

# (IN)SECURE

OPEN. INFORMATIVE. TO THE POINT. Issue 6 - March 2006



**QUANTIFYING THE COST OF SPYWARE TO THE ENTERPRISE  
HOW TO WIN FRIENDS AND INFLUENCE PEOPLE WITH  
IT SECURITY CERTIFICATIONS  
BEST PRACTICES IN ENTERPRISE DATABASE PROTECTION**

# TABLE OF CONTENTS

**Page 04 - Corporate security news**

**Page 07 - Quantifying the cost of spyware to the enterprise**

**Page 11 - How to win friends and influence people with IT  
security certifications**

**Page 13 - Latest additions to our bookshelf**

**Page 15 - Best practices in enterprise database protection**

**Page 18 - Security for websites - breaking sessions to hack  
into a machine**

**Page 21 - Events around the world**

**Page 22 - The size of security: the evolution and history of  
OSSTMM operational security metrics**

**Page 30 - Interview with Kenny Paterson, Professor of Information  
Security at Royal Holloway, University of London**

**Page 32 - Software spotlight**

**Page 33 - War-driving in Germany - CeBIT 2006**

**Page 38 - PHP and SQL security today**

**Page 43 - Apache security: Denial of Service attacks**



## Welcome to (IN)SECURE 1.6 the digital security magazine

Welcome to another issue of (IN)SECURE. As always, we bring you topics that will cater a variety of knowledge levels and I'm sure you'll find them interesting.

I would like to take this opportunity to thank Wendy Nather, the Information Security Officer for the Texas Education Agency that has donated her valuable time to help us make (IN)SECURE better.

If you're interested in writing for us, do drop me an e-mail with the idea. As always, comments and suggestions are much welcome.

Mirko Zorz  
Chief Editor

Visit the magazine website at [www.insecuremag.com](http://www.insecuremag.com)

### **(IN)SECURE Magazine contacts**

Feedback and contributions: Mirko Zorz, Chief Editor - [editor@insecuremag.com](mailto:editor@insecuremag.com)

Marketing: Berislav Kucan, Director of Marketing - [marketing@insecuremag.com](mailto:marketing@insecuremag.com)

### **Distribution**

(IN)SECURE Magazine can be freely distributed in the form of the original, non modified PDF document. Distribution of substantively modified versions of (IN)SECURE Magazine content is prohibited without the explicit permission from the editor. For reprinting information please send an email to [reprint@insecuremag.com](mailto:reprint@insecuremag.com) or send a fax to 1-866-420-2598.

# Corporate security news



## F-Secure Mobile Anti-Virus for Nokia S60 3rd Edition Devices



F-Secure and Nokia have been cooperating in the area of increasing content security for years and have jointly developed distribution models for antivirus solutions. From 2004 onwards, F-Secure Mobile Anti-Virus clients have already been available through Nokia to the users of select Nokia's smartphone models. In addition, F-Secure Mobile Anti-Virus clients have been included into some operator variants of Nokia's mobile devices.

F-Secure Mobile Anti-Virus provides increased real-time, on-device protection against harmful content with automatic over-the-air antivirus updates. It is the world's first and most widely available mobile operator antivirus service. The new F-Secure Mobile Anti-Virus 3.0 supports devices based on Symbian OS v9 and the S60 3rd Edition platform.

## Sophos Launches Fully Integrated Email Security Appliance

Sophos launched the industry's first fully integrated managed email security appliance. Featuring an intuitive web-based interface and automated security updates, the enterprise-grade ES4000 protects against the growing threat of viruses, Trojans, spyware, spam and policy abuse in both inbound and outbound email traffic. With automated virus and spam protection updates delivered every five minutes, Sophos's ES4000 security appliance can process millions of email messages each day. Its innovative 24-hour 'heartbeat' remote monitoring, built-in diagnostics and on-demand remote assistance offer additional support to the email security manager, ensuring uptime whilst greatly reducing administration.



Qualified businesses can take advantage of a free 30-day trial of the ES4000, which will be available from Sophos's network of channel partners.

## Aladdin eToken NG-FLASH: Flash Mass Storage Combined with USB Authentication



Aladdin Knowledge Systems announced eToken NG-FLASH, a device that will combine the powerful capabilities of strong authentication with the convenience of a mass storage drive. The new eToken is scheduled for general availability by April 2006. The USB-based eToken NG-FLASH will be initially introduced in three sizes – 128 MB, 512 MB and 1 GB. Organizations and solution partners will now be able to offer eToken users both the token itself as well as information they need to use while accessing secured data. With Aladdin eToken NG-FLASH, the auto run feature stands as a key benefit, enabling solution providers to pre-load applications and data, and run it directly from the token.

About the size of an average house key, the award-winning Aladdin eToken is easy to use and highly portable, providing users with powerful authentication by requiring something they have, the tamper-proof eToken, and something they know, a password. It is used for secure network logon, secure VPN, Web Sign-On, Single Sign-On, secure email, and numerous other applications. eToken USB and traditional smart card form factors are available with RFID capabilities and one-time password technology. For more information, visit [www.Aladdin.com/eToken](http://www.Aladdin.com/eToken).

## Blue Coat Enables Organizations to Control Skype

Blue Coat Systems, Inc. announced its ProxySG appliances have the ability to control Skype to protect against information leakage and unauthorized “back channel” communications as well as potential future malware. Using ProxySG appliances, organizations can allow or deny access to Skype in total or based on network user name and/or group.



Blue Coat's Skype control makes use of its recently introduced SSL proxy technology, which enables visibility and control of encrypted Secure Sockets Layer (SSL) communications between internal enterprise users and external Internet applications. The ProxySG appliances can differentiate between SSL traffic and other encrypted traffic that uses the firewall's fully open port 80 (HTTP) or 443 (HTTPS). The Skype controlling capabilities can be enacted by adding a simple policy to ProxySG. The pre-written policy is described in a new tech brief from Blue Coat available on the corporate Website at [www.bluecoat.com/downloads/support/tb\\_skype.pdf](http://www.bluecoat.com/downloads/support/tb_skype.pdf).

## VeriSign Introduces Security Risk Profiling Service



VeriSign, Inc. announced the VeriSign Security Risk Profiling Service, the industry's first comprehensive solution to help enterprises identify, visualize and quantify information security risks. The VeriSign Security Risk Profiling Service enables enterprises to make better operational and financial decisions by providing a holistic view of threats, vulnerabilities, network access policies and business impacts and then generating a dynamic risk score based on those factors at a device, business unit, and enterprise level. The service extends VeriSign's portfolio of enterprise risk-management solutions which include VeriSign Managed Security Services, VeriSign Global Security Consulting, and VeriSign iDefense Security Intelligence Services. The service includes sophisticated simulation and modeling technology to help customers understand the impact of emerging threats and potential network security policy changes, and to measure compliance with both internal and external policies and regulations. For more information go to [www.verisign.com/mss/riskprofiling](http://www.verisign.com/mss/riskprofiling)

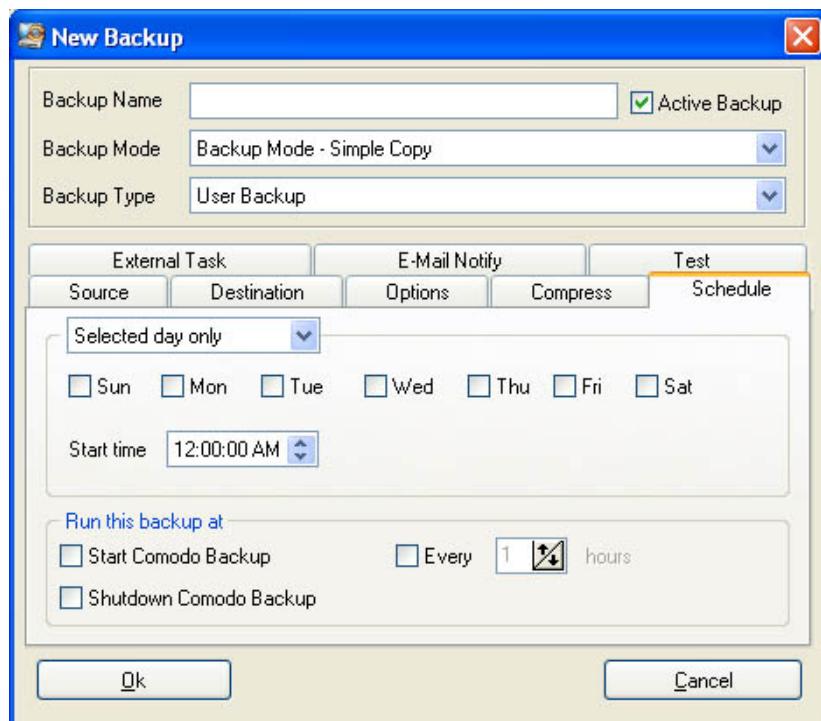
## Neoscale Unveils CryptoStor KeyVault For Multivendor Storage Encryption Key Management

NeoScale Systems Inc. announced CryptoStor KeyVault, the industry's first open security key management system to deliver centralized management of both NeoScale encryption appliance keys and those from third-party storage encryption vendors. With CryptoStor KeyVault, organizations can centrally manage and distribute encryption keys among multiple internal locations, to disaster recovery sites, and to business partners, to facilitate information recovery from any authorized location.



A FIPS 140-2 Level 3 tamper-proof chassis ensures the KeyVault foundation of security is solid. All hardware, software, firmware, and user operation is covered by FIPS certification, leaving no weaknesses. Building on that foundation, secure communications between the KeyVault system, NeoScale appliances, and third-party key management systems is assured with mutual session authentication using public/private key pairs and SSL/TLS protocols.

## Comodo Release Free Windows Automatic File Backup and Recovery Tool



Comodo Inc. announced the release Comodo BackUp, the automated file duplication and recovery tool for Windows XP/2000 that allows users to quickly and easily schedule ongoing backups of critical files. Free of charge, the release addresses a security hole for many users who, whilst acknowledging that regular backups are important, have not yet implemented a solution due to concerns over difficulty and cost. Suitable for home users and network administrators alike, Comodo BackUp protects data from system crashes, accidental deletion and corruption from viruses by generating a safe backup copy of valuable files. Backups can be saved to local and network drives as well as FTP servers and CD/DVD rewriters. Should the original files become damaged or lost, users can quickly recover them using Comodo BackUp's one touch 'restore' feature. For more information, do visit [www.comodo.com](http://www.comodo.com)

# Quantifying the cost of spyware to the enterprise

By Bryan Gale



**Spyware has become one of the biggest security and productivity threats on enterprise desktops today, and as a result, the cost to organizations is increasing by the day. The impact of spyware ranges from annoying to dangerous, and spyware programs are draining organizations of millions in lost productivity, IT costs, and stolen intellectual property, customer data, and financial assets. As such, protection from spyware has become a top-line item for CIOs across the globe.**

In fact, a recent report from Forrester shows just how high-profile the threat has become:

"In January 2005, Forrester conducted a survey of roughly 200 technology decision-makers from North American SMBs and enterprises. The results show that spyware was considered the No. 4 threat to these organizations. However, when we asked this same question in June 2005 to SMBs, the spyware threat had moved up to No. 2, while viruses and worms took the No. 1 spot." - The Forrester Wave: Enterprise Antispyware Q1 2006.

Spyware is already infecting the vast majority of enterprise PCs. In its Q4 2005 State of Spyware Report, Webroot Software reported that its Enterprise SpyAudit had seen system monitors increase by 50% each of for the three previous quarters. And while most IT managers understand the significance of the threat, many are not able to clearly identify and estimate the costs associated with spyware in their organizations. Here we will examine some of these costs and attempt to put a price on the effects of spyware on your enterprise.

## Spyware's Direct Costs: What Spyware Is Costing Your Company Right Now

With spyware widespread throughout the enterprise, businesses today are incurring significant soft and hard costs from decreased employee productivity and IT time spent detecting and cleaning up infected systems.

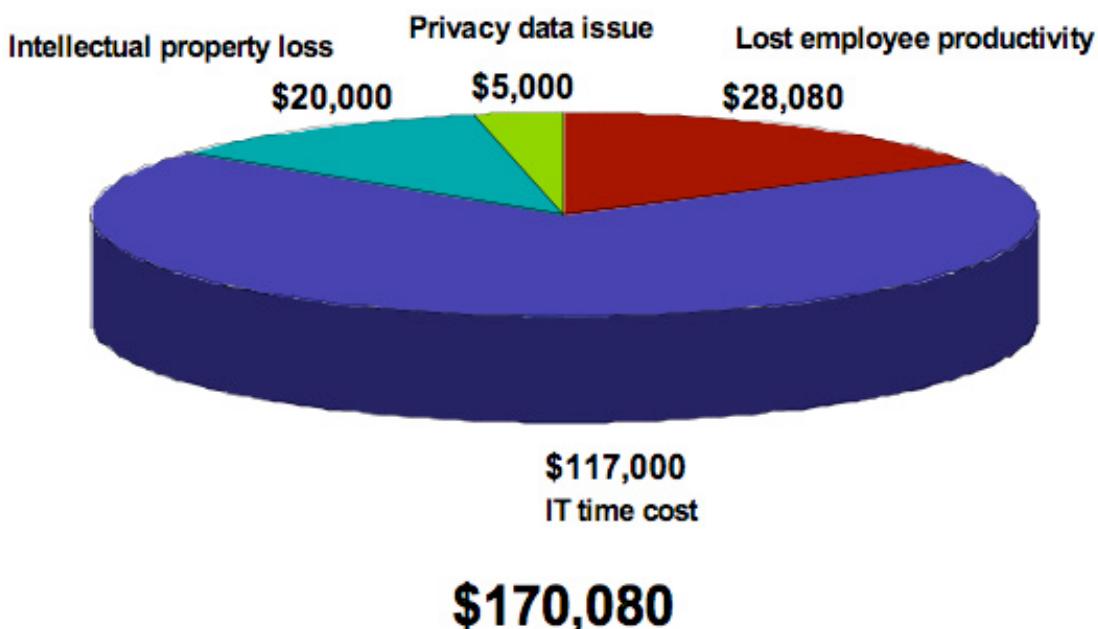
### Lost Employee Productivity

It is a well-documented fact that spyware has a direct and very real impact on employee productivity. Employees with spyware-infected PCs are often hindered by slowed system performance, and they can lose significant time and important data to computer crashes.

While costs related to a decline in system performance or crashes can be significant, they are difficult to quantify and thus are not included in our analysis. We will instead focus on the costs associated with productivity losses incurred while employees' systems are being cleaned and repaired from spyware infection.

# Cost of Spyware

Estimated annual costs for a company with 2,000 PCs



With the pervasiveness of spyware on enterprise computers, spyware-related troubleshooting and repairs can result in a considerable amount of lost time to a company's staff. An employee can lose hours trying to locate and remove spyware programs themselves or working with help desk support staff. If a particular instance of spyware is resistant to removal, even more time is lost.

