sshed” into.

Onward, now, to a real-life example. Here, we set up dynamic forwarding to bypass a firewall which restricts BitTorrent access, preventing access to trackers or peers outside of the local network, but allowing SSH access to remote hosts – perhaps for remote administration of the international offices.

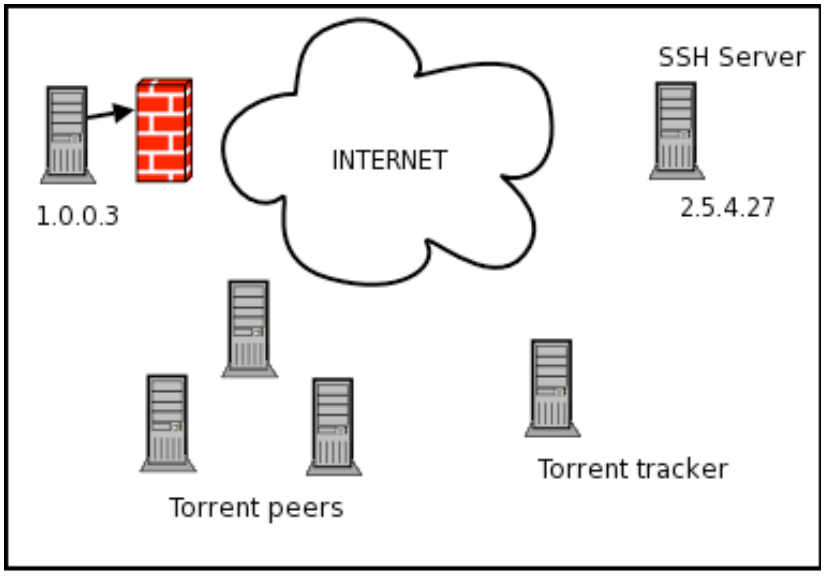


Fig. 3.1

Figure 3.1 shows a setup where a computer on the local network, 1.0.0.3, is trying to access a torrent tracker. The firewall blocks this connection attempt. In figure 3.2, however, the user on 1.0.0.3 has created a dynamic SSH tunnel to 2.5.4.24, using the command:

```
ssh -D 1080 user@2.5.4.24
```

The user can now tell his BitTorrent software to use the SOCKS5 proxy at address 127.0.0.1:1080, and the connections are made through the encrypted tunnel (which the firewall allows to pass, since SSH traffic is allowed), and out to the torrent tracker and peers. The torrent traffic from the tracker and peers returns to the proxy system (the SSH server) and back through the encrypted link to the original client. The firewall knows only that an SSH session is in place. The encryption ensures that it cannot determine the content of the session, the integrity-checking detects any changes the firewall may attempt to make to the session, and the authentication prevents the firewall from staging man-in-the-middle attacks.

From a less technical perspective, the SSH dynamic forwarding enables the use of programs like BitTorrent behind a NAT/firewall which prohibits such traffic. This seems complex to begin with; however, when disregarding all the technical details of the forwarding it can become simple for a less technically minded person to implement, providing the user has access to an SSH server outside of the restrictions of the firewall/NAT.

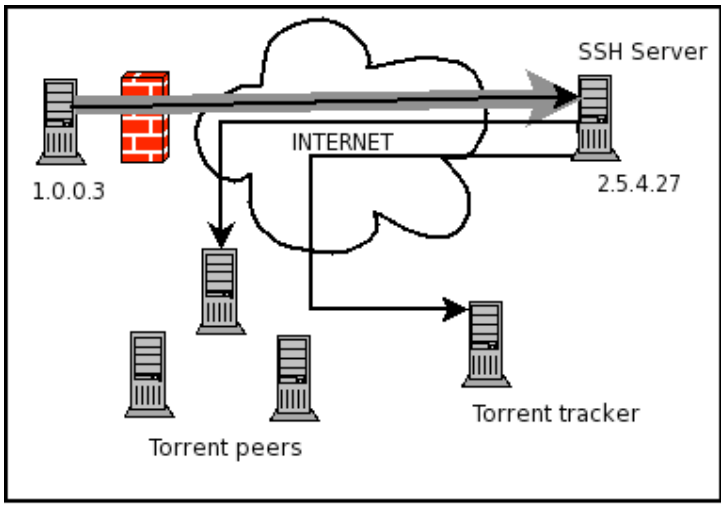


Fig. 3.2

The dynamic port forwarding described here presents a powerful mechanism for subverting firewall rule sets. It is possible, if a firewall allows SSH both inbound and outbound, to set up SOCKS5 proxies via SSH which effectively render the firewall useless to anyone with an account on an SSH server inside the firewall. Such activities are the topic of part two of this article that you can read in the next issue of (IN)SECURE.

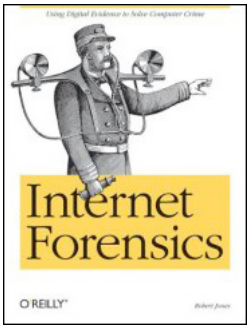
Andrew J. Bennieston contributes to leading computer security websites and forums. His writing efforts include articles, tutorials and book/software reviews. His skillset includes C/C++, PHP, Python and Linux administration, as well as writing about security and programming (not to mention writing about himself in the third person). His personal website is located at http://stormhawk.coldblue.net and he may be contacted at andrew@coldblue.net.

Liam Fishwick is an undergraduate in Physics at the University of Warwick, UK. His computing experience includes Linux and Windows administration and he was instrumental in testing the examples used in this article.

Internet Forensics

by Robert Jones

O'Reilly, ISBN: 059610006X



Targeted at programmers, system administrators and power users, this book tries to provide the information on extracting clues from a range of different sources. It describes how the attackers are covering their tracks and provides tricks that can be used to see through their disguises. The examples in this book are explained in detail and show how much you can find out with ingenuity and a little work. "Internet Forensics" is organized around the core Internet technologies - email, web sites, servers and browsers.

Advanced Host Intrusion Prevention with CSA

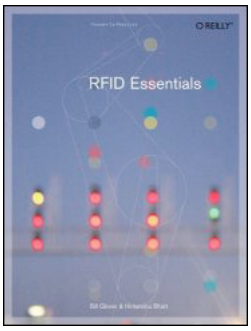
by Jeff Asher, Paul Mauvais, Chad Sullivan

Cisco Press, ISBN: 1587052520

Advanced Host Intrusion Prevention with CSA is a practical guide to getting the most out of CSA deployments. This book helps ease the fears of security administrators seeking to install and configure a host IPS through methodical explanation of the advanced CSA features and concepts. It helps administrators and security engineers to implement CSA appropriately, giving their organizations better protection from the various threats that are impacting their business and enabling them to comply with various legal requirements put forth by such legislature as: HIPAA, SOX, SB1386, and VISA PCI.

RFID Essentials

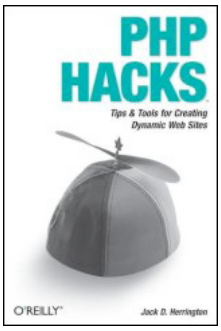
by Bill Gloverand Himanshu Bhatt
O'Reilly, ISBN: 0596009445



Radio Frequency Identification (RFID) is rapidly changing the way business is being conducted. The book is aimed toward developers, system and software architects, and project managers, as well as students and professionals in all the industries impacted by RFID who want to understand how this technology works. As the title suggests, this book is about RFID in general and not just the most recent developments, but it will provide readers with the information and understanding they need to start designing, building, or integrating with RFID systems.

PHP Hacks: Tips & Tools For Creating Dynamic Websites

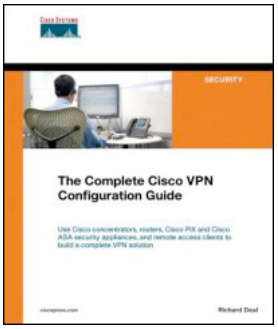
by Jack D. Herrington
O'Reilly, ISBN: 0596101392



Herrington's book shows PHP developers how to take their PHP applications to a higher level of sophistication and style. It takes the language beyond traditional web programming and into mapping, graphing, and multimedia. From adding new front-facing features like graphing, flash, instant messenger, and e-mail access to back-end hacks that show how to create PHP applications that are easy to maintain and extend, "PHP Hacks" delivers hands-on tools for enhancing PHP applications. Unfortunately, the book doesn't cover any specific information on PHP security.

The Complete Cisco VPN Configuration Guide

by Richard Deal
Cisco Press, ISBN: 1587052040

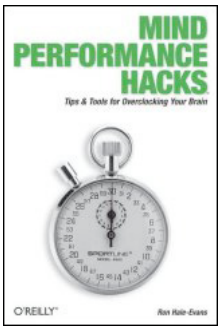


With over 1000 pages, this publication contains detailed explanations of all Cisco VPN products, describing how to set up IPsec and Secure Sockets Layer (SSL) connections on any type of Cisco device, including concentrators, clients, routers, or Cisco PIX and Cisco ASA security appliances.

With copious configuration examples and troubleshooting scenarios, it offers clear information on VPN implementation designs.

Mind Performance Hacks

by Ron Hale-Evans
O'Reilly, ISBN: 0596101538



The book promotional materials introduce Mind Performance Hacks as a publication that provides real-life tips and tools for overclocking your brain and becoming a better thinker. Grounded in current research and theory, but offering practical solutions that you can apply immediately, this member of the "Hacks" series offers good read on things such as using mneomonic tricks to remember different type of information, performing complex math in your head, estimate square roots, tune in your memory and stuff like that.

An inside job

By Melisa LaBancz-Bleasdale

Historically, the approach to enterprise security has been to build the fortress walls bigger and higher - employ more people, write more policies, install more products. Strangely, the more money, resources and solutions we've thrown in that direction, the less invincible we actually are.

Despite heightened awareness and a proliferation of cutting edge security tools, 2005 turned out to be the worst year on record for corporate security breaches. For each new threat there stands a vendor with a plan, but the fact is that the more advanced our security solutions become, so too, do our attackers. The ongoing success of criminal activity clearly shows that threat mitigation requires an ongoing evolution - in our approach to infrastructure security, our implementation of security solutions, and the way we think about threats entering the organization.

Vulnerability Begins at Home

It's a common misconception that if the perimeter is protected, the organization must be secure. This line of thinking is directly challenged by the fact that the biggest threat to an organization actually lies within its boundaries. In their 2005 survey, "The Global State of Information Security," PricewaterhouseCoopers found that 33% of Information Security attacks originated from internal employees while 28% came from ex-employees and partners. Further bolstering these findings, law enforcement experts estimate that more than 50% of all security breach cases are the result of employees misusing access privileges. Malicious insiders notwithstanding, unintentional threats, introduced by otherwise well-meaning employees make up a staggering percentage of the security problems IT will handle daily.

According to IDC's "Insider Threat Ecosystem" the corporate stratosphere is broken up into four main parts. At the top of the ladder there are the citizens -employees who rarely if ever, do anything to violate the company acceptable use policies and are not a security issue. Second, you have the delinquents (which make up the general employee population) people that take small liberties, check their personal mail, play a game here and there, and do some online shopping.

When they are a security threat, it can be significant but it's rarely intentional. Then you have renegades - folks that spend most of the day doing things they should not and often abuse their Internet privileges to run Skype, install P2P or "underground" IM applications, and even worse, send confidential company data to friends and otherwise interested parties. They pose a huge security threat. Lastly, you have rogues - malicious insiders who routinely embezzle confidential corporate information assets and allow others to view and receive protected information and/or have network access, usually for financial gain. They pose the biggest security threat and are often the hardest to catch.

Though experts widely agree that insiders are among the most insidious threats to the enterprise security infrastructure, companies themselves have been slow to accept this realization. In a recent analyst survey regarding corporate security challenges, respondents unfailingly listed malware as the number one threat to their organization with spyware coming in a close second. Internal threats barely made the list at number five.

THOUGH EXPERTS WIDELY AGREE THAT INSIDERS ARE AMONG THE MOST INSIDIOUS THREATS TO THE ENTERPRISE SECURITY INFRASTRUCTURE, COMPANIES THEMSELVES HAVE BEEN SLOW TO ACCEPT THIS REALIZATION.

