(IN)SECURE

OPEN. INFORMATIVE. TO THE POINT. Issue 8 - September 2006

WINDOWS MOBILE SECURITY SOFTWARE FAILS THE TEST

PAYMENT CARD INDUSTRY DEMYSTIFIED

SKYPE: HOW SAFE IS IT?

TABLE OF CONTENTS

Hello everyone, welcome to issue 8 of (IN)SECURE. We're happy to report that our subscriber list is growing strong. This, combined with the e-mails and quality article submissions, is a clear indication that the security community has embraced this concept and found it to be a valuable resource.

This issue is packed full with material for every knowledge level and will especially be of interest to those that want to know more about the inner workings of the Payment Card Industry since we got two articles related to the topic.

Mirko Zorz
Chief Editor

Visit the magazine website at www.insecuremag.com

(IN)SECURE Magazine contacts

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

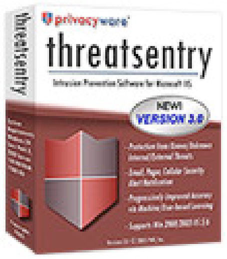
Marketing: Berislav Kucan, Director of Marketing - marketing@insecuremag.com

Distribution

(IN)SECURE Magazine can be freely distributed in the form of the original, non modified PDF document. Distribution of 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 or send a fax to 1-866-420-2598.

Corporate security news

Defend Windows web servers with ThreatSentry 3.0



ThreatSentry 3.0 is a Host Intrusion Prevention System (HIPS) specifically designed to address internal and external unauthorized system access and cyber-criminal threats on Web servers utilizing Microsoft Internet Information Services (IIS). Since its introduction, IIS has grown in popularity and ranks as one of the most widely used platforms for enabling simple to sophisticated Web sites and Web-based applications. While it is well-regarded for its ease of use and range of features, it is frequently targeted by hackers due to a variety of IIS-related vulnerabilities and the inherently open nature of many Web applications – many of which manage sensitive information such as credit card numbers, passwords, or other private information. ThreatSentry pricing starts at $399 per server. For more information visit hwww.privacyware.com

AirDefense Mobile 4.0 released

AirDefense announced the release of AirDefense Mobile 4.0, the newest version of the company's security and wireless network assessment tool. Mobile 4.0 includes a new analysis engine, which is built on the award-winning, patented technology used in the company's flagship product, AirDefense Enterprise. The analysis engine provides network administrators with more than 100 security and performance-based alarms, along with other new features such as alarm notification via email or Syslog messaging. AirDefense Mobile runs on any Windows 2000 or XP platform, and installs on any laptop with an Atheros-based 802.11 a/b/g wireless card, such as Netgear (WAG511) or Cisco (CB21AG). For more information visit www.airdefense.net

SECUDE releases Secure notebook 7.2

SECUDE secure notebook reliably protects notebooks, desktops and external mass storage devices from unauthorised access. Unlike other solutions it encrypts the entire hard disk rather than just individual files or folders, which means it protects temporary files, swap files and even the operating system itself.

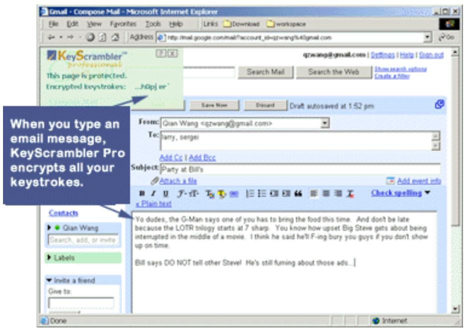
A new feature with version 7.2 is the encryption of hibernation files (the files that a notebook creates just before entering hibernation mode); eliminating the possibility of attack by this route and guaranteeing full protection in all circumstances.

This version also offers a Plug-In for BartPE; the Windows recovery system that boots and runs from CD. It supports the creation of an emergency recovery disk (ERD), which can be used to secure data for emergency cases, preventing loss; as well as getting the notebook running after a system crash. More information is available at www.secude.com

Anti-keylogger plugin for Microsoft Internet Explorer released

A browser plugin named KeyScrambler was recently released by Florida startup QFX Software. The Personal edition is free for download at the company's website and it protects all logins against keyloggers.

The new anti-keylogging tool is an invaluable addition to the IE users' security as it protects all login pages and it does so by encrypting the user's keystrokes at the kernel driver level, before keyloggers can record them. Download the trial from www.qfxsoftware.com



This page is protected.
Encrypted keystrokes: ...h0pj er`

Draft autosaved at 1:52 pm

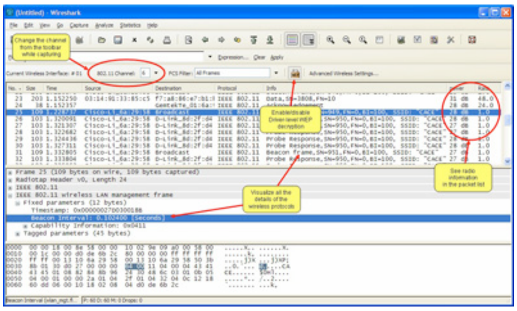
From: Qian Wang <qzwang@gmail.com>
To: larry, sergei
Subject: Party at Bill's

Yo dudes, the G-Man says one of you has to bring the food this time. And don't be late because the LOTR trilogy starts at 7 sharp. You know how upset Big Steve gets about being interrupted in the middle of a movie. I think he said he'll F-ing bury you guys if you don't show up on time.