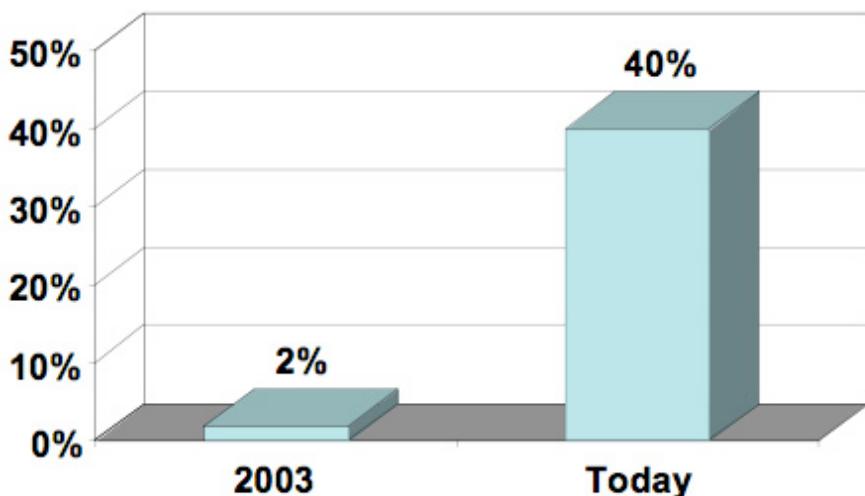
In a typical case, IT staff would start by spending time investigating and troubleshooting the problem. Then additional time might be spent repairing or rebuilding the hard drive.

Finally, the user's applications and data would need to be restored.

An employee could lose hours of productive work time to a single instance of spyware removal.

To calculate the real costs of this impact on productivity, consider this scenario: Based on industry averages, a company with 2,000 PCs spends approximately eighteen hours per week resolving spyware-related desktop issues. Using the industry average value of \$30 per hour of employee time, that would mean a loss of more than \$28,000 in your employees' annual productivity.

## % Spyware-related support calls



Source: Brian Burke, IDC Analyst

## IT Costs

To figure the costs of spyware to your IT department, consider that Gartner estimates the average cost of repairing one spyware-infected PC to be \$375. At an industry average of three weekly incidents per 1,000 workstations, a business with 2,000 desktops stands to lose \$117,000 annually for IT time spent dealing with spyware.

Clearly, the daily costs of spyware to the enterprise are considerable. And with spyware-related support calls on the rise, this is a problem that corporations have to address today.

## The Risks Posed by Spyware: Can Your Business Afford Not to be Protected?

Malicious spyware – the most dangerous threat to the enterprise – is currently infecting a surprisingly high number of enterprise PCs. When you consider that a single instance of these malicious spyware programs poses a serious threat to the security of an enterprise network, companies should not ignore the issue. When a security breach occurs, the costs to an organization can be astounding. Malicious forms of spyware are putting companies at risk for considerable losses to theft of customer data, intellectual property, and financial assets.

## Compromised Customer Data and Consumer Privacy

For a business, the cost of losing its customers' personal data can be devastating to its brand, its reputation, and to its bottom line. With spyware's ability to compromise customer privacy, companies are more exposed than ever to the costs associated with lawsuits and breaches of legislation. California's Security Breach Information Act, for example, stipulates that a company must notify customers whenever their personal information may have been compromised or face possible injunctions and civil lawsuits. Industry-specific privacy regulations also closely govern how companies handle customer data, such as the Gramm-Leach Bliley Act for finance-related industries and the Health Insurance Portability and Accountability Act (HIPAA).

Many high-profile customer privacy breaches have been reported recently, including the LexisNexis case in which 310,000 people's personal information was exposed to unauthorized individuals who compromised the security of a massive database

of public and private information. It is not easy to quantify the substantial negative impact that a publicly announced privacy incident inflicts on a company's brand and reputation to its customers.

## Stolen Intellectual Property

It is difficult to put a dollar figure on the value an organization places on its intellectual property (IP). A recent 2005 report from the FBI estimates that approximately \$62 billion in financial damages occurred due to spyware and other computer-related crimes.

## Cybertheft of Financial Assets

Spyware poses a serious threat when used by cyber thieves. Keyboard loggers and screen capture applications can steal passwords and other sensitive information, leaving businesses vulnerable to theft of financial assets. The damage that spyware can inflict on an organization is significant. Consider last year's cyber theft incident in which a keylogger was used to attempt to steal \$423 million from Sumitomo Mitsui bank. One such spyware-related theft could be devastating to a company, both in the financial loss and the impact to its corporate reputation.

As described, the impact of a single instance of malicious spyware on an organization can be enormous. A spyware infection can lead to serious financial losses and devastate a company's relationship with its customers. With the high rate of spyware infection in corporate PCs today, organizations are realizing the vital importance of being protected from spyware at the enterprise level.

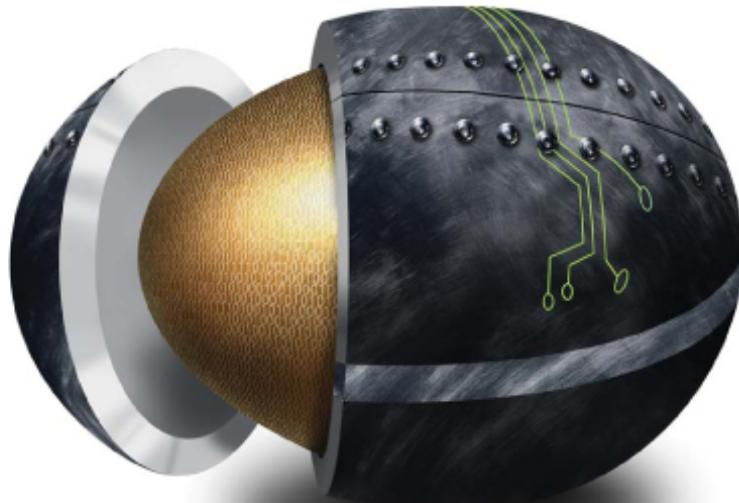
## Conclusion

In summary, businesses today are incurring considerable costs because of the prevalence of spyware in the enterprise. Spyware is having a negative impact on employee productivity and draining valuable IT resources. Even more threatening, however, is the significant level of risk that corporations face from spyware infection – from a devastating financial loss to IP theft to the resulting effects on corporate brand perception. It is critical that corporations put defenses in place to protect their networks from spyware, and to tackle the mounting costs of managing this pervasive problem. To reduce spyware-related costs and maximize protection, IT professionals should seek the most robust enterprise-level spyware solution possible.

Bryan Gale, Webroot Enterprise Product Management. Gale manages the core development teams tasked with building out and upgrading Webroot's market-leading enterprise anti-spyware solution, Spy Sweeper Enterprise.



**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](http://www.infosecuritycanada.com/secure)

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

(ISC)<sup>2</sup> The conference program at Infosecurity Canada includes the preeminent Security Leadership Conference Series. Only (ISC)<sup>2</sup>, 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](http://www.infosecuritycanada.com/besecure)

**REGISTER BY 5/01/06 FOR EARLY-BIRD CONFERENCE DISCOUNTS AND FREE EXHIBITION ADMISSION.**  
[www.infosecuritycanada.com/besecure](http://www.infosecuritycanada.com/besecure)

Premier Education Sponsor:



Global Sponsor:



Diamond Sponsor:



Platinum Sponsor:



Gold Sponsor:



Silver Sponsor:



Bronze Sponsors:



APPLICATION SECURITY, INC.



Education Sponsors:



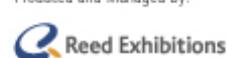
Official Media Sponsors:



Official Radio Sponsor:



Produced and Managed by:



# How to win friends and influence people with IT security certifications

By Peter Berlich



**"If you do not see the way, you do not see it even as you walk on it."**  
**(Zen Koan)**

**Huddled over a drink at the Appelmans Brasserie (and Absinthe Bar - plus, they have free Internet access) in Antwerp is a good moment to think about one's past career. (I recommend a different drink when contemplating future plans.)**

My “real” career in Information Security started less than a decade ago. At the time, I was hired into a role as IT Security Manager on the grounds of technical expertise. I had had little formal training in IT Security or managerial matters, but figured I was up to the technical side of the job and certainly had very concrete ideas on what needed fixing. Although my university degree is in natural sciences, it has provided me with a good foundation for a career in IT. Yet, at some point I felt that formal qualification of my expertise, knowledge and skill was needed. I decided to acquire a security certification, in particular the CISSP (Certified Information Security Systems Professional).

Even though CISM (Certified Information Security Manager) was not yet available at the time, I’m not sure it would have changed anything. I went for the CISSP certification because it offered the best match for my role and it was the most widely accepted. Plus, from what I had heard among my peers, it was on its way to become a de-facto requirement for Information Security practitioners.

When I started studying for the exam I had two main motives:

- I wanted an independent confirmation and assessment of my skills. In my company, I was seen as the key point of reference for questions on IT and Information Security. I felt an obligation to my employer to verify that my skills matched market best practices.
- I saw a need to improve my employability. I was approaching a point in my career where it would be appropriate for someone else to take over my responsibilities, injecting new ideas and new energy, setting some fresh initiatives where I had seen no priority, and maybe coming back on certain compromises.

Suffice to say, obtaining the CISSP proved to be straightforward. I mean this as an encouragement to all of you who are contemplating taking the test. Go and do it, as an investment in your own future.

As the name implies, the CISSP certification is IT Security focused. Becoming a CISSP will not magically turn someone into a security expert, though. CISSP demonstrates you’ve got the basics of your profession right. That’s a lot, but it isn’t everything. Your experience is what will differentiate you.

## From technical to managerial

As I quickly learned, technical proficiency alone can be deceptive. This will not come as too much of a surprise to those who have ever had any type of security-related role. It helps to be technically proficient (and for a long time that was a basis I could always fall back on), but acting as a technical expert did not get me ahead of the game in my role. Corporations will function or fail on a managerial level and that is true for the security, risk and compliance field as well.

But what can one do to change the perception of security as a technical problem? It has long been my conviction that in order to induce change in others, it is yourself who has to change. As a personal career decision and in order to be successful in my role, I decided to leave technology alone.

This can be surprisingly hard and to be honest, took me several years and one new employer (I'll leave it to debate whether I'm quite through with it). It implies repositioning yourself and your role within your organization. It can be even harder to suppress your knowledge of solutions (which may still surpass your peers' and subordinates') and accept that from now on you will delegate technical problems in order to gain a comparative (and sometimes a competitive) advantage.

Focusing on management is certainly worthwhile and it can be fun to learn. Shortly after it became available, I obtained the ISSMP (Information Systems Security Management Professional) concentration on top of my CISSP certification. My motivation for this was different from the first time around. I no longer felt I had to prove anything to myself or others, but I wanted to use the Concentration to position myself within the field and increase the profile of my personal brand.

### Today, tomorrow

The public and private sectors put IT Security on top of their agenda these days, and, as a result, the IT and Information Security job market is growing. At some point though, the market will saturate as businesses seek to curb their investments, security services become more standardized and IT as a whole moves to a more service-oriented business model. Is your career strategy ready?

From my own experience, I see a certain logical sequence of actions in career progression:

- Novices probably should aim for at least one type of formal qualification. Be it CISSP or something else, it will be your key to unlock the IT Security market for you, and in the near future may become a formal requirement for the more senior positions. Start networking.

If you do have a technical background, aim for managerial courses and possibly mid- to long-term for the proverbial MBA (Master of Business Administration).

- Experienced practitioners need to consider the direction in which they want to develop themselves. Get an advanced degree but stay focused. Are you a jack of all trades and a master of none? I hope not.

If you haven't built a good network by now, it's high time. It doesn't matter so much where you get your benchmark from as long as you are in touch with your peer group. It will gain you a reference point and keep you sane.

- Senior IT Security people, you may be on top of your game but do you have an exit strategy for when the market matures? Will you be able to defend your role against younger incumbents? At what level can you function as a line manager or in another staff function?

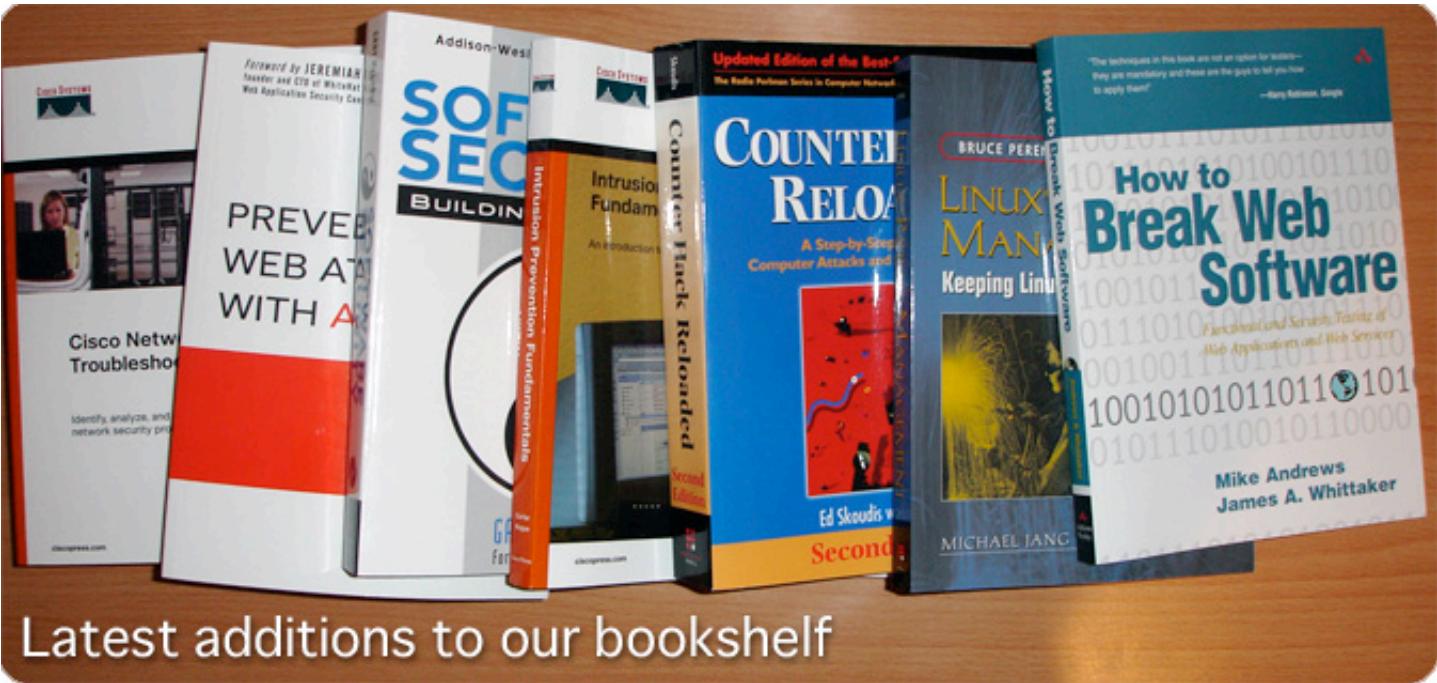
You have all the qualifications you will need and you will have built a strong network. It will be hard for you to bid good-bye to it all, but brace yourself for moving on. Be prepared to prove your value, your proficiency and your potential definitely at every point.