Although respondents see insider threat as a 'bottom of the stack' concern, analysts such as IDC's Brian Burke rank it much higher on the corporate threat mitigation task list, if not number one itself. It is important however to look at the context of such surveys. Most respondents were IT or security managers, people tasked with the protection of the network whose primary focus is on the network perimeter.

While inappropriate access is a security breach, it would more likely be HR or Legal that would be concerned with employees viewing confidential wage information. IT would be more concerned about keyloggers and malware. "In order to secure the enterprise, it must be done from the inside out, defining and more importantly, enforcing access and use policies as well as agreeing that security is cross-organizational, not a segmented exercise," says Tim Johnson, SurfControl's Product Marketing Manager for Enterprise Threat Shield.

Eliminating the Symptoms

Analysts overwhelmingly agree that security threats such as spyware are merely a symptom of a much bigger cause. The pervasiveness of spyware within an organization can be tied to a human cause - the internal threat that sets malicious activities in motion. Whether by naively clicking through pop-ups or by purposefully installing unapproved and dangerous applications on the network, spyware wouldn't have a home if an employee had not opened the door in the first place.

In a recent spyware survey that examined a one-month period commencing early January 2006, respondents noted that a majority of the ten worst spyware threats were propagated through stealth installations such as those included on the back of a file sharing or in a "smiley" application.

Mythbusting

In order to effectively eliminate spyware, an organization must be able to differentiate between the myths and the realities surrounding it. SurfControl's Johnson provided the following top six myths and related to malware and spyware and the truth behind them.

1. Spyware is an isolated problem.

2. Blocking at the gateway is good enough.

3. Locking down the desktop is good enough.

4. Drive-by downloads are a primary source of penetration.

5. The problem comes from the outside in.

6. No one wants spyware.

And now for the truth:

1. First and foremost, spyware is the symptom of user behavior, not the problem itself. With the rare exception of spyware using system exploits to propagate in a corporate environment (one in which the admin hasn't properly patched a system) spyware comes in as the direct result of user behavior. It can also be the result of naiveté, i.e., a user clicking on an attachment or following through on a phishing attack. There are still those that believe Prince Monbombo of Tanzania actually has millions for their bank account. There are also those who feel that they are doing something legitimate, such as intentionally installing a "cool" tool that has utility or value to them. It also occurs through intentional abuse, like installing password cracking tools. It can be the side-result of users installing games, P2P or IM agents that in turn, install spyware. No matter how it comes in to the network, there is always a user involved.

2. Stuff comes in at the desktop all day long. No one ever breached the Great Wall of China by military force: they either bribed the guards or walked around the end. Blocking at the gateway without removing the culprit makes no sense from a security standpoint. You have detected a threat to your network, you know where it is but you've done nothing to remove it. It's essentially locking the doors and windows of the house - with the burglar still in the basement – and not bothering to call the police. You know the problem is there so you should get rid of it.

Data also leaves via the desktop. Some P2P and IM applications stay completely inside the network and are difficult to detect. Gateway defenses will never detect these threats. Information can flow from a secured portion of the network to an unsecured portion and out the door from there.

FIRST AND FOREMOST, SPYWARE IS THE SYMPTOM OF USER BEHAVIOR, NOT THE PROBLEM ITSELF.

3. If "locking down" the desktop and restricting user installation were effective, then there would be no need for antivirus software. Things can save, install and run locally even if the user doesn't have admin rights. For instance, the Windows system driver, secdrv.sys, lets an application install without rights. Game software often uses this driver and so do the bad guys. The creators of spyware are savvy enough to design around acceptable use policies and depend on the inquisitive nature of human beings to get around such restrictions.

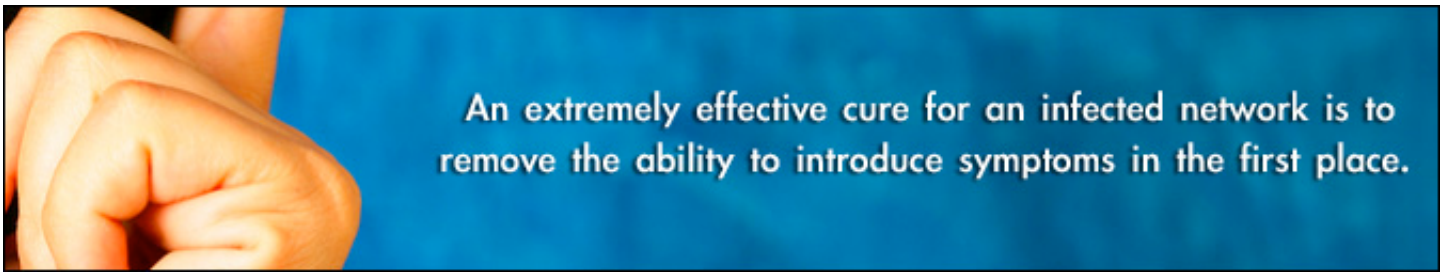
4. "Drive-by downloads" should never occur in a corporate environment. Drive-bys are widely employed by sites that users should not be visiting during working hours nor while using company assets. For instance, no one has gotten spyware by looking for cars on the Ford.com web site. Any decent web filter will prevent users from going to sites that supply or carry spyware. Drive-by downloads aren't something that an admin should be afraid of if the proper tools are in place.

5. Companies are indeed attacked from the outside on a regular basis and there are definitely security concerns related to outside influences, however, it would be both irresponsible and naïve to overlook the idea that internal users represent an even bigger threat to security, compliance and business continuity. Not planning for this inevitability results in an incomplete security infrastructure and presents open opportunities to breach the system.

6. While it is true that no organization actually *wants* spyware, the fact is that spyware applications often appear to be a real utility that users believe they need or want. They may also come in the guise of other applications reliant on the spyware's existence to function, like free games, IM, or P2P – which are also utilities users want. Primarily, that's how users are duped into installing it – time after time. The unfortunate truth is that once they've installed it, they will likely rename what they aren't supposed to have installed to avoid detection.

Worse, they will probably turn off their spyware protection – if possible – especially if the protection stands in the way of getting their cool new utility.

Johnson explains, “There are clear signs that the network has been infected long before it actually implodes. Obvious indicators would be: A sudden increase in media files, a sudden increase in "word.exe" or "salesreport.doc" files, multi-gigabyte MS Office documents appearing without reason, and a not so sudden but marked increase in help desk calls, slow machines, crashes, loss of network performance, and disappearing or corrupted documents. All of above require a thorough examination of network symptoms to find and eliminate the root cause.”



What’s a Company To Do?

The situation may seem bleak, because indeed, employees are a necessary requirement for doing business, yet there are a number of things companies can do to greatly minimize the internal threat to their organization.

First and foremost, all organizations should make a Web filter a required part of their network security arsenal. The filter should prohibit users from visiting known spyware and drive-by download sites. It should also prevent communication with phone home sites. While most symptoms can be cured right there at the filter, it’s not enough.

Companies need an effective email filter capable of blocking spyware from entering the network via active HTML, attachments, phishing, spam and other email-borne vectors. This is critical to securing the communications medium. Yet blocking shouldn’t stop with email. There also needs to be something at the desktop level that stops the spyware as it’s introduced, NOT after it is already saved and running.

Lastly, companies should implement a solution that disallows running or installing programs (such as games, P2P, and IM applications) that in turn, install spyware. Group Policy Objects - or similar tools - are not enough as they can be easily tricked or circumvented.

An extremely effective cure for an infected network is to remove the ability to introduce symptoms in the first place. Users unfortunately shoulder most of the blame when it comes to introducing spyware. “Diehard delinquents and rogues will do whatever they can to hold onto their messaging, music, games and other nifty widgets. If they can turn off protection, they will. If they can hide their spoils, they will. Enacting policies is a great idea, but completely ineffectual if they aren’t regularly, equitably and instantly enforced. Preventative tools are a step in the right direction, but only if they are not of the ‘one-size-fits-all-magic-bullet’ variety,” says Johnson.

Workable solutions must have comprehensive, scalable and customizable capabilities to meet the evolving needs of today’s organizations. 2006 promises a whole new host of challenging and sophisticated security threats – a good deal in the form of fun new utilities employees will surely love. For the health and safety of the network and to prevent the disruption of company operations, it is imperative that organizations implement solutions that users cannot easily evade or interfere with - widgets be damned.

Melisa LaBancz-Bleasdale is a San Francisco area communications consultant and strategist specializing in the security industry. Her focus is on emerging and innovative security technology, current events and market concerns. Visit www.superheated.com to find out more about Melisa.

Hone your skills.

Defeat the attackers roaming your cyber streets! Black Hat USA will once again gather the world's information and computer security elite to share their knowledge and experience with you. Six days. Thirty-three classes. Sixty presentations.

Black Hat®

Briefings & Training USA 2006

July 29 - August 3 • Caesars Palace • Las Vegas

www.blackhat.com

sponsors

platinum

Ernst & Young — Quality In Everything We Do

Microsoft

gold

CITADEL

Configuresoft

QUALYS

silver

ArcSight · Aracaden · CENZIC · CORE · GRANITEEDGE · IOActive · Juniper · Lancope · nCircle · netforensics · radware · SAINT · SPI DYNAMICS · StillSecure · TippingPoint · watchfire · WEBSENSE

In the past year, security podcasts have been gaining momentum and some have built quite and impressive listening audience.

Since this method of sharing information has become so effective we thought we bring one of the most well known security podcasters to introduce you to some of this favorite shows.

The podcasts listed at the following page are the choices of Martin McKeay, the host of the Network Security Podcast.

Martin says: “I record a weekly show about all matters relevant to IT and security with a focus on the Payment Card Industry (PCI) Data Security Standards. I podcast because it gives me an excuse to research interesting stories and technologies.”

However, Martin is not just a podcaster, he’s a really prolific blogger. You can follow his writing and podcasting at www.mckeay.net or you can read his Computerworld blog at www.computerworld.com/blogs/mckeay.

Martin says: “There are several dozen security podcasts in production at this time, and I've picked five of the ones I listen to on a regular basis. I've chosen these because they represent a good variety of skill levels, and each podcast has something you can learn from it. And for me, that's what podcasting is about, the learning.”

Security Now!
http://thisweekintech.com

I've been listening to Security Now! since the first episode. This is not necessarily a podcast for seasoned security professionals, but it's definitely the one to recommend to friends and family who are curious about security.

Steve Gibson sometimes gets extremely excited by particular technologies, but Leo Laporte is there to ground him. I've especially enjoyed their recent shows on encryption, which take the listener from the basics of a ROT-13 to modern day public key encryption technologies.