Bill says DO NOT tell other Steve! He's still fuming about those ads...

When you type an email message, KeyScrambler Pro encrypts all your keystrokes.

AirPcap USB 2.0 WLAN packet capture device available


(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Expression... Clear Apply
Current Wireless Interface: # 01
802.11 Channel: 6
FCS Filter: All Frames
Advanced Wireless Settings...
No. Size Time Source Destination Protocol Info Power Rate
Change the channel from the toolbar while capturing
Enable/disable Driver level WEP decryption
See radio information in the packet list
Visualize all the details of the wireless protocols

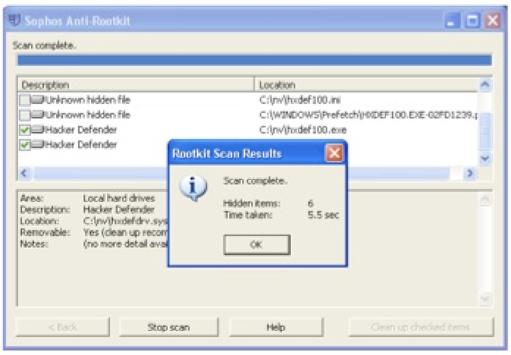
Frame 25 (109 bytes on wire, 109 bytes captured)
Radiotap Header v0, Length 24
IEEE 802.11
IEEE 802.11 wireless LAN management frame
Fixed parameters (12 bytes)
Timestamp: 0x000000027D0300188
Beacon Interval: 0.102400 [Seconds]
Capability Information: 0x0411
Tagged parameters (45 bytes)

CACE Technologies announced the release of AirPcap USB 2.0 WLAN packet capture device for Windows. The device enables troubleshooting tools like Wireshark and WinDump to provide information about the wireless protocols and radio signals.

The AirPcap adapter, together with the Wireshark Network Analyzer, gives you a detailed view on the 802.11 traffic, including control frames (ACK, RTS, CTS), management frames (Beacon, Probe requests and responses, Association/Disassociation, Authentication/Deauthentication) and data frames. The captured frames include the 802.11 Frame Check Sequence, and it's possible to capture frames with an invalid FCS to spot remote access points with a weak signal. For more information visit www.cacetech.com

Sophos offers free rootkit detection and removal tool

Sophos today announced the availability of a new free-of-charge, standalone tool offering comprehensive rootkit detection and removal capabilities. Sophos Anti-Rootkit complements Sophos Anti-Virus 6.0 and other vendors' anti-virus solutions by providing an additional layer of protection for the Windows NT/2000/XP/2003 operating systems.



Scan complete.

Description	Location
□ Unknown hidden file	C:\nv\hxdef100.ini
□ Unknown hidden file	C:\WINDOWS\Prefetch\HXDEF100.EXE-02FD1239.|
☑ Hacker Defender	C:\nv\hxdef100.exe
☑ Hacker Defender	

Area: Local hard drives
Description: Hacker Defender
Location: C:\nv\hxdefdrv.sys
Removable: Yes (clean up recom
Notes: (no more detail ava

Scan complete.

Hidden items: 6
Time taken: 5.5 sec

Unlike other tools available, Sophos Anti-Rootkit warns if removal of a particular rootkit will impact upon the efficiency or integrity of the infected PC's operating system. This feature lets network administrators make an informed decision on how they want to proceed. Download the software from www.sophos.com/products/free-tools

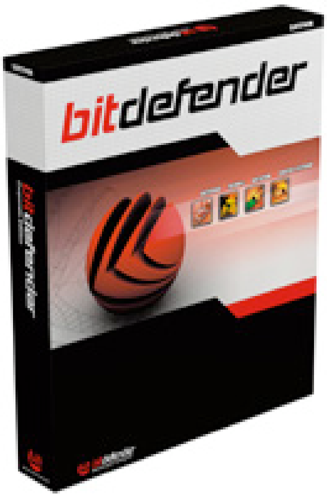
New Bue Coat applicances offer better performance

Blue Coat Systems announced it is releasing new appliance hardware models offering throughput performance increases of approximately two to three times higher than existing models. The new appliances run the same existing Blue Coat SGOS software for WAN optimization and Web security and control. A new add-in card for visibility, control and acceleration of SSL traffic now features a chip that is certified to Federal Information Processing Standards (FIPS) 104-2.

Performance increases in the new models are the result of faster CPUs, greater memory and overall system improvements. The models offer more memory capacity than comparable current models and many of them offer larger disk space with the option for even greater disk space. For more information visit Blue Coat Systems at www.bluecoat.com

BitDefender unveils next generation security products

BitDefender announced the launch of version 10 of its line of solutions for consumers and small businesses.