In a nutshell, build your career plan on your strengths and ambitions. Decide early on whether you want to be a top expert or a good manager and stick to your strategy. Adapt and maintain it with reason, and don't confuse hedging your bets with keeping all options open. Progress requires focus.

On a related note, make a conscious decision to stay open-minded. More important than climbing the ladder fastest is the ability to grow as a person and take new perspectives.

The hallmark of a true leader is not just the ability to influence, but openness to learn from others.

Good luck!

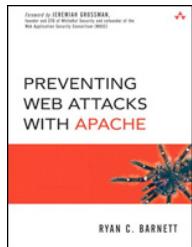


## Latest additions to our bookshelf

### Preventing Web Attacks with Apache

by Ryan C. Barnett

Addison-Wesley Professional, ISBN: 0321321286

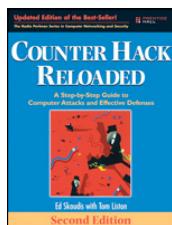


Preventing Web Attacks with Apache brings together step-by-step guidance, hands-on examples and tested configuration files. Building on his groundbreaking SANS presentations on Apache security, Ryan C. Barnett reveals why your Web servers represent such a compelling target, how significant exploits are performed, and how they can be defended against. Exploits discussed include: buffer overflows, denial of service, attacks on vulnerable scripts and programs, credential sniffing and spoofing, client parameter manipulation, brute force attacks, web defacements, and more.

### Counter Hack Reloaded : A Step-by-Step Guide to Computer Attacks and Effective Defenses

by Edward Skoudis, Tom Liston

Prentice Hall PTR, ISBN: 0131481045



This is a second edition of Skoudis' popular book released back in 2002. With almost 45 percent new material, Counter Hack Reloaded, Second Edition, systematically covers the latest hacker techniques for scanning networks, gaining and maintaining access, and preventing detection. With this book you should learn exactly how to establish effective defenses, recognize attacks in progress, and respond quickly and effectively in both UNIX/Linux and Windows environments.

### Software Security: Building Security In

by Gary McGraw

Addison-Wesley Professional, ISBN: 0321356705

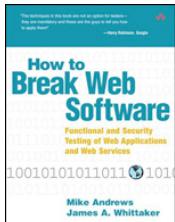


Beginning where the best-selling book Building Secure Software left off, Software Security teaches you how to put software security into practice. The software security best practices, or touch points, described in this book have their basis in good software engineering and involve explicitly pondering security throughout the software development life-cycle. This means knowing and understanding common risks, designing for security, and subjecting all software artifacts to thorough, objective risk analyses and testing.

## **How to Break Web Software: Functional and Security Testing of Web Applications and Web Services**

by Mike Andrews, James A. Whittaker

Addison-Wesley Professional, ISBN: 0321369440



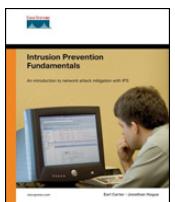
This is a really interesting book that holds all the important details on the typical insecurities of web applications. Written in a very easy to follow way, the authors provide a lot of practical examples on both ways to hack applications, as well as to secure them.

“How to Break Web Software” is accompanied with a companion CD that holds the majority of products covered, as well as some useful pieces of code discussed throughout the book.

## **Intrusion Prevention Fundamentals**

by Earl Carter, Jonathan Hogue

Cisco Press, ISBN: 1587052393



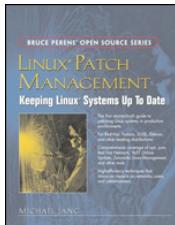
Intrusion Prevention Fundamentals offers an introduction and in-depth overview of Intrusion Prevention Systems (IPS) technology, especially Cisco’ products. Using real-world scenarios and practical case studies, this book walks you through the life-cycle of an IPS project—from needs definition to deployment considerations.

Implementation examples help you learn how IPS works, so you can make decisions about how and when to use the technology and understand what “flavors” of IPS are available.

## **Linux Patch Management**

by Michael Jang

Prentice Hall PTR, ISBN: 0132366754



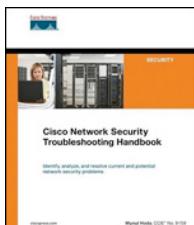
This book presents presents patching solutions for Red Hat, Fedora, SUSE, Debian, and other distributions. The author systematically covers both distribution-specific tools and widely used community tools, such as apt and yum.

Linux Patch Management provides Linux professionals start-to-finish solutions, strategies, and examples for every environment, from single computers to enterprise-class networks. This title is a part of the well known Bruce Perens’ Open Source Series.

## **Cisco Network Security Troubleshooting Handbook**

by Mynul Hoda

Cisco Press, ISBN: 1587051893



Cisco Network Security Troubleshooting Handbook can help you analyze current and potential network security problems and identify viable solutions, detailing each step until you reach the best resolution.

Through its modular design, the book allows you to move between chapters and sections to find just the information you need. Chapters open with an in-depth architectural look at numerous popular Cisco security products and their packet flows, while also discussing potential third-party compatibility issues. By following the presentation of troubleshooting techniques and tips, you can observe and analyze problems through the eyes of an experienced Cisco TAC or High-Touch Technical Support (HTTS).



## Best practices in enterprise database protection

By Ulf Mattsson

**Organizations are now required to protect sensitive data, or face the wrath of public consequences - be that public disclosure to your customers or regulatory non-compliance. With growing incidents of intrusions across industries and strong regulatory requirements to secure private data, enterprises need to make DBMS security a top priority.**

This article will review best practices with real world solutions to protect the confidentiality and integrity of your database. Operational hurdles will be examined, such as multiple database deployments and heterogeneous environments. New solutions are presented that save money by displacing multiple point solutions, are easy to implement, scalable, and require no application changes. These sophisticated integrated multi-tier solutions for application and data assurance are combining the strengths of database encryption, auditing controls and business activity monitoring. Although most DBMS security requirements will be met by native DBMS features, many DBMSes do not offer a comprehensive set of advanced security options; notably, many DBMSes do not have security assessment, intrusion detection and prevention, data-in-motion encryption, and intelligent auditing capabilities. DBMSes are not intelligent when it comes to security: for example, if a user has privileges, the DBMS does not stop the user or even determine why he or she might be trying to query the schema repeatedly or trying to access all private data. What if the user is a hacker or a disgruntled employee?

### What are the common ways databases can be attacked?

Making your database secure is not an easy task. The challenges are coming from all angles, inside the organization as well as from the outside. As we look at database security, the starting point is

always to know which threats you are addressing, and to ensure the measures you are considering are appropriate for the threats. Organizations are exposed to different threats to the data – via applications, databases, file systems, and backups. The primary vulnerability of pure database security and database encryption is that it does not protect against application-level attacks. For databases that need the highest level of protection, such as Internet-based database applications, consider using specialized intrusion detection and prevention tools to track and eliminate suspicious activities.

### How should enterprises secure their databases to meet compliance requirements such as SOX, HIPAA, GLBA, PCI, SB1386, etc.?

While laws and regulations interpret "protecting privacy" in a number of ways, situations, any enterprise solution for protecting data - especially data at rest - must include the following components:

- Centralized security policy and reporting across different systems.
- Segregation of data administrative roles and security roles.
- Secure encryption technology to protect confidential data and careful management of access to the cryptography keys.

## **Should application security be integrated with database security? If so, why?**

We continue to see a trend in the direction of more advanced attacks against databases. Synchronized and automated threat responses between the application level and database level provide an effective protection against external and internal attacks.

Automated escalation of threat responses between the application level and database level directs the focus of countermeasures in time and between different IT system components, and also optimizes the balances among security level, performance aspects and ease of administration.

## **When it comes to database protection, are native DBMS security features good enough, or do enterprises need to supplement them with third-party security solutions?**

The major DBMS products on the market provide many - but not all - of the key functions within the three major DBMS security categories. Thus, growing concerns about security vulnerabilities and regulatory requirements have created a need for specialized DBMS security vendors, particularly in the areas of encryption, vulnerability assessment, intrusion detection and prevention, and monitoring.



**We continue to see a trend in the direction of more advanced attacks against databases.**

## **What are the key challenges and issues facing customers when dealing with database security?**

Although database security is clearly the best approach to securing sensitive information while maintaining accessibility for the organization, there are always concerns about the level of impact a solution may have on performance, scalability, availability and administration.

The challenge is to balance security and performance by narrowly focusing protection on the critical information that needs to be secured, and being aware how that information is used by various applications. Not all approaches to database security have comparable performance curves, but there are approaches that can minimize the impacts. A solution that can balance the security, performance and scalability is the key to any enterprise wide solution. Best practice is also to provide a centralized security policy and reporting across different systems.

## **Many enterprises want to protect private data from DBA's - is this possible? If so,**

## **how can they go about implementing such separation?**

The major DBMS products on the market does not provide a segregation of data administrative roles and security roles. Third party products can solve this requirement and provide the needed secure encryption technology to protect confidential data and careful management of access to the cryptography keys.

## **With more enterprises wanting to encrypt their databases, what are the benefits and challenges of data-at-rest database encryption?**

Database-layer encryption protects the data within the DBMS and also protects against a wide range of threats, including storage media theft, well-known storage attacks, database-layer attacks, and malicious DBAs. Deployment at the column level within a database table, coupled with access controls, will prevent theft of critical data.

Application-layer encryption requires a rewrite of existing applications, which is impractical due to limited IT resources, lack of access to source code, or a lack of familiarity with old code.

Rewriting applications is also very costly, risky and introduces an implementation time delay factor. Lastly, all applications that access the encrypted data must also be changed to support the encryption/decryption model. Storage-layer encryption alone can only protect against a narrow range of threats, namely media theft and storage system attacks.

### **What does a comprehensive database security solution consist of?**

A comprehensive best practice database security solution is based on segregation of duties and consists of encryption, assessment, alerting and auditing, and is tightly integrated with other technology stack components.

### **Majority of enterprises have heterogeneous DBMSes. What are the best practices to secure databases in such environments?**

Best practice is to provide a centralized security policy, key management, and reporting across different systems.

### **How can production data be securely used in a test system?**

Production data is in many cases need to ensure quality in system testing. Key data fields that can be used to identify an individual or corporation need to be cleansed to de-personalize the information. Cleansed data needs to be easily restored (for downstream systems and feeding systems), at least in the early stages of implementation. This therefore requires a two-way processing. The restoration process should be limited to situations for which there is no alternative to using production data (eg. interface testing with a third party or for firefighting situations). Authorization to use this process must be limited and controlled.

In some situations, business rules must be maintained during any cleansing operation (e.g. addresses for processing, dates of birth for age processing, names for sex distinction). Scrambling should be either consistent or variable with different cleansings. There should also be the ability to set parameters, or to select or identify fields to be scrambled, based on a combination of business rules. A solution must be based on secure encryption, robust key management, separation of duties, and auditing.

Ulf T. Mattsson is the CTO of Protegility. His extensive IT and security industry experience includes 20 years with IBM as a manager of software development and a consulting resource to IBM's Research and Development organization, in the areas of IT Architecture and IT Security.

## **HNS SECURITY SOFTWARE DATABASE**

**Get the largest selection of the best security software for Windows, Linux, Mac OS X and Windows Mobile platforms.**

**20 CATEGORIES  
2 MILLION DOWNLOADS SO FAR**

**[www.net-security.org](http://www.net-security.org)**



## Security for websites - breaking sessions to hack into a machine

By Colm Murphy

**Security on websites is based on session management. When a user connects to a secure website, they present credentials that testify to their identity, usually in the form of a username and password. Because the HTTP protocol is "stateless," the web server has no way of knowing that a particular user has already logged in as they browse from page to page. Session management allows the web-based system to create a 'session' so that the user will not have to re-authenticate every time they wish to perform a new action, or browse to a new page.**

In essence, session management ensures that the client currently connected is the same person who originally logged in. Unfortunately however, sessions are an obvious target for a malicious user, because they may be able to get access to a web server without needing to authenticate.

A typical scenario would involve a user logging on to an online service. Once the user is authenticated, the web server presents this user with a "session id." This session ID is stored by the browser and is presented wherever authentication is necessary. This avoids repeating the login/password process over and over. It all happens in the background and is transparent to the user, making the browsing experience much more pleasant in general. Imagine having to enter your username and password every time you browsed to a new page!

The session ID itself is simply a string of characters or numbers. The server remembers that the session ID (SID) was given to the user and allows access when it is presented. As a result, the Session ID is of great value and malicious users have, for years, searched for ways to compromise it and use it to circumvent authentication mechanisms.

Session Management is all about protecting this session ID, and in modern day interactive web applications this becomes critical.

So how to get your hands on a Session ID? There are a number of techniques attackers use to compromise a Session ID. The most obvious is to attack the server. The server often stores the session ID somewhere, and more worryingly, the server sometimes stores the session ID in a world-readable location. For example, PHP stores its session variables in the temporary /tmp directory on Unix. This location is world-readable, meaning that any user on that system can easily view the session IDs with basic utilities that are part of the Unix API. This is serious risk, particularly on shared hosts since many users will be active on the system. This issue has since been addressed but it is just one example.

Another method is to attack the client. Microsoft Internet Explorer, for example, has had numerous flaws that allowed web sites to read cookies (often used to store the Session ID) to which they did not belong. Ideally, only the site that created the cookie should have access to it.

Unfortunately, this is not always the case, and there are many instances of cookies being accessible to anyone. On top of this, a browser's cache is often accessible to anyone with access to that computer. It may be a hacker who has compromised the computer using some other attack, or a publicly accessible computer in an Internet café or kiosk. Either way, a cookie persistently stored in the browser cache is a tempting target.

Unencrypted transmissions are all too common and allow communication to be observed by an attacker. Unless the HTTPS protocol is used, a Session ID could be intercepted in transit and re-used. In fact, it is possible to mark cookies as 'secure' so they will only be transmitted over HTTPS.

This is something I have rarely seen developers do. Such a simple thing can go such a long way.

## UNENCRYPTED TRANSMISSIONS ARE ALL TOO COMMON AND ALLOW COMMUNICATION TO BE OBSERVED BY AN ATTACKER. UNLESS THE HTTPS PROTOCOL IS USED, A SESSION ID COULD BE INTERCEPTED IN TRANSIT AND RE-USED.

Another way to that is used to compromise a Session ID is to attempt to predict it. Prediction occurs when an attacker realizes that a pattern exists between session IDs. For example, some web based systems increment the session ID each time a user logs on. Knowing one session ID allows malicious users to identify the previous and next ones. Others use a brute force attack. This is a simple yet potentially effective method for determining a session identifier. A brute force attack occurs when a malicious user repeatedly tries numerous session identifiers until they happen upon a valid one. Although it is not complicated, it can be highly effective.

So what can you do to mitigate these attacks?

**1.** Always use strong encryption during transmission. Failure to encrypt the session identifier could render the online system insecure. In addition, for cookie based sessions, set the SSL-only attribute to "true" for a little added security. This will reduce the chance that an XSS attack could capture the session ID because the pages on the unencrypted section of the site will not be able to read the cookie.