PaulDotCom Security Weekly
http://www.pauldotcom.com

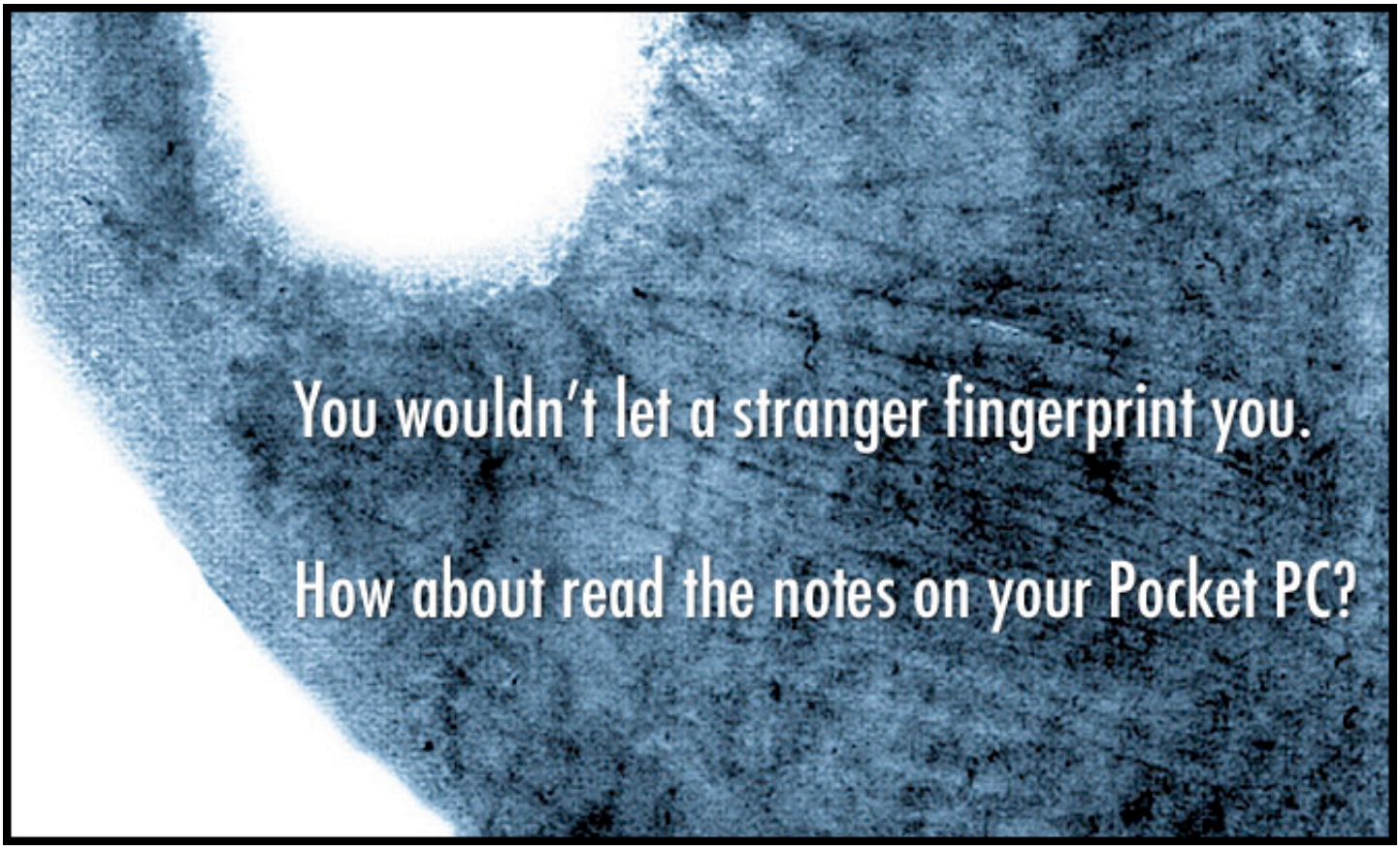
Paul, Larry and sometimes Twitchy bring us a deeper understanding to the technology behind many of the security issues we face today. They not only record a weekly podcast, they have semi-regular PauldotCom TV episodes. Larry has a passion for wireless and 'Storytime with Twitchy' is always amusing.

Security Catalyst
http://www.securitycatalyst.com

Michael Santarchangelo is a polished speaker with a desire to teach security professionals as well as home users. The Security Catalyst podcast often focuses on explaining to the end users how to setup the basic security measures like their firewall and anti-virus, but also has interviews with industry experts to discuss real world security.

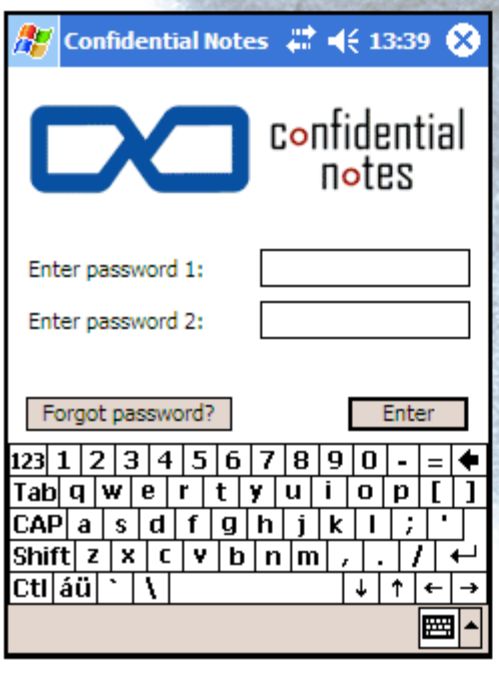
Mighty Seek
http://www.mightyseek.com/

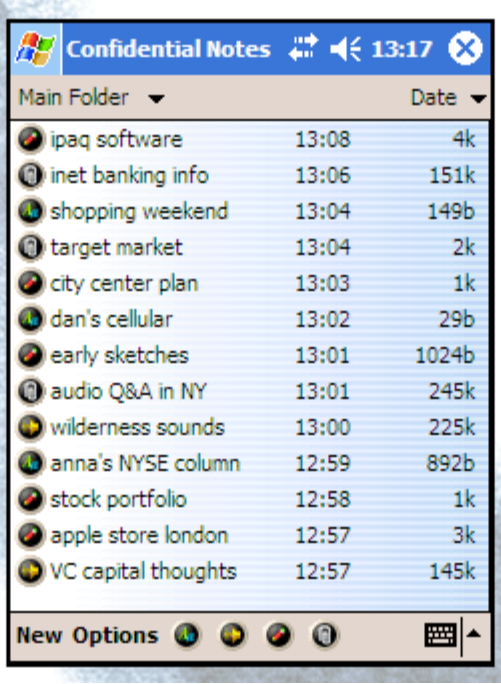
This is one of the podcasts that start gets into the real arcanum of security. Dan Kuykendall is an ex-network security professional who has turned his attention to securing software. As a programmer, Dan is someone who knows the intricacies of a privilege escalation attack, and will tell you how to avoid them in your code.



Confidential Notes is a practical and easy to use solution that instantly provides you with a high level of security for your mobile data.

For more information on Confidential Notes visit www.pocketpcsecurity.com





Patricia Sueltz joined SurfControl in 2005 from SalesForce.com where she was President, Global Operations. Prior to this Pat was Executive Vice President of Services and a Corporate Officer of Sun Microsystems, for four years having previously held a number of senior positions at IBM, including Technical Assistant to the Chairman and CEO, and a two year assignment in the UK early in her career. Pat has also served as a Board member of Delphi and Amgen, both Fortune 500 companies, and serves on the national board for the American Foundation for the Blind. Pat is based in SurfControl's US Headquarters in Scotts Valley, California.

What has been your biggest challenge as the CEO of SurfControl?

SurfControl has thousands of customers, millions of users, and manages more than a billion filtering requests per day.

A lot of people aren't aware of our depth of expertise and breadth of resources in successfully protecting some 14 million users, so articulating our value proposition is our greatest opportunity (not challenge!).

How has SurfControl's strategic focus changed from previous years?

Because today's threats challenge every point of Internet vulnerability, we are more focused on delivering to customers layered solutions rather than point products. You can't protect a business completely if you only protect one layer – email but not web, on but not off of the network, PC, but not other mobile devices. Our solutions provide this important, multi-layered approach.

Another change is a much stronger focus on the channel. We have great partners who know that we don't compete with them, and that our goal is mutual success.

We're getting excellent results in terms of deeper and additional partner relationships and more growth. In fact, about 80% of new billings come from our more than 1,500 channel partners worldwide.

How much progress did SurfControl make in the enterprise market in the past year?

We're making healthy progress on many levels. We've gone from a position of no growth to modest growth. We've regrouped internally and have a strong organization, as well as a terrific management team. Sales productivity is up, channel sales are up, and customers are realizing the value of comprehensive Internet protection. The opportunities are immense, and we're very excited about them!

What are SurfControl's strengths in the market? How are you building on these advantages?

SurfControl's strengths revolve around the ecosystem we've built: solid products and solutions, customers, employees and partnerships. We're investing in this ecosystem overall to gain more ground and build on this already great momentum. Ultimately, I'm a CEO who believes that if you don't have a great team, you don't have anything. I spend a lot of time with customers and one piece of feedback I get consistently is that our employees are the best to work with in the industry.

Whether customers are exploring, buying, implementing or upgrading our solutions – they like working with our team. I'm very proud of that feedback.

With the constant evolution of threats, what kind of technology challenges does SurfControl face?

We are focused on staying ahead of the curve and delivering relevant, real-time protection to our customers. That means being compatible with every device that connects to the Internet – PDAs, Xboxes, and everything else you can imagine – with multiple platforms and delivery mechanisms.

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

Education and awareness. We have to make sure people understand the extent of risk and danger out there, and get them to act on it.

We're not just dealing with 18-year old malicious hackers, we're guarding against cyber-terrorists who want to hurt other people and businesses.

In addition to our layered protection solutions for incoming and outgoing content, our threat detection experts have the ability to identify and stop phishing attacks, like the one recently leveraged against Chase Bank customers. This particular attack attempted to have customers reveal personal information, via a toll-free number. It potentially could have had a huge impact on Chase's business, including exposing confidential information, customers, revenue and reputation.

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

The port 80 threat – since viruses and malicious code enter the network that way. Also, sites like myspace, devices like the Xbox – anything that's vulnerable. This is more than just threat protection, it's a platform for security to guard our businesses and our families.

In your opinion, how important are e-mail and web filtering in the overall security architecture?

E-mail and web filtering solutions are important parts of SurfControl's Enterprise Protection Suite, which includes another important element: desktop protection. Customers are now thinking in terms of "security in the large" – beyond threat protection to company policies, management and compliance with these policies. SurfControl thinks in terms of the blended threat protection which needs to be located at the various layers of the network.

What are your future plans? Any exciting new projects?

We have a lot of opportunity in security and content management; this extends to new devices, form factors, and delivery mechanisms. CEOs and CIOs want us to help them protect their businesses and we'll continue to do that.

For the near future, we will concentrate on great innovation, extending partnerships and relationships, focusing on customers, and building our team. I think that's a good start.

WINDOWS - GFI LANguard Network Security Scanner
http://www.net-security.org/software.php?id=481

GFI LANguard Network Security Scanner is a tool to audit network security and proactively secure it. It scans entire networks from an attacker's perspective, and analyses machines for open ports, shares, security alerts/vulnerabilities, service pack level, installed hotfixes and other NETBIOS information such as hostname, logged on user name, users etc.

LINUX - Bastille Linux
http://www.net-security.org/software.php?id=217

The Bastille Hardening System attempts to "harden" or "tighten" Unix operating systems. It currently supports the Red Hat, Debian, Mandrake, SuSE and TurboLinux Linux distributions along with HP-UX and Mac OS X. We attempt to provide the most secure, yet usable, system possible.

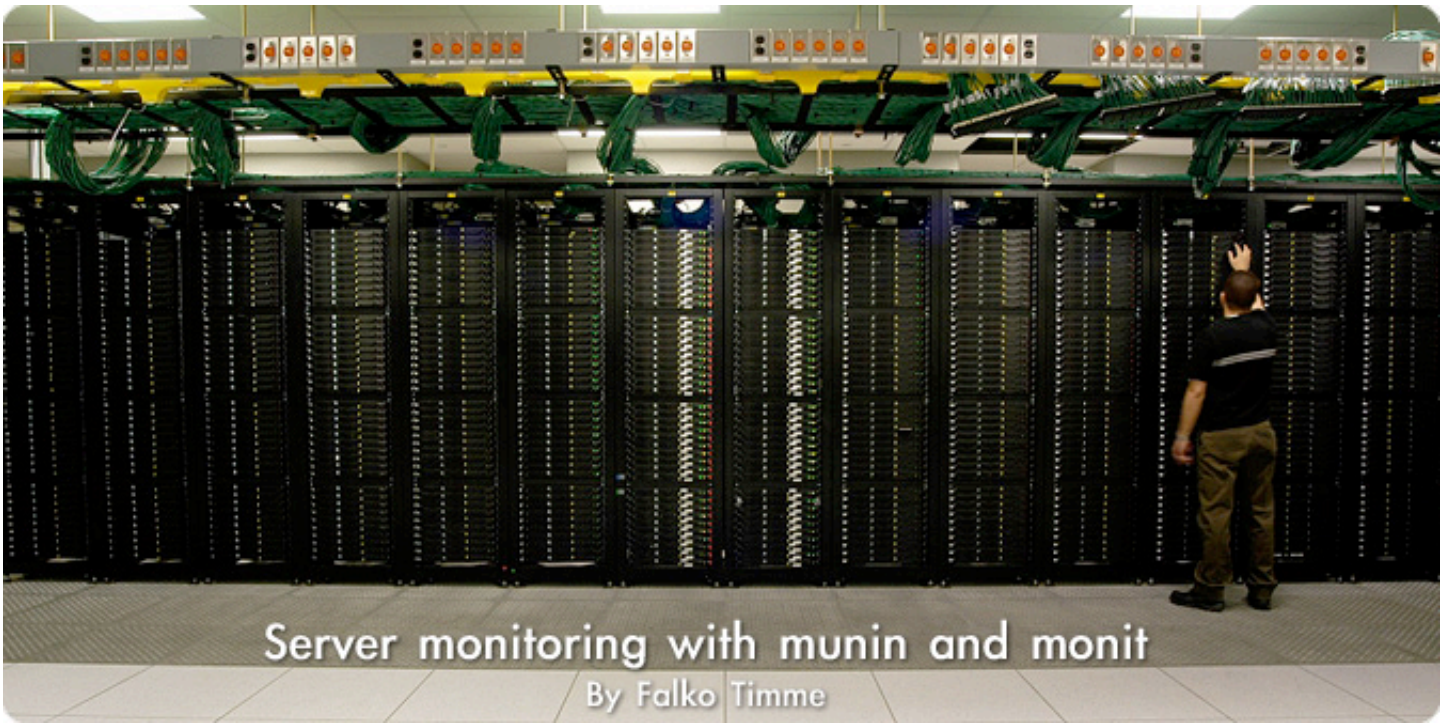
MAC OS X - KisMAC
http://www.net-security.org/software.php?id=625

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.