Employing BitDefender's new patent pending B-HAVE (Behavioral Heuristic Analyzer in Virtual Environments) technology, version 10 of BitDefender's Internet Security, Antivirus Plus, and Antivirus security solutions offer consumers and small to mid-sized businesses the industry's strongest heuristics-based technology for proactively monitoring and detecting today's most malicious viruses, spyware, spam and phishing activity.

Additionally, all of the solutions will include an anti-rootkit module for detecting and removing rootkits. More information is available at www.bitdefender.com

Payment Card Industry demystified

By Michael Dahn

Over the years the landscape of information security has changed from the need to implement perimeter protection to the concept of defense-in-depth and edge-security. Both of the latter concepts are a result of the changing landscape of fraud. In an effort to prevent fraud and reduce risk across the board, different industries have implemented their own set of compliance requirements.

On the surface the PCI DSS looks very detailed, especially when compared with other standards such as HIPAA, GLBA, and SOX. Underneath the clearly outlined requirements and audit procedures is a lengthy list of compensating controls, third-party systems, outsourcing, small data caveats, and that doesn't even break the surface of the individual requirements and their intent. As PCI begins to gain critical mass and more companies begin to comply there is a need for clarity of vision and understanding for each part of the standard.

This article begins to demystify the Payment Card Industry Data Security Standard; explains the industry, its players, and how they relate; and explain the long list of nuances and differences in these definitions. Through detailed explanation the reader should have a much stronger understanding of the history, current landscape, risks, and best ways to mitigate those risks for your company or the companies you work with. This paper will not make you an expert on the payment card industry but it will give you a great start in beginning to understand the compliance process.

A quick review of the headlines in 2005 demonstrates that organized crime is successfully compromising organizations of all kinds to gain access to credit and debit card data. It seemed like every week there was a new data compromise showing up in the news, eerily shadowing the many more that never made it to press. The credit card associations saw this fraud coming and have been working since 1999 to move the industry onto a more secure path, but it is not as easy as many assume.

The payment card industry is a unique beast when compared with others because it does not fit into a single procrustean box. While other industries fall into "verticals" such as financial services, manufacturing, or education, the payment card industry is described as a "horizontal" because it cuts across most other vertical industries. The majority of companies accept credit cards as payment for services and thus falls under the umbrella of the payment card space. Due to its large size making any change in this market is a slow process that takes time and patience.

The card associations finally combined forces in December of 2004 by creating a common compliance standard to which they all agreed. This reduced the overlap and redundancies as well as compliance costs for companies. The industry emerged in 2005 with a new standard for compliance, but crime continued to increase more than ever as criminals found new and creative attack vectors to target the industry. The card associations, overwhelmed with fighting fires on multiple fronts, tried to push companies to increase the security of their data systems to prevent future fraud. In June of 2005 a large and mostly unknown credit card data processor CardSystems Solutions Inc. (CSSI) was compromised and liable for the potential loss of 40 million credit card numbers. This was the largest data security breach to date and made worse by the fact that CSSI was listed on the Visa web site as a compliant service provider. This one event rocked the industry because of the media coverage it obtained. It seemed as if the public was suddenly concerned with their personal privacy and they began fighting back against the senseless loss of personal information.

In October 2005, John Coghlan, the new President and CEO for Visa U.S.A., announced his focus in helping secure the payment card industry. Although forgoing the use of credit cards is almost unimaginable for many people, the risk of brand reputation loss and the slowing of an ever expanding market could cause millions of dollars of loss for Visa as well as other card associations. Industry experts began to look at all the moving parts and realize the magnitude of what it meant to secure credit card data. For years, companies were storing credit card data along with all the other data they collected because data storage was cheap. Now they were being told not only should they not store it but if they do there is a whole list of controls they must have in place. In many instances these controls relied on software that was sold to them by third parties – entities that were outside their control.

As companies moved slowly towards compliance another problem arose. The standard was so new that everyone interpreted it a little differently. One would think that between security professionals they would all interpret a certain requirement a little different but more or less the same. This assumption proved very wrong as information security consulting companies were submitting proposals for work that varied from $10,000 to $400,000 for the same project. It was clear that these requirements needed some clarification so companies and professionals would have a common understanding about their intent and thus their implementation.

To address this communication problem, Visa U.S.A. (and the other regions internationally) launched a training program for qualified professionals to provide them a common understanding of the industry, compliance requirements, and their intent. This paper does for the individual what Visa has already done for the qualified security companies – it explains the intent, clarifies the ambiguity, and provides examples for how the payment card industry compliance requirements affect your business. After reading this paper you should be better able to understand their recommendations and qualify them to save your company or department time and money.

Creating and rolling out any new standard for any industry is not an easy task. The British standard for information security management (BS 7799) began as a code of practice in 1992 but was not formalized into a standard until 1995. Even then it was not until December of 2000 that it became an international standard as ISO 17799. In 2002, the second part of the standard was published as BS 7799-2. Then in October of 2005 a final draft of ISO 27001 was published that described how to apply the controls of ISO 17799 and how to build and maintain an information security management system (ISMS). It has taken 13 years for the standard to mature from a code of practice into a fully working certification program. This shows that standards are not created perfect but evolve and change over time.