**2.** Expire sessions quickly. Force the user to log out after a short period of inactivity. This way, an abandoned session will only be live for a short duration and thus will reduce the chance that an attacker could happen upon an active session. It is also wise to avoid persistent logins. Persistent logins typically leave a session identifier (or worse, login and password information) in a cookie that resides in the user's cache. This substantially increases the opportunity that an attacker has to get a valid SID.

**3.** Never make the Session ID viewable. This is a major problem with the GET method. GET variables are always present in the path string of the browser. Use the POST or cookie method instead or cycle the SID out with a new one frequently.

**4.** Always select a strong session identifier. Many attacks occur because the SID is too short or easily predicted. The identifier should be pseudo-random, retrieved from a seeded random number generator. For example, using a 32 character session identifier that contains the letters A-Z, a-z and 0-9 would have  $2.27e57$  possible IDs. This is equivalent to a 190 bit password. For example, using a 32 character session identifier that contains the letters A-Z, a-z and 0-9 is equivalent to a 190 bit password and is sufficiently strong for most web applications in use today.

**5.** Always double check critical operations. The server should re-authenticate anytime the user attempts to perform a critical operation. For example, if a user wishes to change their password, they should be forced to provide their original password first.

**6.** Always log out the user securely. Perform the logout operation such that the server state will inactivate the session as opposed to relying on the client to delete session information. Delete the session ID on logout. Some applications even force the browser to close down completely, thus ensuring stripping down the session and ensuring the deletion of the session ID.

**7.** Always prevent client-side page caching on pages that display sensitive information. Use HTTP to set the page expiration such that the page is not cached. Setting a page expiration that is in the past will cause the browser to discard the page contents from the cache.

**8.** Always require that users re-authenticate themselves after a specified period even if their session is still active. This will place an upper limit in the length of time that a successful session hijack can

last. Otherwise, an attacker could keep a connection opened for an extremely long amount of time after a successful attack occurs.

9. It is possible to perform other kinds of sanity checking. For example, use web client string analysis, SSL client certificate checks and some

level of IP address checking to provide basic assurance that clients are who they say they are.

All in all, web applications rely on good session management to stay secure. If you follow some of the steps outlined in this article and be aware of the risks, you are well on your way to leveraging the full benefits of web applications.

Colm Murphy is the Technical Director of Espion. In 2002, Espion co-founded the Irish Honeynet, with a view to researching hacking and attack behaviour in the Irish arena.



The advertisement features a large image of a hand in a black glove opening a blue door handle, symbolizing hacking or breaking into a website. To the right of the image, the text "IS YOUR WEBSITE HACKABLE?" is displayed in large white letters on a red background. Below this, the text "Check with Acunetix Web Vulnerability Scanner" is shown. The Acunetix logo, consisting of a red stylized 'a' icon followed by the word "acunetix" in red lowercase, is prominently displayed. The main headline "Web Vulnerability Scanner" is written in large red letters. A detailed description follows: "Audit your website security with Acunetix Web Vulnerability Scanner: Hackers are concentrating their efforts on attacking applications on your website. 75% of cyber attacks are launched on shopping carts, forms, login pages, dynamic content, etc. Firewalls, SSL and locked-down servers are futile against web application hacking. Check your website for vulnerabilities to SQL injection, cross site scripting and other web attacks before hackers do!" Below this, a section titled "Use Acunetix to:" lists ten bullet points detailing the scanner's capabilities. A quote from Gartner Group is included: "Securing your web application should be your #1 security concern. ‘75% of cyber attacks are launched on web applications.’" (GARTNER GROUP). At the bottom, the Acunetix logo is shown again, along with the text "Download your free trial today from <http://www.acunetix.com>". On the right side, a screenshot of the Acunetix software interface is displayed, showing a tree view of scanned files and a results pane listing various security findings.

# Events around the world



## **Infosecurity Europe 2006**

25 April-27 April 2006 – Olympia, London, UK  
[www.infosec.co.uk](http://www.infosec.co.uk)

## **LayerOne 200**

22 April-23 April 2006 – Pasadena Hilton, Los Angeles, California, USA  
<http://layerone.info/>

## **Infosecurity Europe 2006**

25 April-27 April 2006 – Olympia, London, UK  
<http://www.infosec.co.uk>

## **InfoSeCon 2006**

8 May-10 May 2006  
Hotel Croatia, Dubrovnik, Croatia  
<http://www.infosecon.org>

## **DallasCon Information & Wireless Security Conference 2006**

1 May-6 May 2006 – Dallas, Texas, USA  
<http://www.DallasCon.com>

## **iTrust 2006**

16 May-19 May 2006 – Piza, Italy  
<http://www.iit.cnr.it/iTrust2006/index.htm>

## **Eurocrypt 2006**

28 May-1 June 2006 – St. Petersburg, Russia  
<http://www.iacr.org/conferences/eurocrypt2006/>

## **OWASP AppSec Europe 2006**

29 May-31 May 2006 – K.U. Leuven, Belgium  
<http://www.owasp.org>

## **The Third Conference on Email and Anti-Spam (CEAS 2006)**

27 July-28 July 2006 – Mountain View, California , USA  
<http://www.ceas.cc>



## The size of security: the evolution and history of OSSTMM operational security metrics

By Pete Herzog

**There are two thriving schools of management when it comes to measuring security: the Thinkers and the Feelers. The Thinkers show how easy it can be with pencil and checklist in hand and a critical eye for best practices. The Feelers simply claim security is too complex and too unwieldy to put a number on it and continue to use values such as hot, cold, high, low, critical, and red as a measure of their “informed” opinions (aka gut feeling).**

Although on opposite ends of the spectrum, both schools instigate and perpetuate the myth of security metrics. The Thinkers think that anyone who can tally anything can produce a metric, which is true. The Feelers feel that the complications of unknowns in a threat matrix multiplied against a vast quantity of unknown vulnerabilities, of which some may be black boxes inside of black boxes, requires deeper insight to quantify security as an experience. (And there might be a reference to Tao or Buddha in there somewhere as well.) However, the Feelers are also correct. Measuring security requires the consideration of numerous variables and is greatly hinged on which way one is looking at it.

We are not born with a good sense of perspective. We learn that this big house we live in is not so big as we get to visit other, bigger houses. We learn that our big father or big mother is maybe not so big as we grow. But we also learn that we can overcome this perspective in the geometrical sense. We learn that one meter to me is one meter to you. We are astonished to learn that with such a metric, we weigh much less on the moon than we do on the Earth (although at that young age we never do account for the big helmet and

moon boots). So we later learn that our metric is relative. We learn perspective.

While learning, we begin to understand exact measurements. Some learn to feel out a pinch and a dollop. Some learn to measure ingredients by milligram mass and milliliter volume. And as such, we gravitate towards being either a metrics feeler or thinker. Great chefs exist in both courts. However, as we approach more creative and complicated constructs, we begin to borrow from both schools of thinking. Doing so is called the scientific method.

The scientific method requires a theory, a measured test of that theory, and measured results. Subscribing to only one school of thought can hurt this process. Therefore, to apply both schools of thought we use experiences to construct theories of how something should work, apply a methodology to make sure we try all possibilities within that theory, carefully measure the interactions and responses, and rely upon our experience again to understand the result. There are security metrics that apply the scientific method to this process. However, they don't apply well to operational security. What does not exist is an elegant solution

for operational security metrics that produced a consistent, predictable response from many complicated variables.

With the introduction of the Open Source Security Testing Methodology in January 2001 (the OSSTM manual is freely available at [www.isecom.org](http://www.isecom.org)), the process towards consistent and repeatable operational security metrics began, even if it had not even been a known milestone at the time.

The theory is that the achievement of a method for auditing to assure that the tests for a security process (operations) can be consistent and repeatable is the first step to quantifying operational security. It is as if previously, all carpenters had self-created meter sticks and independent methods of measuring a piece of wood that relied upon perspective and experience. In such a case customers would need to understand what a #3 table referred to and whether it fit their needs. This occurs ubiquitously in the security industry today as security consultancies need to provide follow-up workshops to explain the report and why something is labeled as “critical” or the little thermometer pictures is in dark yellow.

Another case may be that the customer requests a big table, but may have a different notion of big from that of the carpenter. This is a situation where the resulting mistake is crystal clear in security test reports. Two tests from independent auditors may have one rate the same target as a 8 on the scale of 10 for security and the other will rate it as “Moderately Secure”. Furthermore, both testers will use different attack vectors, as they need to grab some of that impressive treasure to wave around at that follow-up workshop. This technique is best left for stage magicians, tarot card readers, horoscope makers and artists, but not security auditors. When the details of how something is done focus on the end result, the test becomes a measure of the tester rather than of the target.

Another issue is how security tests are defined by commercial services and often follow marketability rather than sensibility. It is still the norm today to find penetration tests and vulnerability assessments made from such a perspective and under such time limitations that all that can truly be measured is customer happiness.

The fastest path to customer satisfaction is the theatrics of smiles and shock, the same can be said again of audits which require a checklist of defined solutions rather than functionality. Many existing regulations and even legislation will require the determination of an existing solution such as anti virus, IDS, firewall, or a specific

commercial brand of best practice. If you have the named solution, you pass regardless of whether it's configured “correctly” or configured at all. We need security metrics to be pragmatic, applicable, and apply the scientific method to ensure reliable input from both schools. Which is why the introduction of the OSSTMM, which requires a defined set of parameters and a complete process for a thorough test, has made it possible for every auditor to have both a consistently engraved meter stick and a clear methodology for maximizing thoroughness in a test.

With a standardized way to test, the OSSTMM elegantly evolved a method for measurement. Beginning with version 2, the OSSTMM addressed security metrics in terms of risk with Risk Assessment Values (RAVs). This was the first attempt to combine both schools of thinking. However, by following both schools, the errors in the metric were unfortunately the combined errors of both schools. The very first error was to quantify risk, a hotly contested and opinionated subject. While we all may agree that there is some risk, assigning accurate rates to that risk is not possible due to its relative nature. It's like assigning a universal value to “Small”. The RAVs had really all the problems of bad security metrics, some of which you will know are in other attempts at security metrics as well:

**1. The metric is to quantify a qualified concept.** Such is the problem of quantifying where weights must be assigned. Why should we accept a certain weight? If we are given a weight of 5, why shouldn't it be 50? If we accept a scale of 10x, why should it not be 200x? If the answer for these questions cannot be based in fact, and empirical evidence through experience cannot be considered fact (“that's the way it always is”), then this is not a valid quantification. Historical use for quantification does work, but universal acceptance is difficult (the pound versus the stone versus the kilogram), and without a natural comparison it cannot be re-created from scratch. We must all be able to all re-calibrate our measurement tools with the same method.

**2. The metric is not relative.** As we must learn perspective, we all learn it differently. Imagine if we could only measure the size of tables, but not chairs. A security metric which measures only servers and not networks or personnel security awareness is not a valid metric.

**3. The metric doesn't scale.** For example, a metric which provides quantification for big things but not small things is not a valid metric. We find historical quantities need adjustments to move to extremes.

How many dollops of hydrogen are in the sun? At some point, a reference point needs to be made between historical metrics and modern ones. However, this still does not ensure accuracy. A pinch of salt for a person with big fingers is clearly different from a pinch for a person with little fingers.

**4. The metric does not account for false trust.** If the measurement or the metric includes arbitrary weights and quantifications or has not/cannot be independently validated, then it is not a valid metric.

**4.1. Arbitrary weights** often serve as a placeholder value of qualified intensity; they also require trust in the weight to function correctly. Oftentimes, it is an authority that determines this weight. While this may function well for comparing two similar tests, it still does not stand independently or against a test which is not similar. One must have false trust in weights for them to work.

**4.2. Arbitrary quantifications** are most often found in automated or semi-automated tools with a large circulation, which require the tool itself to make the same metric repeatedly. It is most awful when it only serves the commercial interest of the tool creator because the tool is closed, its methods are opaque, and/or the quantification process is unknown. Even if the quantification is simple to figure out or put into other tools, there is no basis for the quantification other than someone put it there. Some good examples of this are vulnerability scanning tools which provide high, medium, and low threat values for vulnerabilities. Even if these classifications come from a common source such as the CVE, the CVE classifications also contain bias at the very least due to the nature of a vulnerability to behave differently according to the test vector and the host environment.

**4.3. Bias** is a part of being human. This means it is in our tools, theories, analysis, and recommendations. However, it does not need to be in the auditing process. For example, art is often considered subjective and creativity a part of art. Although many confuse creativity with art, it is also a significant portion of the scientific method. An auditor uses creativity to extend the parameters of an audit to new environments and new technologies, investigate the realm of new threats, and to improve analysis through the discovery of new, direct and indirect response types. Creativity is not a bias when used as an extension of an investigative methodology. However, when creativity is used as the investigative technique, then it is a bias. Many times we refer to a auditor's "gut instinct" or a hacker's intuition in finding holes. An

auditor's experience is valued commercially over his/her technique. These are biases based on creativity, and most often subtract from the audit process rather than improve it. The reason for this is that as humans, we let experience dictate our efficiency. As our experience grows, we take short-cuts in our audits and form conclusions before all the results are in. The result of an incomplete test set is an incomplete conclusion, often sold with a set of inappropriate recommendations.

**4.4. Conflicts of interest** are biases where ulterior motives cause improper test results. This can be as simple as choosing the wrong tool for a type of test because that is the tool the auditor knows how to use. It's like the old joke of the man looking for his car keys under the street lamp instead of next to the car where he dropped it because that's where the light is. Nowhere is bias more evident than in metrics which rely on the interview process in whole or in part. The interviewee will be biased for many reasons even if on a subconscious level. Furthermore, if the audit requires the interview questions to tally a metric, there is no guarantee that the interviewee will be able to answer the operational status of security measures beyond the already biased marketing material from the security solution provider.

Shortly after the release of OSSTMM 2.0, research into improving the RAVs meant solving those issues that plagued all security metrics. Approximately 2 years later, the first of the revised RAVs went into beta testing for OSSTMM 3.0. To solve the aforementioned problems, both the methodology and the concept of the metrics had to change. Changing the methodology to assure proper calculations turned out to be the easy part. Defining the rules for operational security quantification required looking at security in a new way. Analysis of security tests provided insight to which calculations would be factual and which could not be quantified. This simplified the concept greatly because it meant that we no longer had to find some obscure unifying algorithm; we only had to interpret and calculate the natural balance between secure and insecure to create a hash. This hash consisted of four calculations: operational security, loss controls, security limitations, and actual security.

All four calculations had to be based entirely on the scope in order for the scaling to work. This meant that we had our first problem. If we cheat on the scale then we can improve our security metric. This is an issue in many industries, but we found the solution from the accounting industry to be close to the best.

In accounting, strict rules and guidelines have been created by regulatory boards to prevent such tricks as reporting earnings but not losses, or reporting inventory sold but not returns. For the RAV we found that a clear audit checklist must be completed and submitted with each official metric tally to prevent exactly this problem. The audit checklist, known now as the OSSTMM Audit Report (OAR), minimizes cheating by requiring the auditor to sign-off on the basis of a security test:

**1. Scope.** What was tested? This is the enumeration of gateways and gatekeepers to physical and information assets, including the gateway/gatekeeper itself as an asset (although they are often represented financially as a cost). The scope can be one of or a range of computers, personnel, frequencies and power levels, phone numbers, applications, processes, or GPS coordinates. All security channels can be quantified in this manner.