POCKET PC - WiFiFoFum
http://www.net-security.org/software.php?id=547

WiFiFoFum is a WiFi scanner and war driving software for Pocket PC 2003 and Windows Mobile 5 Pocket PC and Smartphone editions.

If you want your software title included in the HNS Software Database e-mail us at software@net-security.org



This article describes how to monitor your server with munin and monit. munin produces nifty little graphics about nearly every aspect of your server (load average, memory usage, CPU usage, MySQL throughput, eth0 traffic, etc.) without much configuration, whereas monit checks the availability of services like Apache, MySQL, Postfix and takes the appropriate action such as a restart if it finds a service is not behaving as expected.

The combination of the two gives you full monitoring: graphics that lets you recognize current or upcoming problems (like "We need a bigger server soon, our load average is increasing rapidly."), and a watchdog that ensures the availability of the monitored services.

Although munin lets you monitor more than one server, we will only discuss the monitoring of the system where it is installed here.

This tutorial was written for Debian Sarge, but the configuration should apply to other distributions with little changes as well.

1. Current situation

Our system's hostname is `server1.example.com`, and we have a web site `www.example.com` on it with the document root `/var/www/www.example.com/web`.

2. Install and configure munin

To install munin on Debian Sarge, we do this:

```
apt-get install munin munin-node
```

Next, we must edit the munin configuration file `/etc/munin/munin.conf`.

We want munin to put its output into the directory `/var/www/www.example.com/web/monitoring`, therefore we change the value of `htmldir`, and we want it to use the name `server1.example.com` instead of `localhost.localdomain` in the HTML output, therefore we replace `localhost.localdomain` with `server1.example.com`. Without the comments, the changed file looks like this:

```
vi /etc/munin/munin.conf
```

```
dbdir   /var/lib/munin
htmldir /var/www/www.example.com/web/monitoring
logdir  /var/log/munin
rundir  /var/run/munin

tmpldir /etc/munin/templates

[server1.example.com]
    address 127.0.0.1
    use_node_name yes
```

Next we create the directory `/var/www/www.example.com/web/monitoring` and change its ownership to the user and group munin, otherwise munin cannot place its output in that directory. Then we restart munin:

```
mkdir -p /var/www/www.example.com/web/monitoring
chown munin:munin /var/www/www.example.com/web/monitoring
/etc/init.d/munin-node restart
```

Now wait a few minutes so that munin can produce its first output, and then go to `http://www.example.com/monitoring/` in your browser, and you see the first statistics. After a few days this could look like Figure 1 below and Figure 2 on the following page.

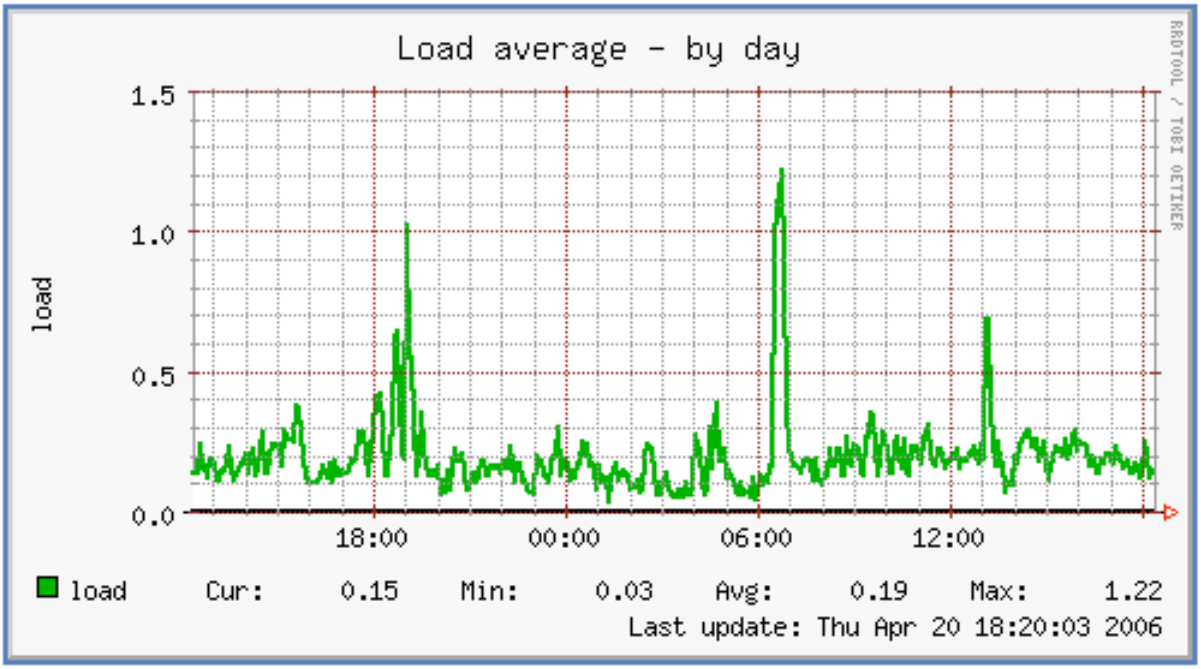


Figure 1. - munin load average graph

3. Password-protect the munin output directory (optional)

You should password-protect the directory `/var/www/www.example.com/web/monitoring` unless you want everybody to be able to see every little statistic about your server.

To do this, we create an `.htaccess` file in `/var/www/www.example.com/web/monitoring`:

```
vi /var/www/www.example.com/web/monitoring/.htaccess
```

```
AuthType Basic
AuthName "Members Only"
AuthUserFile /var/www/www.example.com/.htpasswd
<limit GET PUT POST>
require valid-user
</limit>
```

Then we must create the password file `/var/www/www.example.com/.htpasswd`. We want to log in with the username `admin`, so we enter the command below and afterwards enter a password for `admin` and we're done!

```
htpasswd -c /var/www/www.example.com/.htpasswd admin
```

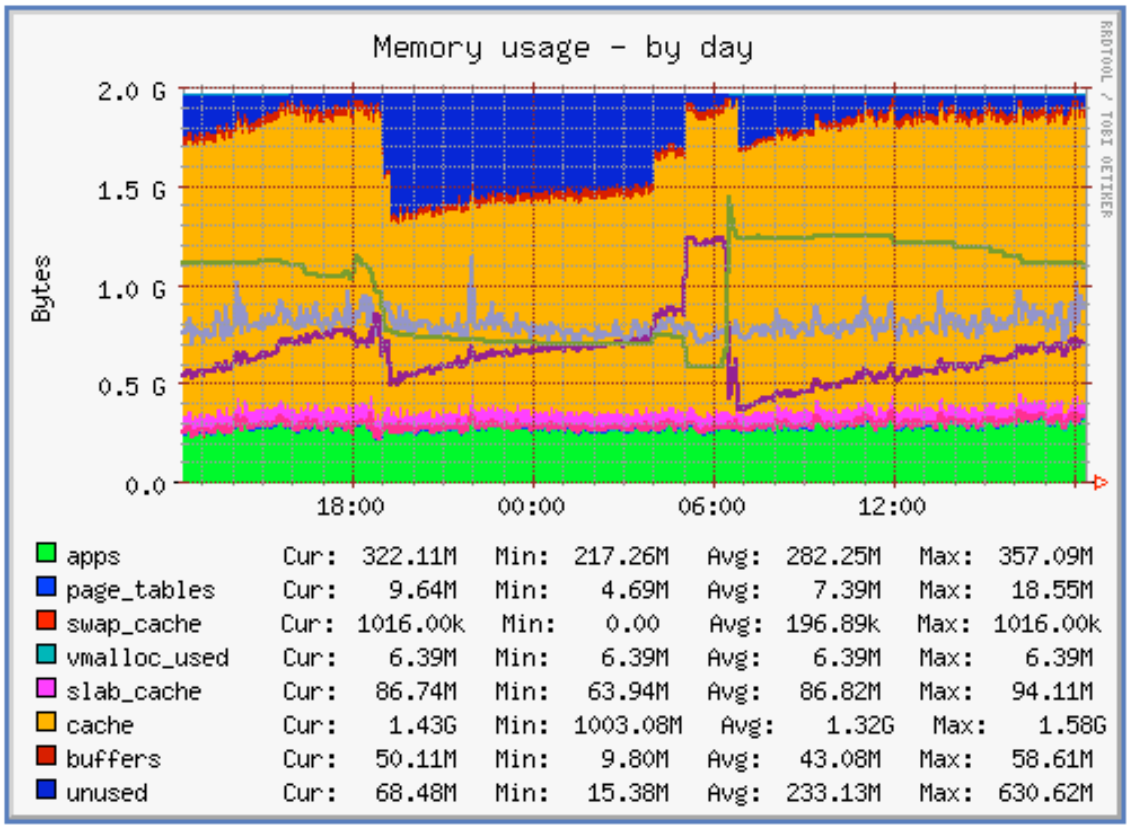


Figure 2. - munin memory usage graph

4. Install and configure monit

To install monit, we do this:

```
apt-get install monit
```

Now we must edit `/etc/monit/monitrc`. The default `/etc/monit/monitrc` has lots of examples, and you can find more configuration examples on www.tinyurl.com/nyvym.

However, in my case I want to monitor `proftpd`, `sshd`, `mysql`, `apache`, and `postfix`, I want to enable the monit web interface on port 2812, I want a https web interface, I want to log in to the web interface with the username `admin` and the password `test`, and I want monit to send email alerts to `root@localhost`, so my file looks like this:

```
vi /etc/monit/monitrc
```

Details on the file contents are on the following page.

```
set daemon  60
set logfile syslog facility log_daemon
set mailserver localhost
set mail-format { from: monit@server1.example.com }
set alert root@localhost
set httpd port 2812 and
     SSL ENABLE
     PEMFILE  /var/certs/monit.pem
     allow admin:test

check process proftpd with pidfile /var/run/proftpd.pid
   start program = "/etc/init.d/proftpd start"
   stop program  = "/etc/init.d/proftpd stop"
   if failed port 21 protocol ftp then restart
   if 5 restarts within 5 cycles then timeout

check process sshd with pidfile /var/run/sshd.pid
   start program  "/etc/init.d/ssh start"
   stop program  "/etc/init.d/ssh stop"
   if failed port 22 protocol ssh then restart
   if 5 restarts within 5 cycles then timeout

check process mysql with pidfile /var/run/mysqld/mysqld.pid
   group database
   start program = "/etc/init.d/mysql start"
   stop program = "/etc/init.d/mysql stop"
   if failed host 127.0.0.1 port 3306 then restart
   if 5 restarts within 5 cycles then timeout

check process apache with pidfile /var/run/apache2.pid
   group www
   start program = "/etc/init.d/apache2 start"
   stop program  = "/etc/init.d/apache2 stop"
   if failed host www.example.com port 80 protocol http
      and request "/monit/token" then restart
   if cpu is greater than 60% for 2 cycles then alert
   if cpu > 80% for 5 cycles then restart
   if totalmem > 500 MB for 5 cycles then restart
   if children > 250 then restart
   if loadavg(5min) greater than 10 for 8 cycles then stop
   if 3 restarts within 5 cycles then timeout

check process postfix with pidfile /var/spool/postfix/pid/master.pid
   group mail
   start program = "/etc/init.d/postfix start"
   stop  program = "/etc/init.d/postfix stop"
   if failed port 25 protocol smtp then restart
   if 5 restarts within 5 cycles then timeout
```