The payment card industry is one of the first to proactively implement an industry specific compliance program. The real estate market implemented a similar industry driven regulation called the REALTOR Secure program but it is nowhere near the size or has as much impact as the one being implemented by the payment card industry. The reason for self regulating is to prevent government intervention and increase consumer confidence. The story goes like this: if the fraud increases too much and the media hypes it, then people will get concerned – if citizens are worried they put pressure on their local and state representatives in government who then pass legislation to control the fraud problem. Legislation is one way of stemming the fraud, but it also binds all of the players in the payment card industry to play by the rules set forth by the federal government. Some may not see a problem with this, but those familiar with the government run Gramm-Leach-Bliley (GLB) Act of 1999 will know that it is better to have Visa as your regulator than the Federal Reserve, FTC, Controller of the Currency and Office of Thrift Supervision. The major difference between industry run regulations and those controlled by the government is that of flexibility. The card associations are better able to update and improve their compliance requirements on a continual basis as opposed to those that govern financial institutions such as Credit Unions with compliance requirements that are only updated on a three year cycle.

...if the fraud increases too much and the media hypes it, then people will get concerned.

This combination of self-regulation and actual teeth to the program (in terms of large fines) are what is driving the industry in the right direction towards protecting a person's credit card data.

The credit card associations include Visa, MasterCard, American Express, Discover, and JCB. These participants came together to agree upon a set of common security requirements that would govern entities that store, process, or transmit cardholder data. The card associations also agreed on the definition of cardholder data as the account number (also known as the Primary Account Number or PAN), the expiration date, track data, personal identification number (PIN) block data, and the card verification value (CVV2). The proper protection of these data elements is mandated by the PCI DSS requirements and must be verified differently depending on the level definition assigned to the organization.

The PCI DSS focuses on 12 different areas of security including: network segmentation, default settings, data encryption, secure network communications, anti-virus software, software development life cycle (SDLC), access restrictions, user authentication, physical security, event logging, testing and auditing systems, and policies and procedures. Each of these areas is optically similar to other information security best practices, but there is a difference in that they focus specifically on cardholder data and the environment that surrounds, connects, and protects that data.

A common confusion is the difference between PCI, Cardholder Information Security Program (CISP), Account Information Security (AIS), and Site Data Protection (SDP). For many who are not familiar with the subtly of the PCI program these acronyms seem interchangeable, but there are important distinctions between them. When the different card associations (Visa, MasterCard, Discover, American Express, and JCB) decided to align their security programs they had to make compromises to account for their differences in structure and location. MasterCard is an association that is internationally chartered meaning that there is only one region that is global in nature. They required their SDP program be implemented universally around the world. Conversely, Visa is made up of six different regions and each has a slightly different way of combating fraud. Visa U.S.A. has the CISP which implements the PCI standard. AIS is the name given to implementation of PCI with the other international Visa regions.

The PCI alignment is the agreement by the different card associations to adopt the following documents as the data security requirements, compliance criteria, and validation procedures.

- PCI Data Security Standard
- PCI Security Audit Procedures
- PCI Self-Assessment Questionnaire
- PCI Network Security Scan Requirements
- PCI Payment Application Best Practices (Proposed)

The PCI DSS applies to any entity that stores, processes, or transmits credit card data and all system components connected to the cardholder data environment. All entities must be compliant, but how they validate their compliance is based on several factors including their transaction volume and what services they provide. These may seem like simple definitions but they grow in complexity with the entity being examined.

Many people get confused about the difference between merchants, service providers, gateways, and data storage entities. The card associations generally break down non-issuing/acquiring/processing entities into: Merchant or Service Provider.

A Merchant is defined as a location or store where purchases are made. The merchant is responsible for the security of the credit card information regardless of who they pass off the information to, such as a service provider.

A Service Provider is defined as an entity that handles credit card information on behalf of a merchant, acquirer, issuer, processor, or other service provider.

Many people think of Amazon, the online book seller, as a simple merchant but they are much more complex than that.

Level 1 Service Provider examples

- Gateways
- VisaNet Processors (member and non-member)
- Data Storage Entity (DSE) - (more than 6 million MasterCard or Visa transactions regardless of acceptance channel)

Level 2 and 3 Service Provider examples

- Data Storage Entity (DSE) - (more than 150,000 and less than 6,000,000 electronic commerce transactions)
- Third-Party Servicer (TPS)
- Independent Sales Organizations (ISO)
- Merchant vendor
- Web hosting company or shopping cart
- Media back-up company
- Loyalty program vendor
- Risk management vendor
- Chargeback vendor
- Credit bureau

Many people think of Amazon, the online book seller, as a simple merchant but they are much more complex than that. Amazon is strangely enough both a merchant and a service provider. They are a merchant because they accept credit cards for the books they sell and a service provider for the transactions they aggregate on behalf of other merchants. Amazon offers other merchants, most notably Target, a storefront for their merchandise. The transactions are processed by Amazon on behalf of many different merchants making them a service provider.