**2. Index.** How were the gateways in the scope counted or classified? This is important to assure elasticity of scale. While the final hashes which we

calculate for Actual Security will basically allow us to compare apples to oranges, we cannot mix such items for calculating the hash itself.

**3. Vector.** What was the perspective of the test? Was the test performed from inside to outside the target zone, within the target zone, outside to inside the target zone, or any other unique perspective? The more vectors tested for the same target, the more accurate the Actual Security calculation will be.

**4. Channel.** The OSSTMM divides tests into five logical channels which allow interaction with physical property or information. The five channels are Physical, Data Networks, Telecommunications Networks, Personnel, and Wireless Communication Networks. Modern technology may cross multiple channels, such as tests via mobile phones or VOIP. The hash can still be calculated even across channels as long as the scope and index remains the same. However, for clarity, completing a new report is recommended for each different channel.

**The OSSTMM divides tests into five logical channels which allow interaction with physical property or information. The five channels are Physical, Data Networks, Telecommunications Networks, Personnel, and Wireless Communication Networks.**

5. The OSSTMM defines six test types which will clarify the depth of the test performed:

5.1. **blind/black box** - the auditor knows nothing about the target but the target is fully aware of what, how, and when the auditor will be testing.

5.2. **double-blind/black box** - the auditor knows nothing about the target and the target knows nothing of what, how, or when the auditor will be testing.

5.3. **gray box** - the auditor is aware of the operational security measures of the target and the target is fully aware of what and when the auditor will be testing.

5.4. **double-gray box** - the auditor is aware of the operational security measures of the target and the target is aware of what and when the auditor will be testing.

5.5. **tandem/white box** - the auditor has full knowledge of the target, its processes, and operational security and the target is fully aware of what, how, and when the auditor will be testing.

5.6. **reversal** - the auditor has full knowledge of the target, its processes, and operational security but the target knows nothing of what, how, or when the auditor will be testing.

Another fine point is that the OAR checklist requires the auditor to report what tests were only completed partially or not at all and why. This al-

lows the auditor, the client, and regulatory boards to have a clear overview as to what has not been accomplished meanwhile providing a certain amount of accountability in the proper direction. One of the other major problems in the security auditing industry is knowing whether or not the auditor could do his/her job correctly and if not, why not? If the client agrees with the terms in the Statement of Work (SoW) but the auditor does not deliver, this is clear in the OAR. But what if the client prevents the auditor from meeting the requirements of the SoW?

Previously, this could only be hinted at with the sometimes extremely large audit reports delivered by the auditor as evidence. With the OAR, this is handled efficiently with reasons and problems for a complete and thorough audit clearly presented. Problems might be insufficient time, insufficient access to the target due to type of test, safeguards, improper authority, or danger to operations. However, once the client accepts this audit report and signs-off on it, the liability is transferred from the auditor. During the Twilight, the time between when the auditor provides the OAR and the client accepts the OAR, there are 72 hours before liability is automatically transferred as stated in the OAR, and therefore should also be stated in the SoW

to be fully legal in many regions. Furthermore, it is possible to have ISECOM as an independent third party to review and certify an OAR for meeting legislative or regulatory compliance needs.

With the development of the OAR, it was possible to solve many of the problems with creating reliable security metrics. Now we needed to move forward with calculations. The next road block was the scope. While we knew the OAR would allow for the client to assume liability for the target scope selected for an audit as well as the channel and vectors, how should the scope be calculated? This is a problem that transcends all channels from data networking to the physical world. For example, a client has a /24 network block, but only a /28 is in use; does the entire block need to be audited? Again, with the client accepting liability for the audit scope, the auditor does what the client wants. However, often the client wants expert advice. For the RAV metrics to properly reflect operational security, it is recommended that all gateways to information or physical property be audited. In this case, we must determine if the entire block is assigned a route to the client, hence making the client liable for where that route goes. If so, then the entire block must be audited. This is

best understood in the physical realm. A client has a commercial building. If only half the building is rented to customers, will the vacant areas need to be protected as well? Or is it likely that anyone who wishes to visit the third floor does not need to pass through a security checkpoint because it is an empty space? Therefore, would a security patrol be able to ignore the third floor because they know it to be vacant, or does it get patrolled especially because it should be vacant?

However, we had all this talk of scope, and then it became clear that if we made any calculations based on the target scope, then any percentages of protection deduced could be easily altered by flexing the number of items in the scope. Oops! So if the scope of 100 items is 50% secure, can we make it 100% secure by reducing the scope by 50? And yes, in initial case studies, this happened. In the larger part of the corporate world, the need to satisfy regulatory groups far exceeds the quest for truth in security. To resolve this, we turned the target scope into what is essentially a target border; for example, the tester may not exceed range X from vector Y. This freed us to use that which is actually visible, which we can test in the scope to base the metrics on.

## A client has a commercial building. If only half the building is rented to customers, will the vacant areas need to be protected as well?

For calculating the RAVs, the first calculation we make from the audit results is that of Operational Security (OPSEC). OPSEC is the prevention of interactivity, opportunity, and blind trust within the target scope. If the scope is a grocery store, the walls are the protection from street-based attacks. If the scope is a network, the denial of routes to hosts are the protection from internet-based attacks.

We determine OPSEC to be the combination of Visibility, Access, and Trust within the scope. Visibility is the number of gateways in the scope that can be determined to exist by direct interaction, indirect information, or passive emanations. This is what we call “opportunity.” Trust is any non-authenticated interaction between any of the gateways within the scope and is really what we know as interdependence. This is similar to what happens in large office buildings where people do not “authenticate” the unknown faces of those who walk by their desks. Access is the number of points and primary types of interaction within each gateway and is also known commonly as “interac-

tions.” The calculation of these three categories provides the quantity of exposure in the scope.

The reduction of the OPSEC total will always improve protection of the scope from that vector and channel, as it means literally to have less exposed, less interactive, and less trust. Calculating OPSEC alone is useful, for example, for procurement.

The new product can be calculated for its OPSEC, and this number can be directly imposed on the existing OPSEC total for the current network to understand the change in operational protection this new product will have on its environment before it is even purchased, let alone installed in the network. In one case study, the RAVs were applied in this manner to evaluate SSL VPNs. Four of the SSL VPNs were audited in a lab before a purchase decision was made. This OPSEC delta was then applied for each VPN to the existing network's OPSEC total to determine which would leave the smallest exposure footprint within the current architecture for the appropriate vector.

For the second step in the process we calculate Loss Controls (LC). Where OPSEC is the wall, LC is the screen door. Wherever exposures occur in a process, the LC provide protection to those exposures. The 10 categories of LC are **authentication, non-repudiation, confidentiality, privacy, indemnification, integrity, safety, usability, continuity, and alarm** which inflect the “who, what, when, where, why, and how” of accessing or utilizing assets.

Authentication is protection from anyone not having both authorization and credentials for access to the gateway (identification is required for credentials). Non-repudiation protects the process from a source denying its role in any interaction regardless whether or not access was obtained. Confidentiality is the protection of the exchange or display of assets from unintended third parties.

Privacy is protection of the method in which parties display or exchange information or physical property from unintended third parties. Indemnification is the explicit protection of information and physical property, including gateways and gatekeepers as assets, enforced by public law or privately by insurance required to recoup the real and current value of the loss. Integrity is the protection of information and physical property from undisclosed changes. Safety is the function where the security mechanisms in OPSEC continue to prevent interactions even in the event of failure. Usability is where loss controls originate from and are controlled by the target. Continuity is the function where the process continues interactions even in the event of failure. Alarm is the timely notification of interactions or accesses and failure of LC.



Security limitations measure the current state of security in regard to known flaws.

The equation for calculating LC is to define what percentage of open operations is covered by LC. This allows us to go to the third step, where we can use the percentages of that which is unprotected to assign a value to limitations in security. Rather than using an arbitrary scale to give a value to a vulnerability, we base the number on the protection levels already determined. This allows for a measure of severity that is based on actual environmental conditions rather than a global number. This is because a metric needs to take perspective into account.

Security limitations measure the current state of security in regard to known flaws. All security limitations are calculated based on simple rules in operational security and loss controls. Furthermore, while we have labeled these classifications as such, the actual name does not matter. Should one choose to name each after levels, colors, or even farm animals, as long as the value associated with each classification is maintained, it will not affect the metrics at all. However, for the sake of clarity, we do need to label them. Therefore, we apply the classifications of vulnerability, weakness, concern, exposure and anomaly.

A vulnerability is defined as a protection flaw that allows for access or trust in the OPSEC sense. A weakness is a flaw which diminishes or negates the effects of loss controls. A concern is a flaw in

the sense of a mistake where a visibility, access, or trust is provided but without operational value for that vector. An exposure is a flaw that provides or extends visibility. Finally, an anomaly is any unidentifiable or unknown element that is a response to the tester's stimulus, consistently or not, and has no known impact on security. This refers often to data gathered which tends to make no sense or serve any purpose as far as the tester can tell, and is reported solely for the reason that it is a response that can be triggered and may be a sign of deeper problems inaccessible by the tester.

At this point, it's easy to think this is too complex. Current articles and interviews with members of the security industry all suggest that metrics must be simple to be used. However, simplicity is often the enemy of utility. A guitar with one string which anyone can learn to play quick and easy! A flute with one hole is a whistle, and we know how enjoyable the soothing sounds of a whistle can be. Realistically, the argument that a simple metric solution is better fails to show the complexities of security, and in turn the proper areas of address and redress to make necessary improvements along with operations.

“Simpler” does not bring satisfaction and therefore will not propagate use. “Simpler” is the enemy of security metrics.

The solution is to have a tool where the auditor can put in the numbers and have a realistic and factual metric that truly reflects operational security. Such a tool need only be made once and then can be re-used multiple times. To make an effective hunting rifle is a complex process that requires a large amount of smithing knowledge learned and studied. However, there is no argument that it is so simple to fire one that they need to be locked away from children.

Complexity is not the enemy, especially when there are as many variables and outcomes as there are in an operational security audit.

Finally, after working through all the complications, the combined value of all three calculations will provide the result known as "Actual Security." Actual security is the hash of the examined operation with its exposures, loss controls which may or may not properly address those exposures and may have security limitations themselves, and any other security limitations within the operational security design. The actual security is represented as a percentage where 100% is the perfect balance of operations and loss controls without limitations.

But it's complicated. How do we explain all these numbers to a client? One argument on a security mailing list claimed that the client has a hard enough time grasping the need for a security test and now to explain all these numbers would be impossible. Which is why we don't need to.

The OSSTMM makes the entire metrics solution open and readable. The client can read up about the metric, understand it, criticize it, and even download a spreadsheet version of the calculator to play with scenarios. However, some clients don't want that. They want to know the state of their security. Notice I did not say the color? By telling a client security is in the "red" or "critical" area, nothing is addressing "how much." How much red is too red? When is less red not red any more? How critical is it? Is it reasonable to expect a client to differentiate between highly critical, critical, and somewhat critical?

The RAVs allow for measurements over time, between industries, between channels, and even in various stages of procurement. The RAVs answer "how much" by providing three separate calcula-

tions for clarity and the actual security percentage. The actual security percentage can be used as both a security uptime indicator or to gauge how current operational security can handle business growth or expansion. The client should even have electronic versions of the RAV spreadsheet calculations to manipulate and discover which areas show the greatest improvements.

The client can ask herself, if we add more systems with more accesses, how much does my security change? If we purchase anti-virus software for all these systems, what loss controls would that provide and how much would that improve actual security? Could a different purchase be made that provides the same loss controls with fewer limitations for a better price? Finally, it is possible to put money values directly into this. If we are at 97% while spending \$500 per month, how much more might we need to spend to be at 99%? While seeming complicated at first, the RAVs provide so much utility towards knowing "how much" that the client will care about knowing what those four numbers mean.

From the two thriving schools of management when it comes to measuring security, both sides want a metric that can answer "How Much?". Both sides want a metric that does not require self justification or active defense, and certainly not one that can be over-turned by a person of authority because it doesn't feel right.

It is clear that both sides understand that better metrics require some complicated calculations. We can all picture the Thinkers with their reams of checklists and the Feelers with all their pretty threat graphs, both trying to tame operational security.

The RAVs are in the review phase and are a cornerstone of OSSTMM 3.0. The goal is a solution as elegant as algebra and as powerful as calculus. Feedback is always welcome.

ISECOM - [www.isecom.org](http://www.isecom.org)

OSSTMM - [www.osstmm.org](http://www.osstmm.org)

RAVs are covered appropriately in both the Security Tester and Security Analyst certifications: [www.opsa.org](http://www.opsa.org) and [www.opst.org](http://www.opst.org)

Pete Herzog is the Managing Director of ISECOM, an open, collaborative, security research community with non-profit status in the USA and Spain. ISECOM's aggressive mission is to make security make sense. ISECOM remains true as a vendor-neutral and non-partisan organization.

# 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](http://www.gfi.com/insec)**





## Interview with Kenny Paterson, Professor of Information Security at Royal Holloway, University of London

By Mirko Zorz



The Information Security Group at Royal Holloway ([www.isg.rhul.ac.uk](http://www.isg.rhul.ac.uk)) is one of the world's largest academic research groups in information security, with about 15 permanent academic staff, 50 PhD students and a thriving masters programme. They carry out research in many areas of the subject, including network security. That is one of Kenny Paterson's areas of specialism, and he teaches their masters course on the topic, and carries out research in the area.

### Your research lead you to the discovery of a high-profile vulnerability. Give us some details.

In late 2004, Arnold Yau (a PhD student in the group) and I began an investigation into IPsec security, in particular the security of the "encryption only" configuration of IPsec. The relevant standards are pretty clear that this configuration should be avoided, but they also mandate it be supported, mostly for reasons of backwards compatibility.

We also found quite a bit of anecdotal evidence, mostly in the form of on-line tutorials, that people might be using it in practice as well. So we decided to do an analysis of the Linux kernel implementation of IPsec, to see how it handled the encryption-only configuration and what, if any, weaknesses it might have. Arnold mostly worked on analyzing the source code, and I worked more on the cryptanalysis side, seeing how features of the code might be exploited in attacks.

By April 2005, about 6 months after starting, we had a fully-implemented attack client which showed the encryption only mode of IPsec to be very weak indeed against certain kinds of active attack. In fact, we were able to break the IPsec encryption in a matter of seconds, even when 128 bit AES keys were in use!

### In your opinion, what is the appropriate approach to take when announcing a vulnerability? What important lessons have you learned during your vulnerability disclosure process?

We worked through NISCC, a UK government agency, and they were able to put us in touch, through their channels, with a large number of vendors and consumers of IPsec. We also discussed things with people in the IETF, to make sure our understanding of the standards was correct. This approach gave all parties some time to assess the impact of our work for their products and deployments ahead of the official vulnerability announcement from NISCC and the release of our research paper describing the work.

We found the vendors to be largely responsive and cooperative, and I think they appreciated the opportunity to work things through in advance. For some vendors, there was no problem: their products didn't allow the encryption only setting to be selected; others had more work to do.