The configuration file is pretty self-explaining; if you are unsure about an option, take a look at the monit documentation: tinyurl.com/nh7yu

In the `apache` part of the monit configuration you find this:

```
if failed host www.example.com port 80 protocol http
      and request "/monit/token" then restart
```

which means that monit tries to connect to `www.example.com` on port 80 and tries to access the file `/monit/token` which is `/var/www/www.example.com/web/monit/token` because our web site's document root is `/var/www/www.example.com/web`. If monit doesn't succeed it means Apache isn't running, and monit is going to restart it. Now we must create the file `/var/www/www.example.com/web/monit/token` and write some random string into it:

```
mkdir /var/www/www.example.com/web/monit
echo "hello" > /var/www/www.example.com/web/monit/token
```

Next we create the pem cert (`/var/certs/monit.pem`) we need for the SSL-encrypted monit web interface:

```
mkdir /var/certs
cd /var/certs
```

We need an OpenSSL configuration file to create our certificate. It can look like this:

```
vi /var/certs/monit.cnf
```

```
# create RSA certs - Server

RANDFILE = ./openssl.rnd

[ req ]
default_bits = 1024
encrypt_key = yes
distinguished_name = req_dn
x509_extensions = cert_type

[ req_dn ]
countryName = Country Name (2 letter code)
countryName_default = MO

stateOrProvinceName             = State or Province Name (full name)
stateOrProvinceName_default     = Monitoria

localityName                    = Locality Name (eg, city)
localityName_default            = Monittown

organizationName                = Organization Name (eg, company)
organizationName_default        = Monit Inc.

organizationalUnitName          = Organizational Unit Name (eg, section)
organizationalUnitName_default  = Dept. of Monitoring Technologies

commonName                      = Common Name (FQDN of your server)
commonName_default              = server.monit.mo

emailAddress                    = Email Address
emailAddress_default            = root@monit.mo

[ cert_type ]
nsCertType = server
```

Now we create the certificate like this:

```
openssl req -new -x509 -days 365 -nodes -config ./monit.cnf -out
/var/certs/monit.pem -keyout /var/certs/monit.pem
openssl gendh 512 >> /var/certs/monit.pem
openssl x509 -subject -dates -fingerprint -noout -in /var/certs/monit.pem
chmod 700 /var/certs/monit.pem
```

Afterwards we edit `/etc/default/monit` to enable the monit daemon. Change startup to 1 and set `CHECK_INTERVALS` to the interval in seconds that you would like monit to check your system. I choose 60 (seconds) so my file looks like this:

```
vi /etc/default/monit
```

```
# Defaults for monit initscript
# sourced by /etc/init.d/monit
# installed at /etc/default/monit by maintainer scripts
# Fredrik Steen <stone@debian.org>

# You must set this variable to for monit to start
startup=1

# To change the intervals which monit should run uncomment
# and change this variable.
CHECK_INTERVALS=60
```

Finally, we can start monit:

`/etc/init.d/monit start`

Now point your browser to `https://www.example.com:2812/` (make sure port 2812 isn't blocked by your firewall), log in with `admin` and `test`, and you should see the monit web interface.

It should look like this:

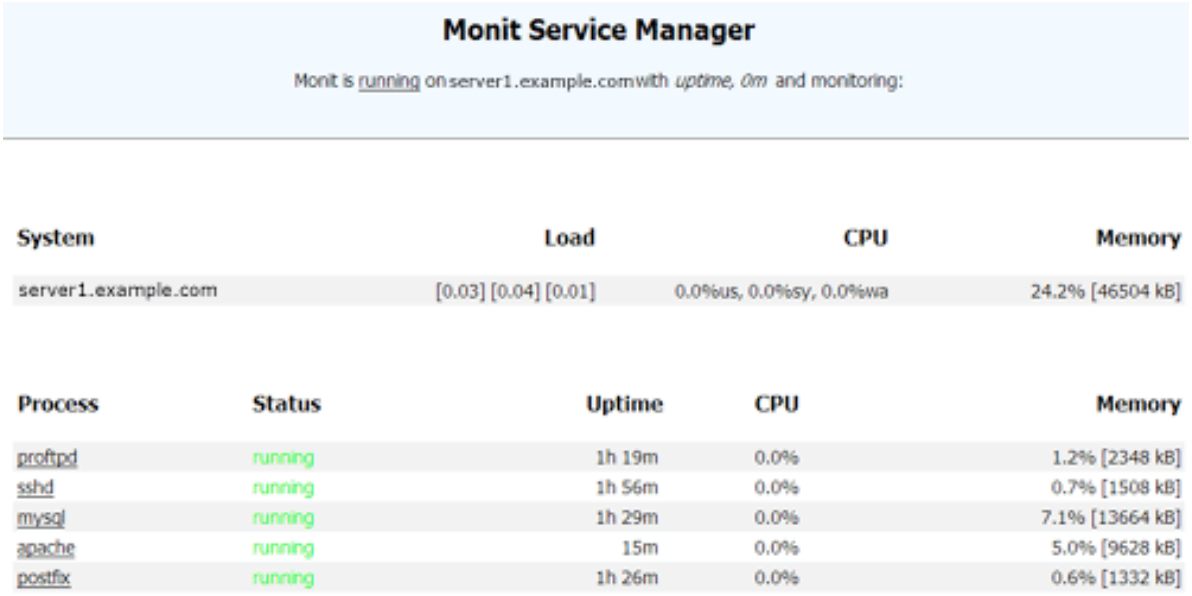


Figure 3. - monit main screen

Parameter	Value
Name	apache
Pid file	/var/run/apache2.pid
Status	running
Group	www
Monitoring mode	active
Monitoring status	monitored
Start program	/etc/init.d/apache2 start
Stop program	/etc/init.d/apache2 stop
Check service	every 1 cycle
Timeout	If 3 restart within 5 cycles then unmonitor else if recovered then alert
Data collected	Fri Oct 21 16:35:16 2005
Port Response time	0.008s to 127.0.0.1:80/monit/token [HTTP]
Process id	7561
Parent process id	1
Process uptime	18m
CPU usage	0.0%
Memory usage	5.0% [9628kB]

Figure 4. - Apache status page

Depending on your configuration in `/etc/monit/monitrc` monit will restart your services if they fail and send notification emails if process IDs of services change, etc.

Get munin at:
http://munin.projects.linpro.no

Get monit at:
http://tildeslash.com/monit/index.php

Falko Timme is a System Developer at projektfarm GmbH, Germany. He enjoys creating Linux tutorials which he publishes on HowtoForge (http://www.howtoforge.com). He is currently writing a book about Linux system administration for O'Reilly together with Tom Adelstein.

Fraught with internal and external security breaches, corporate scandal and increasingly sophisticated attack mechanisms, the past five years have brought about a new era in security awareness. Organizations have seen the fragility of their security infrastructure exposed, their executives indicted and their reputations tarnished.

Personal accountability has now joined the list of top concerns facing today's CEO. In the wake of stricter global compliance requirements companies must strive to understand an expanding variety of applicable data and communication mandates governing their operations.

In Ernst & Young's 8th Annual Global Information Security survey, nearly two-thirds of the 1,300 respondents- made up of global companies, government and non-profit agencies in 55 nations - cited compliance with regulations such as Sarbanes-Oxley, the EU's 8th Directive or their equivalent as the primary driver of information security.

Security and privacy concerns have had global repercussions with worldwide governments enacting rules to safeguard client data and business practices. The Sarbanes-Oxley Act, Companies Act, HIPAA, Data Protection Act, Basel II, and Graham Leach Bliley Act are but a few of the many regulations companies must operationally navigate. Although the stream of regulatory requirements has seemingly little impact on employee activities, conversely, employee activities have an enormous impact on whether or not a company is in compliance.

Due to its complexity and the vastness of the topic, many companies have chosen to adopt a patch-and-persist compliance approach, throwing money at problems when they're told there's a crisis on the horizon. By implementing vendor solutions whose main claim is to cure compliance ills companies look to vendors to ensure their due diligence.

Each law is rife with nuance and vagaries but all were enacted with similar requirements – for each organization to address information management, financial reporting, risk management and security. Additionally, each organization must have in place workable audit mechanisms that allow for the investigation of and access to, the historical record of corporate activity. Security and privacy seem to be the overriding themes, with most of the regulations specifically addressing the integrity of data, the infrastructure, and the prevention of outside influence. Together, global compliance requirements call for appropriate controls on

the enterprise network: monitoring access to or use of, proprietary or sensitive information, exposing, transferring or viewing private data, employing the necessary technology to proactively prevent security breaches to the network, monitor and record company communications, and have a clear-cut IT response plan for security breaches and business continuity failures.

What Have We Learned?

Increasingly sophisticated threats continue to plague the enterprise environment. At best, they disrupt the daily productivity, at worst they bring a company to its knees. Web-based threats have fast become the greatest threat to business integrity with employees providing an excellent conduit for these threats to enter the network.

More alarming than the threats themselves is our collective inability to stem their root cause. According to the April 2006 report issued by PricewaterhouseCoopers on behalf of the UK Department of Trade and Industry (DTI), despite the fact that 100% of large businesses have anti-virus software and 76% have anti-spyware solutions in place, 43% of them were infected with malicious software past year. This trend has changed little since 2004 when the CSI/FBI Computer Crime survey reported that out of 99% of companies using antivirus software, 78% of them were hit by viruses, worms and other malicious attacks.

The pervasive need for constant and convenient connectivity and information access has created portals of vulnerability that are difficult to pinpoint and prevent. Malware, spyware, phishing and hacks continue to bombard even the most fortified networks with internal employees regularly contributing to the threat scenario. Companies tasked with creating a collaborative working environment have also unwillingly opened up the network to increasing vulnerability and attacks.

THE PERVASIVE NEED FOR CONSTANT AND CONVENIENT CONNECTIVITY AND INFORMATION ACCESS HAS CREATED PORTALS OF VULNERABILITY THAT ARE DIFFICULT TO PINPOINT AND PREVENT.

In light of these disturbing statistics, it is clear that in order to effectively safeguard your organization against security threats, a proven, comprehensive, and multi-tiered response to infrastructure security is necessary to maintain ongoing business integrity and continuity, as well as meet stringent internal and external compliance objectives.

Organizations are increasingly exposed to threats to the information in their mission-critical inward- and outward-bound communication channels. These threats exploit a diversity of technical vulnerabilities in IT systems, as well the behavioral characteristics of employees. Regulatory and commercial penalties for failing to secure these channels can be severe and value destroying; regulatory guidance on compliance requirements is, however, still very limited.

Organizations have traditionally responded to regulatory compliance requirements on a law-by-law, or department-by-department basis, which used to be a perfectly acceptable process. In the past, there were relatively few laws, compliance requirements were generally firmly established and well understood, and the jurisdictions within which businesses operated were well defined. Over the last decade, all that has changed. Rapid globalization, increasingly pervasive information technology, the evolving business risk and threat environment, and today's governance expectations have, between them, created a fast-growing and complex body of laws and regulations that impact the organization's IT systems.

While global companies are in the forefront of finding effective compliance solutions, every organization, however small, and in whatever industry, is challenged by the same broad range of state, federal and international regulatory requirements. These regulatory requirements focus on the confidentiality, integrity and availability of electronically held information, and primarily—but not exclusively—on personal data.

Many of the new laws—such as SB 1386 and OPPA—appear to overlap, and not only is there very little established legal guidance as to what constitutes compliance, but new laws and regulatory requirements continue to emerge. Increasingly, these laws have a geographic reach that extends to organizations based and operating outside the apparent jurisdiction of the legislative or regulatory body.

Outward-bound Information Security

In the case of outward-bound information security, the practical approach mirrors the best-practice approach, which is to secure the outward-bound communication channel itself, and to repeat the process for all types of corporate communication. In most instances, there is not yet a body of tested case law and proven compliance methodologies to which organizations can turn in order to calibrate their efforts to comply with all of the existing regulations. There are no technology products that, by themselves, can render organizational compliance with any of the data-security regulations, because all data-security controls consist of a combination of technology, procedure and human behavior. In other words, installing a firewall will not protect an organization if there are no procedures in place for correctly configuring and maintaining it, and if users habitually bypass it—through, for instance, IM, P2P, Internet browsing or the deployment of rogue wireless access points.