A common misconception with PCI is that if a company does not need to validate their compliance then they do not need to be compliant. This is incorrect because all companies must comply with the PCI DSS, but how these companies validate their compliance will differ depending on the type of organization, their transaction volume, and acceptance channels (i.e. e-commerce vs. brick-and-mortar).

Merchants are divided into four levels depending on their transaction level as shown in the table below. A recent change in the level definitions increased the number of Level 2 merchants by making that level agnostic about acceptance channel and thus capturing many large brick-and-mortar retailers that flew under the radar previously by not having e-commerce systems. The deadline for compliance of all merchants, other than those newly classified as Level 2, has already passed.

Merchant Level	Description
Level 1	• Any merchant-regardless of acceptance channel-processing over 6,000,000 Visa transactions per year. • Any merchant that has suffered a hack or an attack that resulted in an account data compromise. • Any merchant that Visa, at its sole discretion, determines should meet the Level 1 merchant requirements to minimize risk to the Visa system. • Any merchant identified by any other payment card brand as Level 1.
Level 2	Any merchant-regardless of acceptance channel-processing 1,000,000 to 6,000,000 Visa transactions per year.
Level 3	Any merchant processing 20,000 to 1,000,000 Visa e-commerce transactions per year.
Level 4	Any merchant processing fewer than 20,000 Visa e-commerce transactions per year, and all other merchants-regardless of acceptance channel-processing up to 1,000,000 Visa transactions per year.

Level 1 merchants validate their compliance by having an annual on-site data security assessment by a qualified security assessor and performing a quarterly network scan by a qualified scan vendor. These requirements are meant to enforce compliance among the riskiest merchants. Level 2 and 3 merchants must only complete an annual self-assessment questionnaire and a quarterly network scan by a qualified scan vendor. The ability to self-assess is given to those merchants that pose a lower security risk. Level 4 merchants must perform the same measures as Level 2 and 3 merchants but their validation dates and enforcement is regulated by their acquirer.

Service providers are divided into three levels depending on their transaction level. Visa and MasterCard differ on their definitions of a service provider meaning the service provider must assess at the greater of the two level definitions they would fall into. The table below outlines the Visa and MasterCard service provider levels.

Visa Service Provider	Description
Level 1	All VisaNet processors (member and Nonmember) and all payment gateways.
Level 2	Any service provider that is not in Level 1 and stores, processes, or transmits more than 1,000,000 Visa accounts/transactions annually.
Level 3	Any service provider that is not in Level 1 and stores, processes, or transmits fewer than 1,000,000 Visa accounts/transactions annually.

MasterCard Service Provider	Description
Level 1	• All third-party processors. • All data storage entities (DSE) that store account data on behalf of Level 1 or Level 2 merchants.
Level 2	All DSEs that store account data on behalf of level 3 merchants.
Level 3	All other DSEs not included in Levels 1 and 2.

Level 1 and 2 service providers validate their compliance by having an annual on-site data security assessment by a qualified security assessor and performing a quarterly network scan by a qualified scan vendor. Level 3 service providers must only complete an annual self-assessment questionnaire and a quarterly network scan by a qualified scan vendor. All service providers must also submit a letter stating the confirmation of their report's accuracy. This provides clearly worded language from the service providers attesting to the fact that the report being submitted to the card associations is correct and valid.

Credit card compromise cases continue to plague the industry as attackers evolve from one method of attack to another. The current trends show credit card compromises are changing from Internet facing organizations down to the application level.

E-commerce merchants were first on the scene for bringing credit card transactions to the Internet. The credit card lends itself easily to purchasing products and services online through its flexibility and almost universal acceptance. Credit cards can either be used in a 'swipe' transaction where the credit card is presented to the merchant and the magnetic track is read or in a 'card not present' transaction where only the credit card number and expiration date are available. Card not present transactions are a higher risk due to the fact that the information could be forged. In addition to the risk of card not present transactions there is the inherent risk that e-commerce systems are susceptible to attack by any user connected to the Internet.

Service providers pose a unique risk in that they typically handle credit card data from multiple entities, either merchants, acquirers, or processors. A gateway aggregates transactions from multiple merchants thus increasing the volume and risk posed by these organizations. Service providers typically aggregate e-commerce transactions but can just as easily aggregate transactions from brick-and-mortar merchants.

Retail merchants pose a specific risk as more and more stores are being connected together via the Internet or use wireless networks for POS or inventory purposes. The first risk arises as retail stores are being connected directly to the Internet. As companies grow and open new stores they are constantly looking for an inexpensive method of remotely managing them. These companies need a way of remotely managing and accessing each store for administrative purposes. As a result many companies install a broadband or dial-up connection to the Internet at each store location. This connection is used to remotely access the store either through a virtual private network (VPN) or other remote control software such as pcAnywhere. The risk associated with a retail location being directly connected to the Internet through the use of remote management software is relatively high with the weakest link in the security chain being the authentication mechanism.