At the same time as this, we were getting useful feedback on the real-world implications of our research. That ultimately helped to make our research paper a better informed piece of work. This benefit was a bit unexpected for us: so one valuable lesson was not to underestimate the value of working with the community of implementors and

users before going public with your research. The proof that this worked in our favour is that our paper has now been accepted for presentation at Eurocrypt 2006, a major international conference in cryptography (to be held in St. Petersburg in May).

**In general, what is your take on the full disclosure of vulnerabilities? Should the vendors have the final responsibility?**

This is a hard one for me, as I don't have direct experience of working on the vendor side. However, software should be a product like any other, and I think the seller of any product ultimately has the responsibility to make sure its fit for purpose. Most software companies understand that perfectly nowadays and big strides have been made in recent years.

**When commenting your research you said: "The open source nature of Linux made the attacks easier". Does that necessarily mean that closed source is better than open source when it comes to security?**

No, not at all! The open source nature of the IPsec implementation we looked at certainly made it easier for us to experiment and to do work on paper before committing to coding. But the attacks we found were not your usual buffer overflows: they required us to build up a detailed understanding of how the Linux IPsec implementation interacted with the IP stack, for example, as well as doing some sophisticated bit manipulations on packets to get the effects we wanted. So our attacks really say very little about the "closed-source versus open-source" debate, which so often focuses only on the number of exploitable buffer overflows and other "standard" vulnerabilities that exist in software.

In fact, our work says more about the complexity of the IETF RFCs and how hard it is for a small team to write an implementation that gets absolutely everything right, from the low-level crypto to the implementation of IPsec policy processing.

**Are you satisfied with how Microsoft is tackling the problems in their software with monthly patch releases? Some argue that a premium service that releases the patches as they are ready should be in place for large customers. Should they do more?**

One problem they do have is that their patches get reverse engineered on a regular basis, and then tools to exploit the vulnerabilities found in this way appear quite soon after.

This wouldn't be a problem if everyone applied the patches immediately, but they don't. This is a bit like the concept of "herd immunity" in immunology: an immunization programme only becomes truly effective when above a certain percentage of people have had the jab - sometimes that percentage is as high as 90%. You can't force people to have immunizations. In the same way, Microsoft can't force people to apply the patches. Of course, it can be argued that applying patches on a monthly basis is a lot less pleasant than having an injection every once in a while!

**What advice would you give to security researchers?**

Persevere - it often takes time, luck and a lot of dead ends to find something interesting. Think about the wider effects of your research, and consider how you can resolve the apparently conflicting aims of getting headlines and of acting responsibly: if you do things in the right way, there is no real conflict.



**www.net-security.org**  
**Get up-to-date security information now.**



## WINDOWS - [VisualRoute 2006](#)

<http://www.net-security.org/software.php?id=2>

VisualRoute delivers the functionality of key Internet "ping," "whois," and "traceroute" tools, in a high-speed visually integrated package. VisualRoute automatically analyzes Internet connectivity and performance problems, displaying the results in an easy to understand table and on a world map.

## LINUX - [Stunnel](#)

<http://www.net-security.org/software.php?id=271>

Stunnel is a program that allows you to encrypt arbitrary TCP connections inside SSL (Secure Sockets Layer). Stunnel can allow you to secure non-SSL aware daemons and protocols (like POP, IMAP, LDAP, etc) by having Stunnel provide the encryption, requiring no changes to the daemon's code.

## MAC OS X - [Little Snitch](#)

<http://www.net-security.org/software.php?id=626>

You start an application that tells you that a new version is available. You suddenly realize that with every start this application connects to the developer's server. Even statistics information about your computer may be sent this way. Little Snitch helps you avoid this situation.

## POCKET PC - [Airscanner Mobile Encrypter](#)

<http://www.net-security.org/software.php?id=547>

Airscanner Mobile Encrypter secures data residing on your PDA and lets you lock your device to keep others from using it. The software has user-selectable, popular encryption and decryption algorithms such as 40-bit RC2, 40-bit RC4 and 56-bit DES and also offers Microsoft's Enhanced CryptoAPI, which supports strong, 128-bit RC4 encryption/decryption algorithms.

If you want your software title included in the HNS Software Database e-mail us at [software@net-security.org](mailto:software@net-security.org)



## War-driving in Germany - CeBIT 2006

By Alexander Gostev and Roel Schouwenberg

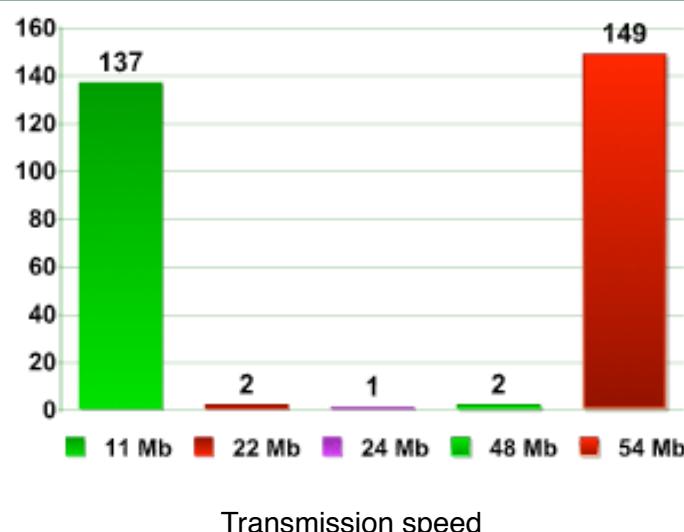
**Our latest research was undertaken on 9th and 10th March 2006, at CeBIT 2006 in Hannover. We collected data on approximately 300 access points. We did not attempt to connect to the networks we found, nor to intercept or decrypt traffic.**

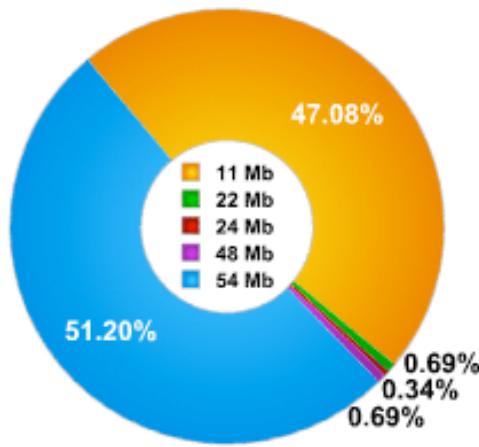
Firstly, trade fairs don't only attract users, software and hardware manufacturers. Hackers are also attracted by the opportunity to break into the networks of companies taking part in such fairs. Almost all firms which participate in such events set up their own local networks, which often connect to the company's main server. These local networks usually have low security settings, and are set up quickly; these factors increase the risk of hacker attacks. Naturally, one of the main ways of attacking such networks is via Wi-fi. Secondly, hackers use trade fairs not just as an opportunity to attack companies; they also target visitors. One notorious example took place at Infosecurity London last year, when a group of scammers installed

several fake access points, which provided a fake interface to connect to the public network. Unsuspecting users connected, and entered their passwords and other confidential data, and this information was sent directly to the hackers themselves.

### Transmission speed

During the research we detected an almost equal number of networks operating at 11 Mbps (over 47%) and 54 Mbps (over 51%). We also detected a small number of access points using less common transmission speeds (22, 24 and 48 Mbps).





Transmission speed, %

### Equipment manufacturers

We detected 18 different equipment manufacturers. 7 manufacturers were the most popular, with

their equipment being used in 28% of the access points at CeBIT2006. An additional 5.5% of access points used equipment from 11 other manufacturers.

Manufacturer	Percentage
Symbol	16.15%
Intel	5.50%
Linksys	1.72%
D-Link	1.37%
Netgear	1.37%
Cisco	1.03%
Proxim (Agere) Orinoco	1.03%
Other manufacturers	5.51%
Unknown, Fake, User Defined	66.32%

Equipment used as a percentage of the number of networks detected

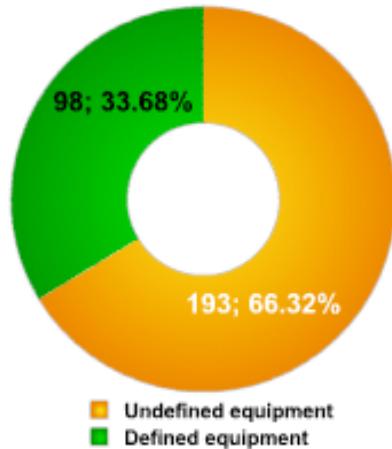
These figures differ significantly from the data collected in China and Moscow. In China, the most commonly used equipment was manufactured by Agere and Cisco (Linksys), while in Moscow, Cisco and D-Link were the most common manufacturers.

However, at CeBIT2006, the most commonly used equipment came from Intel (5.5%) and Symbol (16.5%). It's likely that this discrepancy is caused by the market share which companies hold in different countries.

When equipment for Wi-Fi networks is chosen, the choice is often influenced to some extent by the manufacturer's reputation on the domestic market.

Unfortunately, in a great number of cases, we couldn't determine the equipment manufacturer.

It's likely that the high percentage of cases where the manufacturer could not be determined is due to new equipment being used; such equipment is not recognized by current Wi-Fi scanners.



Defined / undefined equipment

## Encrypted traffic

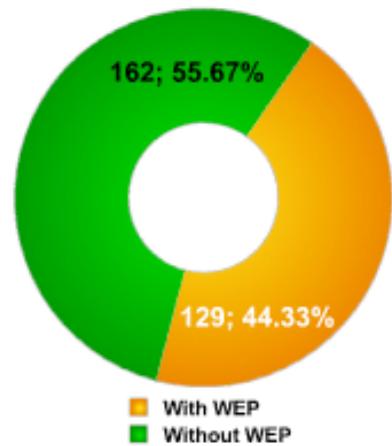
War-driving research in towns around the world shows that the number of Wi-Fi networks which do not use any type of data encryption is approximately 70%. Our research in China showed a significantly lower number, with only 59% of networks having no encryption.

Less than 56% of networks have no encryption protection; this is an improvement both on interna-

tional statistics, and on the statistics we collected in China.

However, even if we subtract public network access points (which we detected as being available at CeBIT2006), the number of unprotected access points is unacceptably high.

It should again be stressed that these points provide access to the local networks of companies participating in CeBIT - a prime target for hackers.



Encrypted / unencrypted networks

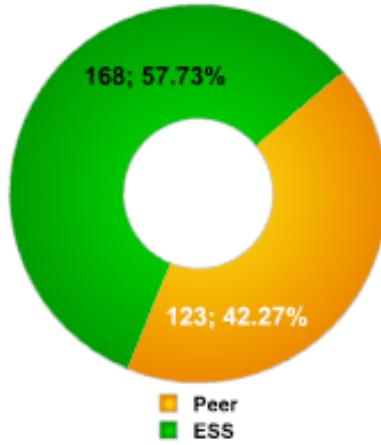
## Types of network access

The vast majority of wireless networks throughout the world (approximately 90%) are based on ESS/AP access points.

As has already been mentioned, networks at CeBIT differ significantly in terms of network infrastructure from standard networks, as the data be-

low shows. Among the connections we detected, more than 40% were IBSS/Peer connections.

This is undoubtedly because of the temporary nature of the networks, requiring a large number of computers to be connected to each other without network cables. Such access points can be regarded as part of the companies' internal networks.

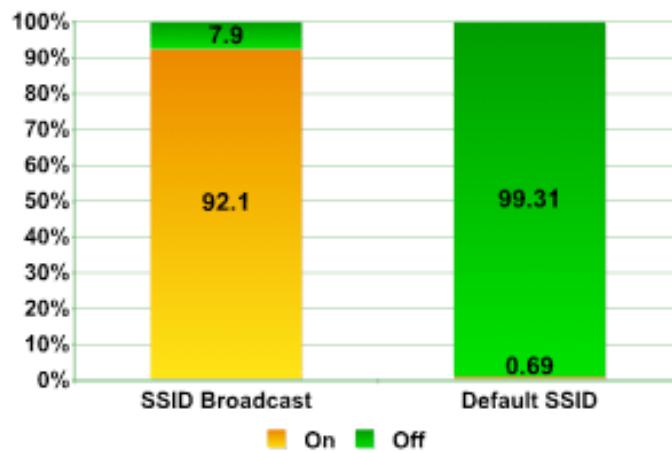


Types of network access

### Default configuration

One of the most effective ways of protecting networks against war-driving is disabling SSID (Service Set Identifier).

Our research showed that approximately 8% of wireless access points at CeBIT2006 had SSID disabled. Out of these, 89% used WEP encryption. There's no question that these wireless access points are the best protected against malicious attack.



Default configuration

Another interesting result was the default SSID. As a rule, this signifies that the administrator of the access point has not changed the router's name. It may also indicate that the administrative account uses the default password - both factors which

make networks potentially vulnerable to attack. We were encouraged that only 2 access points out of nearly 300 used the default SSID, showing that administrators were aware of security issues.

Alexander Gostev is the Senior Virus Analyst at Kaspersky Lab. His responsibilities include analyzing malicious software and detecting new malware.

Roel Schouwenberg is the Senior Research Engineer at Kaspersky Lab Benelux. His responsibilities include monitoring the malware situation in the region, preliminary analysis of malware and developing treatment for new viruses.

# 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](http://www.pocketpcsecurity.com)



This screenshot shows the initial interface of the Confidential Notes application. It features a large blue infinity symbol icon on the left and the text 'confidential notes' next to it. Below this is a section for entering a password, with two input fields labeled 'Enter password 1:' and 'Enter password 2:', each accompanied by a small clear button. There are also 'Forgot password?' and 'Enter' buttons. At the bottom is a virtual keyboard with standard QWERTY layout and additional symbols like '!', '#', and '<'.

This screenshot displays a list of notes within the Confidential Notes application. The notes are organized in a table with columns for the note title, date, and size. The notes listed are: 'ipaq software' (13:08, 4k), 'inet banking info' (13:06, 151k), 'shopping weekend' (13:04, 149b), 'target market' (13:04, 2k), 'city center plan' (13:03, 1k), 'dan's cellular' (13:02, 29b), 'early sketches' (13:01, 1024b), 'audio Q&A in NY' (13:01, 245k), 'wilderness sounds' (13:00, 225k), 'anna's NYSE column' (12:59, 892b), 'stock portfolio' (12:58, 1k), 'apple store london' (12:57, 3k), and 'VC capital thoughts' (12:57, 145k).

	Date	
ipaq software	13:08	4k
inet banking info	13:06	151k
shopping weekend	13:04	149b
target market	13:04	2k
city center plan	13:03	1k
dan's cellular	13:02	29b
early sketches	13:01	1024b
audio Q&A in NY	13:01	245k
wilderness sounds	13:00	225k
anna's NYSE column	12:59	892b
stock portfolio	12:58	1k
apple store london	12:57	3k
VC capital thoughts	12:57	145k

This screenshot shows a single note within the Confidential Notes application. The note is titled 'ARTICLE' in large, bold, black capital letters. The content of the note is a detailed article about the success of a conference and the role of the British Government agency in supporting overseas enterprises. The text is written in a clear, sans-serif font.