THERE ARE NO TECHNOLOGY PRODUCTS THAT, BY THEMSELVES, CAN RENDER ORGANIZATIONAL COMPLIANCE WITH ANY OF THE DATA-SECURITY REGULATIONS.

The nature of inward- and outward-bound digital, electronic communication channels, such as IM, e-mail or memory stick, is that they are data-neutral. This means that any type of data, and any form of content, can pass beyond the corporation through any one of these routes.

Consequently, any attempt to control one type of information in the outward-bound communication channel—financially sensitive information, for instance—can be undermined if there aren't any effective controls against the passage of other confidential information or, in fact, against the passage of information of any sort.

Similarly, threats to any data in the outward-bound communication channel are threats to all data in the channel: a worm, or a more-sophisticated blended threat, can indiscriminately corrupt every type of information in the channel and will not restrict itself only to one legal category of data. Nontraditional Web-based outward-bound communication is similarly vulnerable to information leakage.

Web-based e-mail, Web chat and blogs all provide opportunities for data leakage, whether deliberate or accidental, and this can have seriously damaging effects on the organization. As a direct consequence, any attempt to secure only a limited range of data—medical records, for instance—in the outward-bound communication channel will ultimately fail. A best-practice information security framework supports the coordination of compliance strategy across multiple channels and guides control responses to multiple threats to all sorts of information assets.

Moving Forward – A Best Practice Approach

The regulatory environment is evolving in parallel with the rapid mutations that take place in today's threat environment. Information security technology that is capable of meeting complex threats and regulatory requirements will, of necessity, be multilayered and comprehensive. It must also be capable of rapid adaptation to these changing risks and requirements.

The most common corporate digital communication platforms are e-mail and IM. E-mail is, for most organizations, a ubiquitous and critical application that virtually everyone can access, and the use of IM (both approved and unapproved) is increasingly widespread. These platforms are, as a result, prime areas for information leakage, both deliberate and accidental, of critical data that is covered by HIPAA, GLBA, SOX and other global legislation.

Once staff have been authorized to use an e-mail or IM account, it can be difficult to control enforce acceptable use policies, therefore, it should be each organization's topmost priority to ensure that the content within their primary communication mechanisms are adequately controlled.

Without a cohesive plan of action, enacting internal corporate controls that are aligned with external compliance requirements can be a daunting, disconnected and unenforceable task.

A highly recommended means of achieving a linear approach to compliance is to adopt a best-practice approach, such as that set out in the internationally recognized information security standard ISO/IEC 17799:2005. A best-practice information security framework will support the coordination of compliance strategy across multiple channels and guide control responses to multiple threats to information assets. Taking a policy and solutions-based approach to meeting this best-practice guidance and will help organizations secure broad and ongoing compliance with the regulatory requirements to preserve the confidentiality, integrity and availability of information.

There are two overarching, independently originated best-practice information security frameworks: ISO/IEC 17799:2005 and CobiT. They both support the coordination of compliance strategy across multiple channels, dealing with a wide range of vulnerabilities as well as variable and evolving threats, protecting all sorts of information assets and data types, while allowing for business complexities and external constituencies.

Best-practice frameworks provide a number of interlocking and mutually dependent controls that, between them, enable an organization to secure the confidentiality, integrity, and availability of its information and information assets. They are also technology-neutral, because they recognize that there are neither "one-size-fits-all" technology solutions nor any permanent solutions in a rapidly changing and evolving threat environment. However, technology is considered a primary and viable mechanism for achieving compliance and presenting an organization's due diligence.

Best practice is particularly important on the organizational perimeter. A physically secure organizational perimeter that prevented intruders and attackers from penetrating corporate information systems used to be the only critical component of an effective information security structure. A firewall is no longer an adequate defense. The extension of the network from the desktop onto mobile laptops, remote workstations, PDAs, cell phones and memory sticks, combined with multiple two-way communication channels—text, e-mail, instant messaging (IM), peer-to-peer (P2P) and the ubiquitous Web browser—together with the requirement to control and monitor the content of communications themselves, have created new regulatory compliance challenges for what is now identified as the "inward- and outward-bound communication channel."

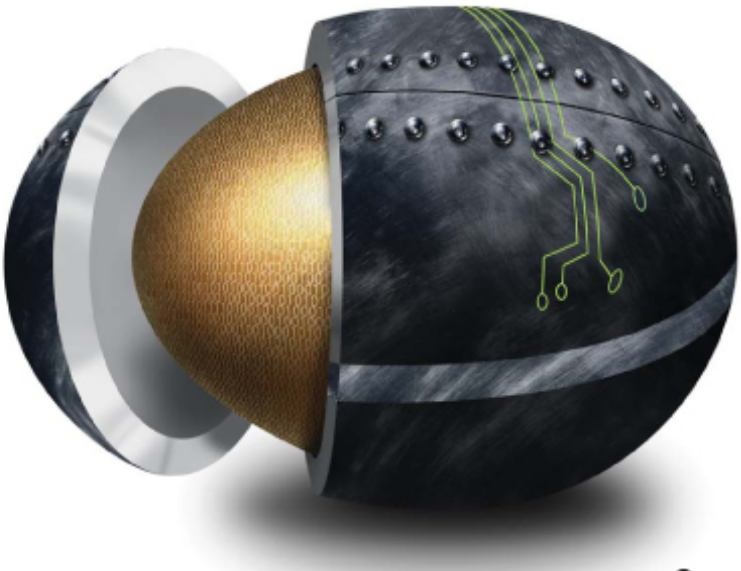
Identifying and dealing with threats to the availability, confidentiality and integrity of information contained within inward- and outward-bound communications is strategic corporate survival. An externally validated, best-practice approach to information security—one that provides a single, coherent, multilayered, channel-specific framework—can enable simultaneous compliance with multiple regulatory requirements.

Although the rewards for adherence to regulatory requirements certainly won't grab headlines, the penalties for failure to do so will. While it's easy to continue on the piecemeal path to policy, technology and process implementation, it is the least reliable and most dangerous approach to meeting comprehensive corporate security and global compliance objectives. Taking a careful, well-planned course of action, coupled with best practice guidelines will help to ensure overall business integrity and longevity.

Jim Murphy is the Product Manager at SurfControl where he is responsible for SurfControl Web Filter, the market-leading Internet content security solution, and SurfControl Instant Message Filter, the company's newest product designed to manage instant messaging and peer-to-peer communications in the enterprise.

infosecurity CANADA

Pre-conference Workshops: June 19, 2006
Conference & Exhibition: June 20-21, 2006
Metro Toronto Convention Centre



Protect Your Business.

Protecting your business makes the difference between profit and loss, success and failure.

Attend Infosecurity Canada, the only conference and exhibition in Canada that focuses on the sharing of information critical to a more secure and compliant information infrastructure. Discover how you can ensure that the information security programs you have in place are compliant and secure. Meet with partners who can provide you with instant access to cutting-edge technologies. Acquire new skills and insights from qualified experts.

- ✓ **Over 70 leading suppliers**
- ✓ **Advanced technologies**
- ✓ **Innovation Theater**
- ✓ **More than 35 in-depth conference sessions**
- ✓ **NEW Exhibits Plus Conference Pass**
- ✓ **FREE daily keynote presentations & general sessions**
- ✓ **Networking Reception**

Information, Education and Networking – Infosecurity Canada brings it all together.

Infosecurity Canada brings together leading experts and innovators from across the country to consult, collaborate, educate and explore new solutions that will mitigate the risks you face. Interact with these thought leaders in the security industry. Debate the issues and latest trends. Discover how to better manage the security strategy that's right for your organization. For a complete list of speakers and sessions, visit **www.infosecuritycanada.com/secure**

CISSPs®/SSCPs® Earn Up To 12 Continuing Education Credits (CPEs) Direct From (ISC)².

(ISC)²® The conference program at Infosecurity Canada includes the preeminent Security Leadership Conference Series. Only (ISC)², the international leader dedicated to educating and certifying information security professionals worldwide, and Infosecurity, the global leader in Information Security events, can offer such a high caliber education program.

www.infosecuritycanada.com/besecure

REGISTER BY 5/01/06 FOR EARLY-BIRD CONFERENCE DISCOUNTS AND FREE EXHIBITION ADMISSION.
www.infosecuritycanada.com/besecure

Premier Education Sponsor: (ISC)²
Global Sponsor: symantec.
Diamond Sponsor: Microsoft
Platinum Sponsor: ca
Gold Sponsor: Cisco Systems
Silver Sponsor: BorderWare
Bronze Sponsors: tyco Fire & Security, ADT, Application Security, Inc., CMI International, McAfee, NCI
Education Sponsors: Concordant, iapp, ICSA labs
Official Media Sponsors: Communications & Networking, Computing Canada, EDGE
Official Radio Sponsor: 680 News All News Radio
Produced and Managed by: Reed Exhibitions

Infosecurity Canada 2006
20 June-21 June 2006 – Metro Toronto Convention Center, Toronto, Canada
http://www.infosecuritycanada.com

Recon 2006
16 June-18 June 2006 – Plaza Hotel Centre-Ville, Montreal, Canada
http://www.recon.cx

HOPE Number Six
21 July-23 July 2006 – Hotel Pennsylvania, New York City, USA
http://www.hopenumbersix.net/

Secure Malaysia 2006
24 July-26 July 2006 – Putra World Trade Centre, Kuala Lumpur, Malaysia
http://www.protemp.com.my

The Third Conference on Email and Anti-Spam (CEAS 2006)
27 July-28 July 2006 – Mountain View, California, USA
http://www.ceas.cc/

Security '06 – 15th USENIX Security Symposium
31 July-4 August 2006 – The Fairmont Hotel Vancouver, Vancouver, B.C., Canada
http://www.usenix.org/sec06/

Biometric Solutions
12 September-13 September 2006 – Husa President Park Hotel, Brussels, Belgium
http://www.biometricsummit.com/

RuxCon 2006
30 September-1 October 2006 – University of Technology, Sydney
http://www.ruxcon.org.au/

Mobile Security
3 October-5 October 2006 – Crowne Plaza, St James, London, UK
http://www.informatm.com/security/?src=net

Infosecurity New York 2006
23 October-25 October 2006 – Jacob K. Javits Convention Center, NY, USA
http://www.infosecurityevent.com

The 11th annual Infosecurty Europe, held on the 25th - 27th April 2006 at the Olympia in London, proved once again to be the most important event for security professionals in Europe.

The show has more than 300 exhibitors and 12,275 visitors (pre ABC audit) compared to 10,974 in 2005, which is a 12% increase.

935 visitors returned on day 2 from day 1 and 875 returned on day 3 from day 2. This just shows how much good information and contacts the event had to offer.

If you were there to improve your knowledge, there was plenty to choose from as 120 speakers worked to deliver keynotes and seminars. Technical sessions included some of the hottest topics at the moment:

- VoIP security
- Patch management
- Identity protection
- The threat of botnets

Among the speakers there were also CEOs that targeted senior managers by discussing the challenges they face today. Very interesting were the panel sessions where one could get answers to some of the eternal questions:

- How much is it really worth spending on security?
- What should I implement immediately to secure the future of my business?

The organizers had a great idea when they introduced “The Lion’s Den” where seven products specialists put their products on the line in front of five senior buyers and authorities in the industry that used their expertise to dismember the offered products.

At Infosecurity, the biggest news was certainly the release of the 2006 DTI Information Security Breaches Survey by PricewaterhouseCoopers and DTI. The survery is the leading source of information on security incidents suffered by businesses. You can download it here - www.tinyurl.com/qswos

SECURE COMPUTING

At Infosecurity, Secure Computing Corporation announced major additions to the former CyberGuard TSP portfolio to support the company's Unified Threat Management offerings. These products include TSP Release 6.4, which integrates Webwasher secure content management features along with enhancements to the TSP firewall and VPN capabilities. Two new products were also added to the TSP product portfolio:

- the TSP 7300 for large enterprises and
- the new TSP 3450J for the medium-sized enterprise.

SurfControl announced that its award-winning family of solutions has been dramatically enhanced to provide around-the-clock protection for all points of Internet content vulnerability.