The second risk outlined for retail merchants is that of wireless networks being used at a store location and not properly secured. A recent report identified "the wireless LAN (WLAN) market will grow at an annual rate of 30 percent per year … [it] also found that WLAN sales have increased 60 percent compared to last year." This growth in wireless networking has not been ignored by retail merchants as they begin to implement such networks for operating their POS or inventory systems. The risk of wireless networks is that few companies implement proper security or network segmentation to make these networks safe for financial transactions.

In the past two years many retail stores have been compromised including DSW Shoe Warehouse, Polo Ralph Lauren, and BJ's Wholesale Club Inc. This trend has increased as attackers learn that compromising these systems is sometimes easier and more lucrative than other locations.

If an attacker wishes to compromise a payment gateway they are usually faced with circumventing a corporate firewall or looking for a vulnerability in one of their Internet applications. Retail merchants on the other hand offer much less resistance with some connected to the Internet with no firewall at all.

For many companies compliance is driven by a stick rather than a carrot. Publicly traded companies comply with Sarbanes-Oxley (SOX) because if they don’t the Securities and Exchange Commission (SEC) could shut them down. Financial institutions comply with Gramm-Leach-Bliley (GLB) so the Federal Reserve or their Financial Deposit Insurance Corporation (FDIC) auditors do not force them to close. The reason companies adhere to the PCI DSS standard is because non-compliance could result in fines (egregious violations up to $500,000), forensic investigation costs, issuer and acquirer losses (unlimited liability for fraudulent transactions and any card replacement costs), as well as any dispute resolution costs.

Although Visa cannot directly fine merchants and service providers they can assign fees to the acquirer who can contractually pass them on to the appropriate merchant or service provider. If an acquirer does not have a direct relationship with a service provider it is important that the merchant who does have that relationship have legal contracts in place to verify they can pass the fees along to the service provider.

Without such contractual assignment of fees the merchant would be stuck with any fees assigned to them resulting from a compromise of their credit card data even if their service provider was at fault.

For many companies compliance is driven by a stick rather than a carrot. Publicly traded companies comply with Sarbanes-Oxley (SOX) because if they don’t the Securities and Exchange Commission (SEC) could shut them down.

In addition to the negative impact there are several positive reasons to comply with the PCI DSS. Merchants that wish to comply with PCI DSS must validate that their service providers are also compliant.

As a result service providers are offering their compliance as a competitive advantage. Although the list of compliant merchants is not publicly accessible, Visa posts a list of all compliant service providers on their website.

Additionally, companies that want to distinguish themselves from their competition or show their customers that their personal data is secure will comply and issue a press release as well as publicizing it in their marketing material. This is especially true with application vendors that have proactively brought their software into compliance with the Payment Application Best Practices (PABP).

The PABP is a set of best practices that has not yet become part of the PCI compliance requirements, but many companies have complied with them in order to obtain a competitive advantage or so their customers can meet their compliance requirements.

Ultimately, the often overlooked benefit to a company that meets compliance with the PCI DSS is that they are more secure. Having reviewed many companies large and small, there is not one that met all of the compliance requirements when first audited. Each company has something to implement: be it policies or a firewall that will make their company and their customer’s data more secure.

Keeping customer data secure may seem like an altruistic goal but transitively it keeps the company in business. There have been many examples where a company lost their customer data that in turn caused long term brand and reputation damage to the company.

An important thing for upper management to understand is the difference between compliance and security. When a company is considering a compliance standard they look to the expert in that one area and have them assist with the one compliance issue instead of examining all compliance requirements surrounding data security. For example a bank may have several compliance requirements such as GLB, PCI DSS and state notification laws (i.e. SB1386). Companies that have multiple requirements should assign the responsibility for data security compliance to an internal person. If external assistance is required then a firm that can help meet compliance with multiple requirements is better than having separate firms assist with addressing individual requirements. This reduces redundancies and cost associated with the compliance process.

Once companies assign an employee the responsibility of compliance that employee should educate upper management about the difference between compliance and security. Although many companies find the compliance requirements arduous and time consuming to comply with, they only represent the minimum best practice guidelines for data security. While compliance meets a minimum standard, some companies may wish to go above and beyond these requirements to ensure the security of their systems in other ways.

This method of thinking represents a differentiation between security and compliance. Although many people think that by meeting their industry compliance requirements they will be secure from all hackers and compromises this is not necessarily the case. One simple example is that of internal employee theft. Contrary to common belief, most security compromises occur as a result of some form of insider fraud. This means that even though a company complies with all stated requirements there is still the risk that an insider with proper access, or in collusion with a second employee, could gain access to sensitive data and remove it illegally from the company.