ARTICLE

Besides the overview on the success of the past year's event and a very positive forecast for this April's conference, journalists were presented with a rather new concept in the field of IT events - assistance for overseas visitors. I should note that the term "overseas" in this case is obviously connected to visitors outside the United Kingdom. As the Infosecurity conference is UK's top information security conference, UK Trade & Investment, the British Government agency that supports overseas enterprises

**Whether your site is the web presence for a large multinational, a gallery showing your product range and inviting potential customers to come into the shop, or a personal site exhibiting your holiday photos, web security matters. After the hard work put in to make your site look good and respond to your users, the last thing you want is for a malicious hacker to come along and break it somehow.**

There are a number of problems in web security, and unfortunately not all of them have definite solutions, but here we'll look at some of the problems that should be considered every time you set out to write a PHP script. These are the problems which, with well-designed code, can be eliminated entirely. Before looking in detail at the solutions, though, let's take a moment to define the problems themselves.

### SQL Injection

In this attack, a user is able to execute SQL queries in your website's database. This attack is usually performed by entering text into a form field which causes a subsequent SQL query, generated from the PHP form processing code, to execute part of the content of the form field as though it were SQL. The effects of this attack range from the harmless (simply using `SELECT` to pull another data set) to the devastating (`DELETE`, for instance). In more subtle attacks, data could be changed, or new data added.

### Directory Traversal

This attack can occur anywhere user-supplied data (from a form field or uploaded filename, for example) is used in a filesystem operation. If a user specifies “`../../../../etc/passwd`” as form data, and your script appends that to a

directory name to obtain user-specific files, this string could lead to the inclusion of the password file contents, instead of the intended file. More severe cases involve file operations such as moving and deleting, which allow an attacker to make arbitrary changes to your filesystem structure.

### Authentication Issues

Authentication issues involve users gaining access to something they shouldn't, but to which other users should. An example would be a user who was able to steal (or construct) a cookie allowing them to login to your site under an Administrator session, and therefore be able to change anything they liked.

### Remote Scripts (XSS)

XSS, or Cross-Site Scripting (also sometimes referred to as CSS, but this can be confused with Cascading Style Sheets, something entirely different!) is the process of exploiting a security hole in one site to run arbitrary code on that site's server. The code is usually included into a running PHP script from a remote location. This is a serious attack which could allow any code the attacker chooses to be run on the vulnerable server, with all of the permissions of the user hosting the script, including database and filesystem access.

## Processing User Data – Form Input Verification & HTML Display

### Validating Input And Stripping Tags

When a user enters information into a form which is to be later processed on your site, they have the power to enter anything they want. Code which processes form input should be carefully written to ensure that the input is as requested; password fields have the required level of complexity, e-mail

fields have at least some characters, an @ sign, some more characters, a period, and two or more characters at the end; zip or postal codes are of the required format, and so on.

Each of these may be verified using regular expressions, which scan the input for certain patterns. An example for e-mail address verification is the PHP code shown below. This evaluates to true if an e-mail address was entered in the field named 'email'.

```
preg_match('/^.[@].{2,3}$/', $_POST['email']);
```

This code just constructs a regular expression based on the format described above for an e-mail address. Note that this will return true for anything with an @ sign and a dot followed by 2 or 3 characters. That is the general format for an e-mail address, but it doesn't mean that address necessarily exists; you'd have to send mail to it to be sure of that.

Interesting as this is, how does it relate to security? Well, consider a guestbook as an example. Here, users are invited to enter a message into a form, which then gets displayed on the HTML

page along with everyone else's messages. For now, we won't go into database security issues; the problems dealt with below can occur whether the data is stored in a database, a file, or some other construct.

If a user enters data which contains HTML, or even JavaScript, then when the data is included into your HTML for display later, their HTML or JavaScript will also get included. If your guestbook page displayed whatever was entered into the form field, and a user entered the following:

```
Hi, I <b>love</b> your site.
```

Then the effect is minimal, when displayed later, this would appear as:

Hi, I **love** your site.

Of course, when the user enters JavaScript, things can get a lot worse. For example, the data below,

when entered into a form which does not prevent JavaScript ending up in the final displayed page, will cause the page to redirect to a different website. Obviously, this only works if the client has JavaScript enabled in their browser, but the vast majority of users do.

```
Hi, I love your site. Its great!<script  
language="JavaScript">document.location="http://www.acunetix.com/";</script>
```

For a split second when this is displayed, the user will see:

Hi, I love your site. Its great!

The browser will then kick in and the page will be refreshed from www.acunetix.com. In this case, it would be a fairly harmless alternative page, although it does result in a denial of service attack; users can no longer get to your guestbook.

Consider a case where this was entered into an online order form. Your order dispatchers would

not be able to view the data because every time they tried, their browser would redirect to another site.

Worse still, if the redirection occurred on a critical page for a large business, or the redirection was to a site containing objectionable material, custom may be lost as a result of the attack.

Fortunately, PHP provides a way to prevent this style of attack. The functions `strip_tags()`, `nl2br()` and `htmlspecialchars()` are your friends, here.

`strip_tags()` removes any PHP or HTML tags from a string. This prevents the HTML display problems, the JavaScript execution (the `<script>` tag will no longer be present) and a variety of problems where there is a chance that PHP code could be executed.

`nl2br()` converts newline characters in the input to `<br />` HTML tags. This allows you to format multi-line input correctly, and is mentioned here only because it is important to run `strip_tags()` prior to running `nl2br()` on your data, otherwise the newly inserted `<br />` tags will be stripped out when `strip_tags()` is run!

Finally, `htmlspecialchars()` will entity-quote characters such as `<`, `>` and `&` remaining in the input after `strip_tags()` has run. This prevents

them being misinterpreted as HTML and makes sure they are displayed properly in any output.

Having presented those three functions, there are a few points to make about their usage. Clearly, `nl2br()` and `htmlspecialchars()` are suited for output formatting, called on data just before it is output, allowing the database or file-stored data to retain normal formatting such as newlines and characters such as `&`. These functions are designed mainly to ensure that output of data into an HTML page is presented neatly, even after running `strip_tags()` on any input.

`strip_tags()`, on the other hand, should be run immediately on input of data, before any other processing occurs. The code below is a function to clean user input of any PHP or HTML tags, and works for both GET and POST request methods.

```
function _INPUT($name)
{
    if ($_SERVER['REQUEST_METHOD'] = 'GET')
        return strip_tags($_GET[$name]);
    if ($_SERVER['REQUEST_METHOD'] = 'POST')
        return strip_tags($_POST[$name]);
}
```

This function could easily be expanded to include cookies in the search for a variable name. I called it `_INPUT` because it directly parallels the `$_` arrays which store user input. Note also that when using this function, it does not matter whether the page was requested with a GET or a POST method; the

code can use `_INPUT()` and expect the correct value regardless of request method.

To use this function, consider the following two lines of code, which both have the same effect, but the second strips the PHP and HTML tags first, thus increasing the security of the script.

```
$name = $_GET['name'];
$name = _INPUT('name');
```

If data is to be entered into a database, more processing is needed to prevent SQL injection, which will be discussed later.

### Executing Code Containing User Input

Another concern when dealing with user data is the possibility that it may be executed in PHP code or in the system shell. PHP provides the `eval()` function, which allows arbitrary PHP code within a string to be evaluated (run).

There are also the `system()`, `passthru()` and `exec()` functions, and the backtick operator, all of which allow a string to be run as a command in the operating system shell.

Where possible, avoid the use of all such functions, especially where user input is entered into the command or code. An example of a situation where this can lead to attack is the following command, which would display the results of the command on the web page.

```
echo 'Your usage log:<br />';
$username = $_GET['username'];
passthru("cat /logs/usage/$username");
```

`passthru()` runs a command and displays the output as output from the PHP script, which is included into the final page the user sees. Here, the intent is obvious: a user can pass their username in a GET request such as

`usage.php?username=andrew` and their usage log would be displayed in the browser window.

But what if the user passed the following URL?

```
usage.php?username=andrew;cat%20/etc/passwd
```

Here, the `username` value now contains a semicolon, which is a shell command terminator, and a new command afterwards. The `%20` is a URL-

Encoded space character, and is converted to a space automatically by PHP. Now, the command which gets run by `passthru()` is:

```
cat /logs/usage/andrew;cat /etc/passwd
```

Clearly this kind of command abuse cannot be allowed. An attacker could use this vulnerability to read, delete or modify any file the web server has access to.

Luckily, once again, PHP steps in to provide a solution, in the form of the `escapeshellarg()` function. `escapeshellarg()` escapes any characters

which could cause an argument or command to be terminated.

As an example, any single or double quotes in the string are replaced with `\'` or `\\"`, and semicolons are replaced with `\;`. These replacements, and any others performed by `escapeshellarg()`, ensure that code such as that presented below is safe to run.

```
$username = escapeshellarg($_GET['username']);
passthru("cat /logs/usage/$username");
```

Now, if the attacker attempts to read the password file using the request string above, the shell will attempt to access a file called `"/logs/usage/andrew;cat /etc/passwd"`, and will fail, since this file will almost certainly not exist.

At all costs, `eval()` called on code containing user input should be avoided; there is almost always a better way to achieve the desired effect. However, if it must be done, ensure that `strip_tags` has been called, and that any quoting and character escapes have been performed.

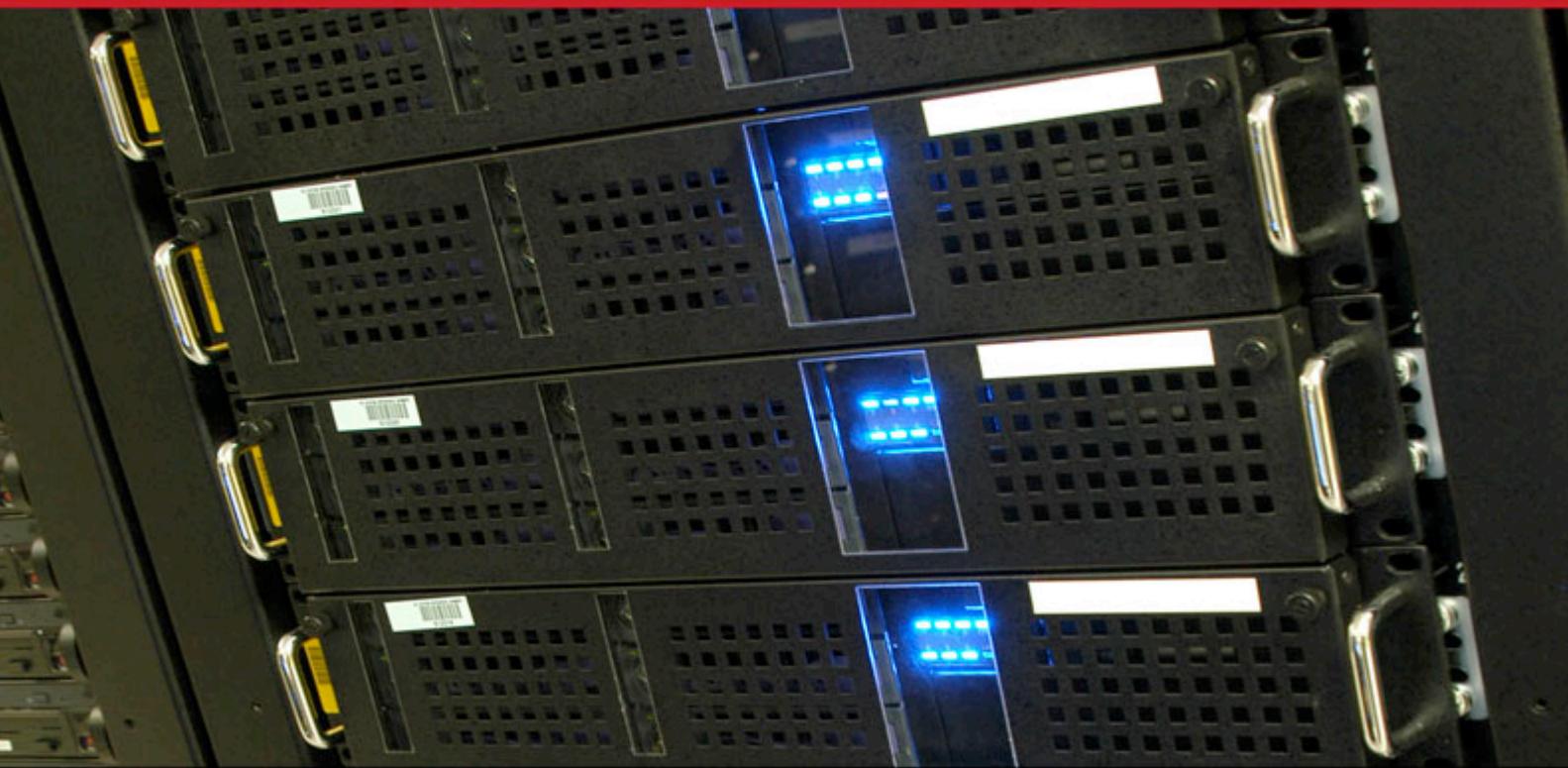
Combining the above techniques to provide tag stripping, special shell character escapes, entity quoting of HTML and regular expression-based input validation, it is possible to construct secure web scripts with relatively little work over and above constructing one without the security considerations.

In particular, using a function such as the `_IN-PUT()` presented above makes the secure version of input acquisition almost as painless as the insecure version PHP provides.