Game-changing enhancements to SurfControl products include:

- Email Protection: SurfControl Email Filter and RiskFilter
- Web Protection: SurfControl Mobile Filter
- Desktop Protection: SurfControl Enterprise Threat Shield (ETS)


Juniper your Net.
Juniper Your Net.
Sid, I think our security has been compromised, what do you think...Sid?
pointsec
becrypt


TREND MICRO
McAfee
IBM On Demand User Management
postini
INTEGRATED MESSAGE MANAGEMENT
JUST SWITCH IT ON!
THALES
NOD32

Who's guarding your Exchange Server?

Fifi = a single anti-virus engine!

Buster = the real thing!

Get the leading email content security & anti-virus solution!

GFi MailSecurity

Email content/exploit checking, anti-Trojan & anti-virus

If you are serious about mail server protection, get the leading email content security, anti-Trojan and anti-virus solution, **GFI MailSecurity for Exchange/SMTP**, the only product to offer these unique features:

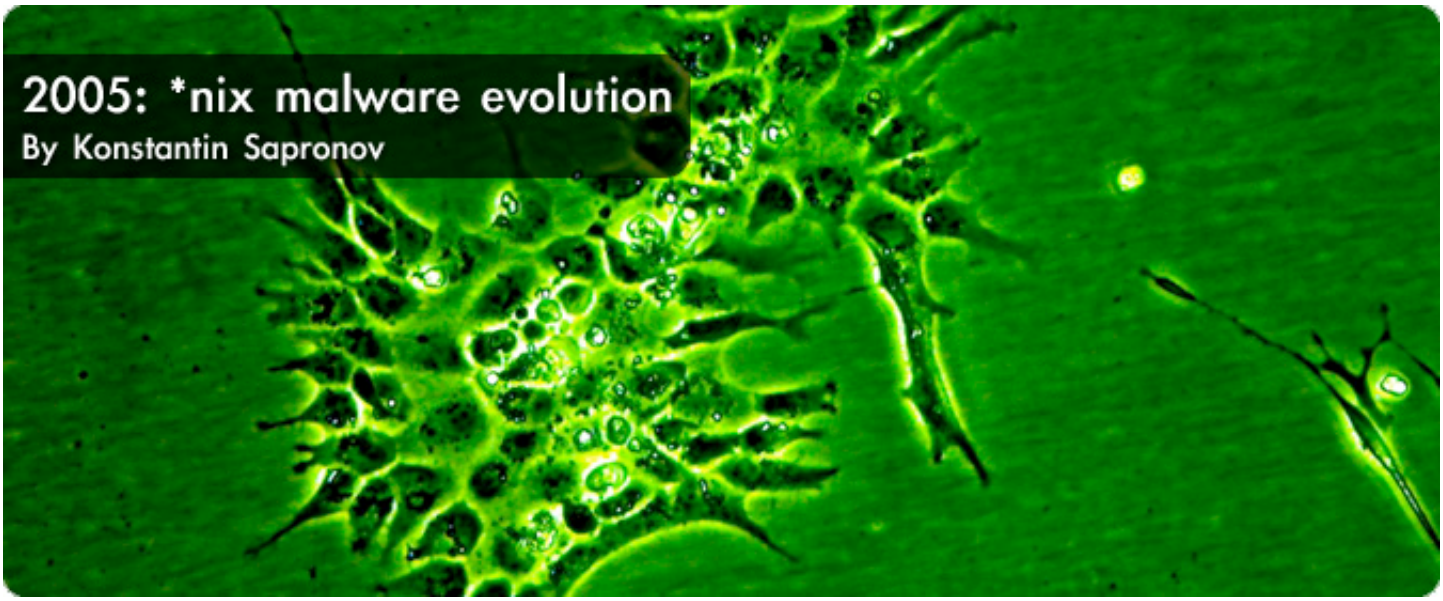
- **Multiple virus engines** – For better security
- **Email content & attachment checking** – Quarantine dangerous attachments and content
- **Email exploit protection** – Perform email intrusion detection and defense
- **HTML threats analysis** – Disable HTML scripts
- **Trojan & Executable Scanner** – Detect potentially malicious executables
- **Server-based anti-spam** – with the GFI MailEssentials bundle!

– Used by customers like NASA, Caterpillar, European Central Bank, MG Rover Group, Toyota & many more

Download your FREE trial from www.gfi.com/insec

GFi NETWORK SECURITY
CONTENT SECURITY
MESSAGING

tel: +1 (888) 243 4329 / +1 (919) 379 3402 | fax: +1 (919) 379 3402 | www.gfi.com/insec



2005: *nix malware evolution

By Konstantin Sapronov

This report covers 2005, and provides an overview of the evolution of malware targeting platforms other than Windows. It includes information on trends; information based on statistics collected throughout 2005, and concludes with forecasts as to how malware for non-Windows platforms is likely to evolve in the near future.

Introduction

Computing history and computer virology did not begin with Windows. Nor did they begin with DOS. The first computer virus, a worm which appeared in 1988, was written for Unix. However, computer virology only really started to evolve with the appearance of millions of machines running under DOS, and then under Windows. Malware evolution reflects the evolution of the computer industry as a whole: the popularity of a platform can be gauged by the number of viruses found in the wild which target the specific platform.

The leading platform is, of course, intel + Win32 (Win32 as a software platform, intel as a hardware platform). More specifically, 32 bit intel is currently the most widely targeted platform. However, the situation is likely to change in the near future as 64 bit platforms become more widely used. Indeed, several proof of concept viruses for Win64 have already been created.

However, where there's a mainstream, there's always an alternative. At one point in time, the main alternative to Windows was OS/2. Today, the alternatives are Linux, FreeBSD and other flavours of Unix. Linux, with its wide variety of implementations, is the undoubted leader.

Slowly but surely Linux is being chosen over Windows not only for servers, but also for desktops. MacOS X's start may also rise; since Apple has switched to intel processors, Macintosh is rapidly gaining popularity.

End user machines are the main target for malware attacks. Trojan programs such as Trojan-Spy, Trojan-Downloader and Trojan-Dropper make up the majority of malicious programs for Win32. In contrast to this, most malicious programs targeting systems running Linux are backdoors. These programs provide remote malicious users with full access to the compromised machine, which can then be used as a launch pad for attacks on other machines.

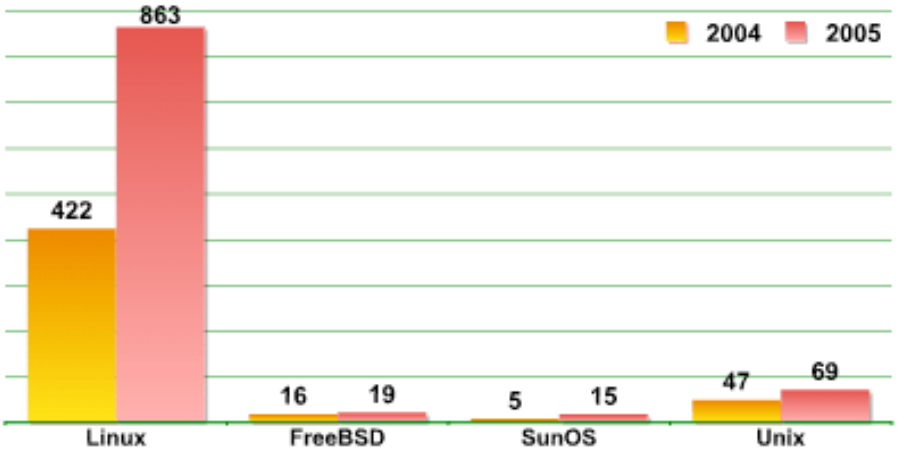
As soon as a platform starts becoming more popular, viruses and other malicious programs for this platform will begin to appear. Initially, such programs will be proof-of-concept (PoC); they are designed to show that it is possible to infect a machine in a particular way, and do not, as a rule, have a malicious payload. Firstly, information about a specific vulnerability in an operating system or an application will be made public. This information is then used to create exploits or backdoors which target the vulnerability.

Of course, software developers issue patches for known vulnerabilities, but this results in virus writers searching for new methods and weak spots to attack. Overall, malware gains momentum in a snowball like fashion. This is what is currently happening with Win32; although this has not yet happened with malware for other platforms, the key phrase here is almost certainly 'not yet'. In spite of the relative peace enjoyed by non-Windows users, alternative platforms are also subject to attack by malicious programs. The following sections of this report cover certain features of alternative platforms and evolutionary trends.

Statistics

The process of malicious code evolution has been described above in detail to enable better understanding and interpretation of the data presented below.

Information in this section covers the evolution of malware for unix type systems. The graph below shows that in comparison with 2004, there was a significant increase in all types of malicious program classified by Kaspersky Lab as MalWare.



The almost 100% increase on last year's figures shows that virus writers are almost overwhelmingly targeting systems running Linux.

This is not at all surprising as Linux is the most popular Unix-type system. It should be mentioned that in spite of the fact that Linux functions on a variety of RISC platforms, binary files which differ from x86 occur very rarely. Under other RISC platforms, such as SPARC, it would be more common to encounter binary files for SunOS. As a rule, such samples are usually a collection of small utilities which are written and compiled for specific versions of an operating system, and designed to target a specific server; for example, a sniffer, backdoor, logcleaner, and kernel modules to mask the attacker's actions - such a collection is called a rootkit. Rootkits are designed for an attack on a particular machine; such a specific attack is far harder to combat than a Trojan launched by a script kiddie.

The major difference between malware targeting Unix and malware targeting Win32 MalWare is the absence of packers. Packers are frequently used to hinder the detection and analysis of malicious programs. However, we have only seen UPX and a few modified versions used in Unix malware.

Overall, in terms of types of malicious code, the Unix picture mirrors that on the Win32 front. The number of viruses which infect files on the local disk is decreasing. Such viruses are usually created for research interest only, and do not have a malicious payload; however, viruses with buggy code may deliver an unintentional malicious payload in that they corrupt the file when injecting their code. There have been no epidemics caused by Unix viruses, and in general they are viewed as 'collection' viruses.

Nevertheless, some Unix malware is interesting: one example is Virus.Linux.Grip, which uses the brain fuck interpreter to generate key codes. The codes are then used for TEA (Tiny Encryption Algorithm) encryption.

However, this is only really of interest to researchers, and has no practical application. Those who write such viruses are, perhaps, acting on the Linus Torvalds philosophy of 'just for fun'.

Programs which are written in order to compromise servers, so that they can then be used as platforms for future attacks, are a different matter. There are many such programs, including backdoors, exploits, sniffers, floodders and other hacktools. The number of such programs is increasing exponentially with the popularity of Linux itself.

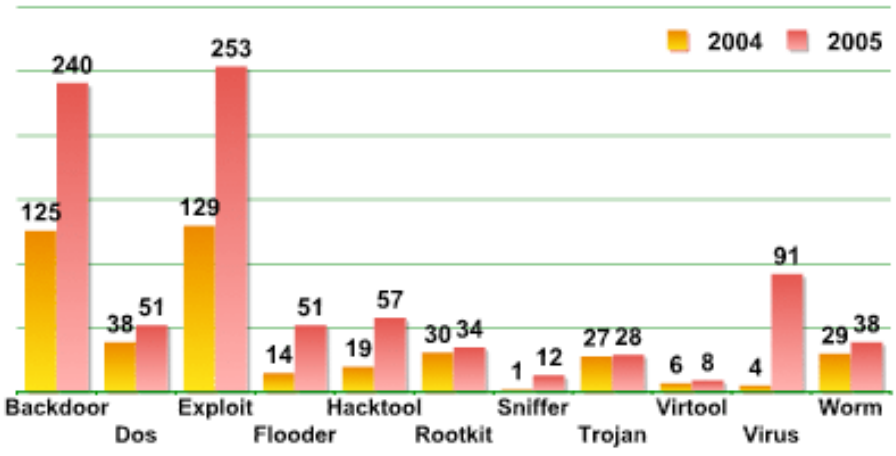
Last year, a number of worms for Linux were detected, including Net-Worm.Linux.Lupper and Net-Worm.Linux.Mare, a variation on the theme introduced by Lupper. Both these worms exploit the same vulnerability, and have similar propagation methods. One component which the worms included was the Tsumani backdoor. As the worm evolved (i.e. as new variants were created), new functionality was added. The most recently detected variant of Net-Worm.Linux.Mare downloaded an ircbot, which acted as a backdoor.