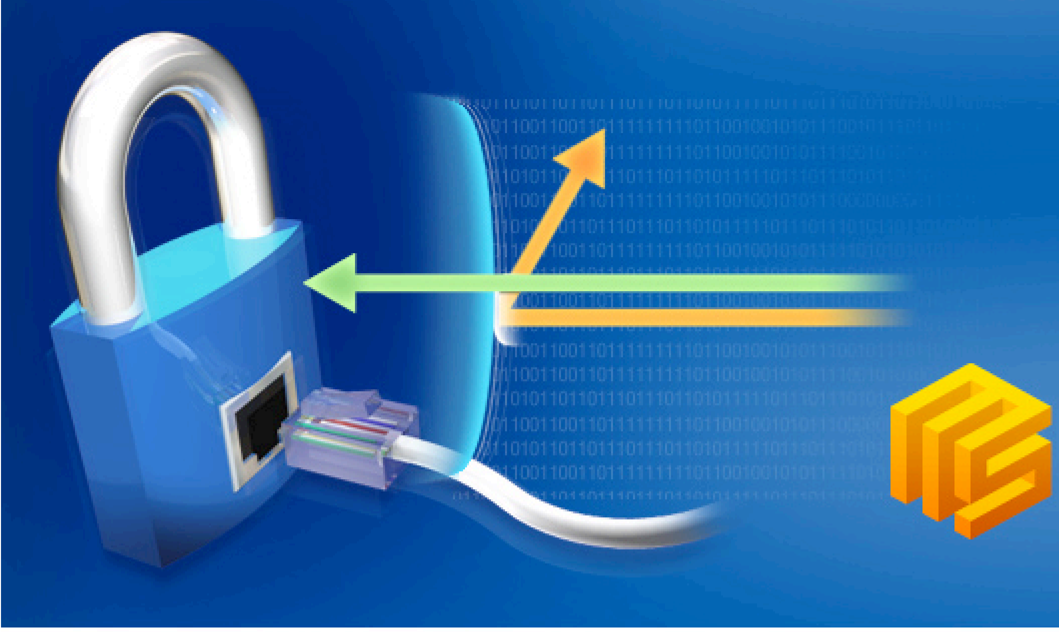
Another example of where compliance does not equal security is that of operational management over information security systems. To meet compliance requirements a company must have certain controls in place as well as operational management of these controls. A company may be compliant one day and not the next because the operational controls were not followed throughout the year. This is a reminder that compliance is measured as a point in time but security is continuous 24 hours a day, 7 days a week, and 52 weeks a year.

The requirements look simple at first but there are many nuances to them that require a careful understanding of the credit card industry and all players involved. It is important that companies understand their risk exposure and what they need to validate compliance. Only by understanding the framework can a company then begin to dissect the details and intent behind each requirement.

But before deciding whether or not to comply it is important to understand the risks and implications of either decision. Compliance does not equal security so creating a compliance work plan should also involve mapping the security needs of your company to the desires of the compliance requirements. Only then will compliance become an integral and beneficial part of your business.

Michael Dahn is the President of Volubis, Inc. responsible for the management of consultants and project engagements. Mr. Dahn has a technical background in the management, design, systems integration and implementation of information security technologies for financial institutions, commercial and international clients.

Mr. Dahn serves on the Board of Directors for the InfraGard National Members Alliance and is a Certified Information Systems Security Professional (CISSP). His professional memberships include the (ISC)2, High Technology Crime Investigation Association (HTCIA), Information Systems Security Association (ISSA), and InfraGard.



ModSecurity for Apache

ModSecurity™ is an embeddable web application firewall. It provides protection from a range of attacks against web applications and allows for HTTP traffic monitoring and realtime analysis with no changes to existing infrastructure.

Why ModSecurity?

ModSecurity puts you back in control. Here are the top six reasons to use it:

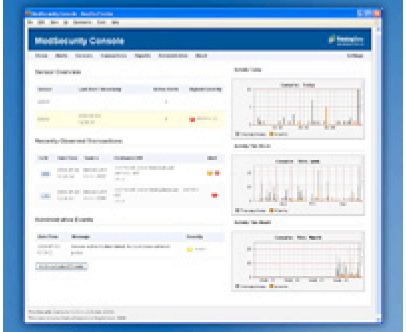
1. **Embeddable**; Works with your existing architecture. Quick to install and does not cause disruption. Quick to remove, too, if you decide you don't like it.
2. **Network-based**; To protect many web servers at once, or applications running on web servers other than Apache, install ModSecurity as part of an Apache-based reverse proxy.
3. **Monitoring**; Unlike many other network-based tools, ModSecurity is capable of observing SSL-encrypted web traffic.
4. **Just-in-time patching**; Reduces the window of opportunity by making it possible to patch a vulnerable application from the outside, with no access to the source code.
5. **Forensic logging**; You will be able to see the attack payloads transported in the HTTP request bodies. Choose what you want to log: just attacks, everything or (through the flexible rule language) exactly what you want logged.
6. **Detection and protection**; Works as an intrusion detection tool but can easily be configured to add a protection layer to your applications, defending from classes of attack at once.

ModSecurity for Apache is a free open source product. OEM licences and commercial support contracts are available from Thinking Stone.

ModSecurity Console

Real-time log and alert centralisation solution for ModSecurity

- All-in-one solution, comes with embedded web server and database.
- Reliable log centralisation, storage, and maintenance.
- Clean web-based graphical user interface.
- Email and PDF reporting.
- Portable and easy to install.