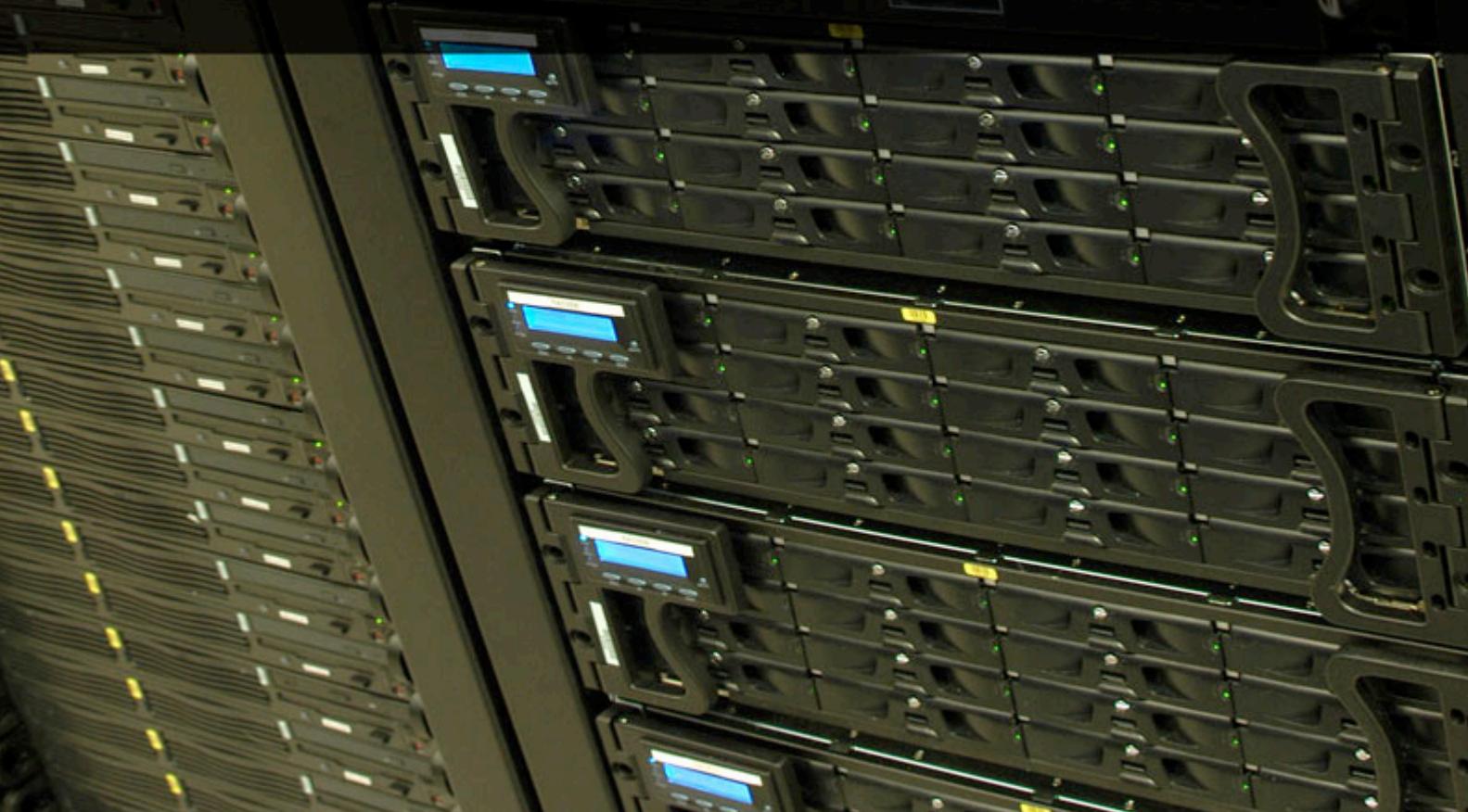
Andrew J Bennieston has been building secure PHP systems for several years, and contributes to leading computer security websites and forums. He takes an active role in researching the best practices in secure programming and applying those to working systems. Article commissioned by Acunetix ([www.acunetix.com](http://www.acunetix.com)), their flagship product Acunetix Web Vulnerability Scanner, scans a website for vulnerabilities to SQL injection and PHP security, amongst others.

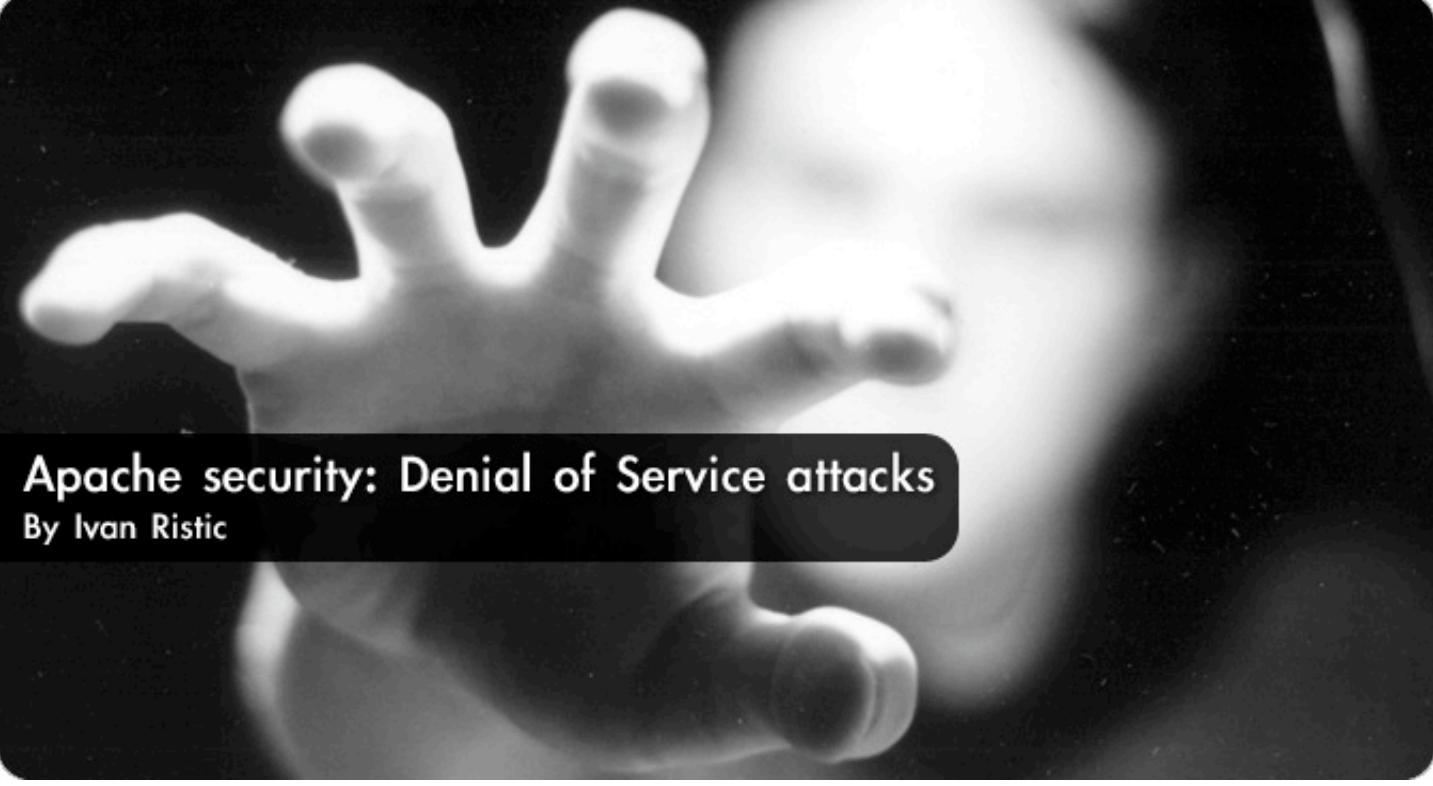
# TAOSECURITY

THE WAY OF DIGITAL SECURITY



**Understanding the network is the key to success in the digital realm.  
TaoSecurity works with customers to assess the threats to their  
organizations and improve digital situational awareness.**





## Apache security: Denial of Service attacks

By Ivan Ristic

**With other types of attacks being easy, almost trivial, to perform, hardly anyone bothers attacking Apache directly. Under some circumstances, Apache-level attacks can be easier to perform because they do not require as much bandwidth as other types of attacks. Some Apache-level attacks can be performed with as few as a dozen bytes. Less-skilled attackers will often choose this type of attack because it is so obvious.**

### Apache Vulnerabilities

Programming errors come in different shapes. Many have security implications. A programming error that can be exploited to abuse system resources should be classified as a vulnerability. For example, in 1998, a programming error was discovered in Apache: specially crafted small-sized requests caused Apache to allocate large amounts of memory. For more information, see: "YA Apache DoS Attack," discovered by Dag-Erling Smørgrav ([tinyurl.com/hdf56](http://tinyurl.com/hdf56))

More serious vulnerabilities, such as nonexploitable buffer overflows, can cause the server to crash when attacked. (Exploitable buffer overflows are not likely to be used as DoS attacks since they can and will be used instead to compromise the host.) When Apache is running in a prefork mode as it usually is, there are many instances of the server running in parallel. If a child crashes, the parent process will create a new child. The attacker will have to send a large number of requests constantly to disrupt the operation.

**TIP:** A crash will prevent the server from logging the offending request since logging takes place in

the last phase of request processing. The clue that something happened will be in the error log, as a message that a segmentation fault occurred. Not all segmentation faults are a sign of attack though. The server can crash under various circumstances (typically due to bugs), and some vendor-packaged servers crash quite often.

In a multithreaded (not prefork) mode of operation, there is only one server process. A crash while processing a request will cause the whole server to go down and make it unavailable. This will be easy to detect because you have server monitoring in place or you start getting angry calls from your customers.

Vulnerabilities are easy to resolve in most cases: you need to patch the server or upgrade to a version that fixes the problem. Things can be unpleasant if you are running a vendor-supplied version of Apache, and the vendor is slow in releasing the upgrade.

### Brute-Force Attacks

Any of the widely available web server load-testing tools can be used to attack a web server.

It would be a crude, visible, but effective attack nevertheless. One such tool, ab (short for Apache Benchmark), is distributed with Apache. To perform a simple attack against your own server, execute the following, replacing the URL with the URL for your server.

```
$ /usr/local/apache/bin/ab -n 1000 -c 100  
http://www.yourserver.com/
```

Choose the concurrency level (the -c switch) to be the same as or larger than the maximum number of Apache processes allowed (`MaxClients`). The slower the connection to the server, the more effect the attack will have. You will probably find it difficult to perform the attack from the local network. To defend against this type of attack, first identify the IP address the attacker is coming from and then deny it access to the server on the network firewall. You can do this manually, or you can set up an automated script. If you choose the latter approach, make sure your detection scripts will not make mistakes that would cause legitimate users to be denied service. There is no single method of detection that can be used to detect all attack types. Here are some possible detection approaches:

- Watch the `mod_status` output to detect too many identical requests.
- Examine the access log in regular time intervals and count the number of requests coming from each IP address. (This approach is usable only if you are running one web site or if all the traffic is recorded in the same file.)

I designed three tools that can be helpful with brute-force DoS attacks. All three are available for download from [www.apachefirewall.org](http://www.apachefirewall.org).

**blacklist** - Makes the job of maintaining a dynamic host-based firewall easy. It accepts an IP address and a time period on the command line, blocks requests from the IP address, and lifts the ban automatically when the period expires.

**apache-protect** - Designed to monitor `mod_status` output and detect too many identical requests coming from the same IP address.

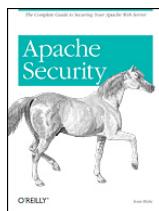
**blacklist-webclient** - A small, C-based program that allows non-root scripts to use the `blacklist` tool (e.g., if you want to use `blacklist` for attacks detected by `mod_security`).

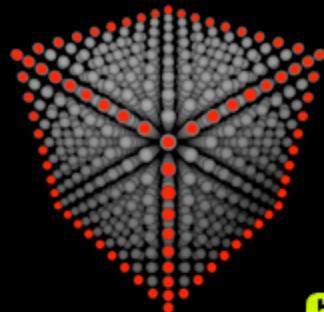
## Programming Model Attacks

The brute-force attacks we have discussed are easy to perform but may require a lot of bandwidth, and they are easy to spot. With some programming skills, the attack can be improved to leave no trace in the logs and to require little bandwidth. The trick is to open a connection to the server but not send a single byte. Opening the connection and waiting requires almost no resources by the attacker, but it permanently ties up one Apache process to wait patiently for a request. Apache will wait until the timeout expires, and then close the connection. As of Apache 1.3.31, request-line timeouts are logged to the access log (with status code 408). Request line timeout messages appear in the error log with the level `info`. Apache 2 does not log such messages to the error log, but efforts are underway to add the same functionality as is present in the 1.x branch.

Opening just one connection will not disrupt anything, but opening hundreds of connections at the same time will make all available Apache processes busy. When the maximal number of processes is reached, Apache will log the event into the error log ("server reached MaxClients setting, consider raising the MaxClients setting") and start holding new connections in a queue. This type of attack is similar to the SYN flood network attack we discussed earlier. If we continue to open new connections at a high rate, legitimate requests will hardly be served. If we start opening our connections at an even higher rate, the waiting queue itself will become full (up to 511 connections are queued by default; another value can be configured using the `ListenBackLog` directive) and will result in new connections being rejected.

Defending against this type of attack is difficult. The only solution is to monitor server performance closely (in real-time) and deny access from the attacker's IP address when attacked.





# HITBSecConf2006 - Malaysia

September 18th - 21st 2006

DEEP KNOWLEDGE SECURITY CONFERENCE

**6 Hands-On Technical Training Tracks**

**Over 24 world known network security experts & researchers**

**Asia's Biggest Network Security Event**

Venue: Westin Kuala Lumpur

18th - 19th September 2006

Hands-On Technical Training

20th - 21st September 2006

Dual Track Security Conference

20th - 21st September 2006

Capture The Flag

Technology Showcase & Exhibition

Papers & Presentations By:

Bruce Schneier (Keynote 1)

Mark Culphey with John Viega (Keynote 2)

Raoul Chiesa

Philippe Biondi

Van Hauser (THC)

The Grugq

Michael Davis

Thorsten Holz

Fabrice Marie

Shreeraj Shah and many more...

<http://conference.hackinthebox.org/hitbsecconf2006kl>

**LAVASOFT**

*protect your privacy*

*The leading antispyware developer  
now delivers the best personal firewall protection*



**LAVASOFT PERSONAL FIREWALL**

*Superior security shield against hackers, worms and Trojans*

[www.lavasoft.com](http://www.lavasoft.com)

Register by March 22nd & take  
advantage of our early bird rate!

# 3RD ANNUAL ID THEFT SYMPOSIUM CUSTOMER IDENTIFICATION & AUTHENTICATION MANAGEMENT IN FINANCIAL SERVICES

May 22 – 23, 2006 • Marriott Marquis, New York

## SECURITY SOLUTIONS FOR THE FINANCIAL COMMUNITY

### FEATURED SPEAKERS INCLUDE:

- Richard A. Parry, *SVP, Consumer Risk Management, JP MORGAN CHASE*
- Donna Stone, *Delaware, Chair, FINANCIAL SERVICES STANDING COMMITTEE OF THE NATIONAL CONFERENCE OF STATE LEGISLATURES*
- Brad Keller, *eCommerce Business Risk Manager, WACHOVIA*
- Brad Nightengale, *Vice-President - Emerging Product, VISA USA*
- Jennifer L. Bayuk, *Chief Information Security Officer, BEAR STEARNS AND CO., INC.*
- Nancy Callahan, *Vice President, AIG IDENTITY THEFT AND FRAUD DIVISION*
- Jeffrey Hunker, *Professor of Technology Policy, CARNEGIE MELLON UNIVERSITY*
- Joe Borg, *Director, ALABAMA STATE SECURITIES COMMISSION*
- Paul J. Trimbur, *Mail Theft, Violent Crimes & Narcotic Investigations, U.S. POSTAL INSPECTION SERVICE*
- Steve Harbeck, *Chairman, SECURITIES INVESTOR PROTECTION CORPORATION (SIPC)*
- Ronald Waldman, *Senior Attorney, FEDERAL TRADE COMMISSION (FTC)*
- Peter Cassidy, *Secretary General, ANTI-PHISHING WORKING GROUP*
- Russ Ryan, *Vice President, NATIONAL BIOMETRIC SECURITY PROJECT*
- Doug Johnson, *Senior Policy Analyst, AMERICAN BANKERS ASSOCIATION*



CONFERENCE CHAIRMAN AND SPECIAL CONTRIBUTOR:

Richard A. Parry  
*Senior Vice President, Consumer Risk Management*  
**JP MORGAN CHASE**