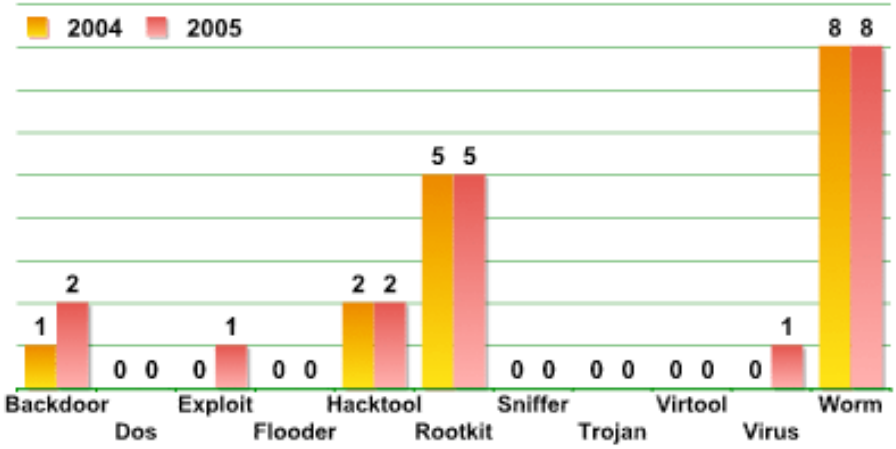
Another malware incident in the Linux world in 2005 occurred in September, when a Korean Mozilla distribution placed on a public server was found to be infected. The distribution contained binary files infected with Virus.Linux.Rst.

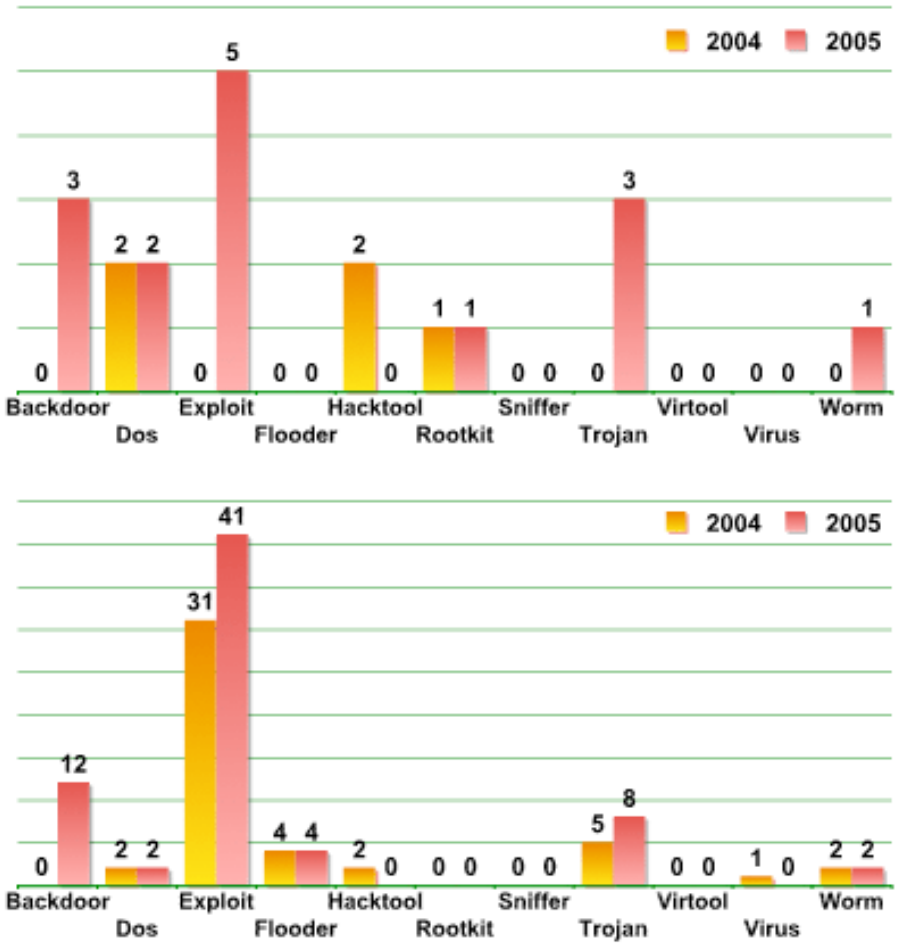
These were the only significant events caused by Linux malware in 2005. In comparison with the epidemics caused by Scalper and Slapper in 2002 and 2003, it was a quiet year.

Rootkits are a hot topic for the media; however, in contrast to the extensive activity in the Win32 world, there has been no really new rootkits for Linux, simply variations on old themes. As for other Unix platforms, the situation is even quieter. However, this is understandable; after all, other Unix platforms cannot compete either with Linux or Windows in terms of popularity.

The data presented below has been compiled from repeated analysis of the Kaspersky Lab antivirus databases at varying points in time. Some categories contain no data; this means that the Kaspersky Lab collection does not contain any malware targeting the designated platform from these families.







The future

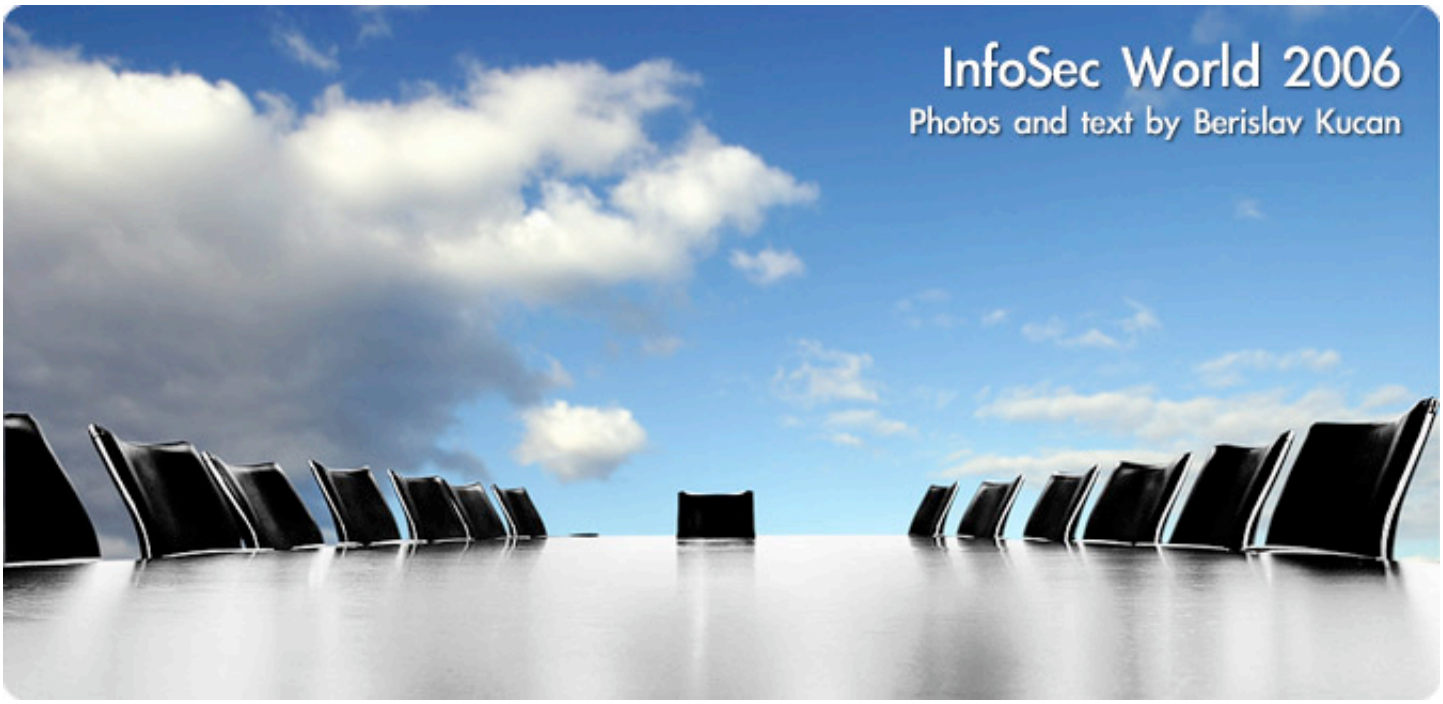
It's well known that making predictions is a risky game, as anything can happen in the course of six months. However, we're going to take that risk. Above all, the era of 64 bit architecture is dawning; once such architecture is firmly entrenched on users' machines, virus writers will react to this fact. There are of course complications here, such as the fact that binary code for AMD64 and for IA64 are different, and this means that separate versions will have to be compiled for each platform.

Apple gives even more scope for development and malware evolution; the move to intel processors may be revolutionary. The fact that Apple computers have excellent design, and that OS X could be called 'Unix with a human face' may make it a hit among PC users.

The OS X kernel is based on FreeBSD, and the experience and ideas applied to the creation of malware for FreeBSD may also be applied to create OS X malware. In addition to this, the operating system developers have also made errors. Over the past few weeks, we've seen two proof of concept worms for OS X, and these clearly illustrate errors in the system architecture. There has also been an exploit for the Safari web browser, which makes it possible to launch a script and execute commands on the user's computer. It therefore seems clear that OS X may be fertile soil for security researchers.

Another rapidly developing arena is mobile devices. Here Linux is also offered as an alternative to Symbian and Windows Mobile. Many major manufacturers have either already developer, or planning to offer devices with Linux. The only thing that is needed to encourage the evolution of Linux mobile malware is a critical mass of users. It may be that the development of some, as yet unknown or little used, technology will also act as a stimulus for malware evolution. Technologies and propagation methods which seem exotic today - - such as Bluetooth a few years ago - may shortly become industry standard for mobiles and PCs alike.

Konstantin Sapronov works at Kaspersky Lab, a leading developer of secure content management solutions that protect against viruses, Trojans, worms, spyware, hacker attacks and spam.



At the beginning of this April we attended InfoSec World 2006 in Orlando. Organized by MIS Training Institute, the event was held at the Coronado Springs Resort, popular venue located by one of the beautiful lakes in the Disney area.

InfoSec World 2006 attracted more than 1,700 attendees which is an increase of more than 200 over their 2005 event. In addition, the 144 companies exhibiting provided attendees with a rich representation of products and technologies in the security marketplace.

"We continually seek to provide highly relevant sessions and engaging speakers to our events," said Conference Chair, Ken Cutler, CISSP, CISM, CISA, Vice President, Information Security, MIS Training Institute. "We're proud to see that these efforts have paid off with a significant boost in attendance and very positive feedback from exhibitors and attendees alike."


WEBSENSE


INFOSEC
WORLD
CONFERENCE
& EXPO 2006
INFOSEC
WORLD


McAfee
Proven Security

The Region's Leading Information Security Event

SecureMalaysia2006

Conference & Exhibition

24 - 26 July 2006 • PWTC, Kuala Lumpur

Secure Malaysia 2006, Malaysia's international information security event is undisputably the region's leading event to address issues in information security and promote collaboration between industry players.

Secure Malaysia 2006 Exhibition is held over 3 days bringing you advanced technologies aim to secure information in this era of advanced information sharing. Leading industry players will be exhibiting and sponsoring Secure Malaysia 2006. So ensure your presence at the exhibition and conference to meet new and existing clients.

Attractions:

- A 2-day international conference jointly organised by ISC² and NISER, featuring prominent and globally recognised speakers. Log on to our website for full details of our high powered speakers.
- Held concurrently with CardEx Asia 2006, Asia's 6th Card Conference & Exhibition.
- Introducing RFID Expo Asia and meeting the growing demand for RFID technology in Asia.
- The 2nd D'UCOTY Awards, recognising industry excellence in the smartcard industry.

Conference Organised by: (ISC)² NISER

Exhibition Organised by: protemp Protemp Exhibitions Sdn Bhd

Concurrent Events: CardEx Asia 2006 Conference & Exhibition; RFID expo ASIA Exhibition

Protemp Exhibitions Sdn Bhd
Tel: 603- 6140 6666 • Fax: 603-6140 8833 • E-mail: karendass@protemp.com.my

www.informationsecurityasia.com