Early Adopter Discount Now $350

www.thinkingstone.com
www.modsecurity.org

ThinkingStone
Securing Web Applications

Skype: how safe is it?

By Tom Newton

VoIP has hit the headlines in recent months and while some stories have focussed on the ways in which the technology is proliferating throughout the commercial world, other perhaps more alarming articles have touched on the security risks. Whilst these reports haven't quite hit levels of mass hysteria, and coverage has, by and large, been fueled by vendor hype, the discussion surrounding VoIP security has merit.

Although the underlying technologies of VoIP have been around almost as long as IP and implementations have existed for many years, it is only now that usage is extending from intra-office systems to worldwide usage both commercially and privately. To this extent, VoIP is an immature technology.

Until commerce relies on a system, it is unlikely to be adequately tested. Before the World Wide Web was a commercial prospect, it was held together by software which would now be viewed as somewhere between quaint and crazy. VoIP has matured, but is yet to really be tested. In addition, a number of companies have begun offering gateway services from Plain Old Telephone Systems (POTS) to VoIP and vice-versa, greatly enhancing its functionality and assisting quick take-up.

VoIP is an immature technology emerging into an increasingly hostile world, but there's little we can do about this. In a world where agility and time-to-market routinely come before cost and security, the roll-out of new technologies is as inevitable as the change of season. IT security professionals would urge caution in a situation such as this - watch the early adopters and you might just avoid getting burned. Why this article? Surely this situation is sufficiently commonplace as to render it uninteresting? Perhaps it is, until you consider Skype.

Skype re-writes VoIP rules

Skype is VoIP on steroids. Even before eBay's muscle backed the telecoms company, Skype swept all before it becoming the de facto standard in a short space of time. The reasons for this are more than mere good timing.

The Skype client is ‘free’, at least to the extent it costs no money. This, plus cross platform compatibility, good voice quality and a range of peripheral services such as Skype Out have helped the software client to over 247 million downloads (source: Skype.com). Other than its ubiquity, there are other interesting, and in some cases slightly disturbing, features of Skype.

One of the reasons Skype is so easy to use is that it works on almost any network, even behind a NAT or firewall with no special configuration. Such NAT traversing peer-to-peer activity is almost impossible to detect or block, especially when you factor in the encryption of Skype data. Any network administrators reading should be worried at this point. Without resorting to client-side restrictions, Skype is very difficult to stop; layer 7 blocking may be effective, but this is rarely black and white. Skype transfers information, including file transfer and instant messages, both in and out of the corporate network, unchecked, unrestricted and encrypted. Security professionals should be pulling their hair out because of this, and there should be P45s in waiting for any IT administrator who hasn’t recognised this issue.

Secrecy poses questions

Other concerns with this technology stem from the closed nature of Skype's protocol. Its website gives little away and few know in detail the internal workings of Skype. It just works, apparently. This poses a number of problems.

Firstly, because Skype may route your calls through untrusted hosts, your data must be encrypted. Even if this were not the case, it is likely that you'd wish to secure your data. The encryption scheme used is, to all intents and purposes, untested. Bruce Schneier, one of the most respected security authorities, suggests that the best thing you can say about an encryption scheme is: "We can't break it". This is even better if other clever people can't break it either. However, the encryption used in Skype is afforded little of the rigorous academic and commercial review of say AES or other freely examinable algorithms. Similarly, the underlying peer-to-peer systems are unknown. How peers through which your data are routed are chosen remains unknown. It is not impossible that a wily attacker might exploit bugs or nuances in routing to their own ends. Study of Skype's protocol for any purpose is expressly forbidden in the license, which does not inspire confidence.

Secondly, closing the protocol necessitates closing the client. This may not appear to be a significant issue, but in this instance it means that the only Skype clients are Skype clients (if you follow my capitalization). This represents a problem akin to that experienced by Microsoft Outlook users some years ago - the evolutionary ‘dead-end’ that is a homogeneous environment. With one dominant client, the first email worms spread rapidly and caused significant damage. Similarly, Internet Explorer's dominance gave it a high profile to would-be attackers. Once a security flaw is found in Skype (and anyone who believes any software other than "Hello World" is immune from security flaws has been watching cartoons), it is exploitable worldwide. In terms of worms and viruses, this is write once, execute anywhere. Admittedly, email worms have calmed somewhat, and are now more reliant on wetware flaws (human error) than bugs in a particular software client, but email is a much more mature technology. Worms, trojans and viruses, however have also matured. Expect increasingly sophisticated tricks as PCs are ‘owned’ by hackers.

This ‘one client’ approach not only forcibly widens a user's circle of trust (those entities in which a user is willing to entrust their security), but it adds a well known trouble-causer to the list. eBay, Skype's 2.5 billion dollar new owners, have a less than exemplary record with regard to their handling of user data. Existing articles have already flagged this salient point, but if you wish to talk with other ‘skypers’, you're going to have to agree to eBay's terms. How its policies will stack up outside the US remains to be seen. Many businesses would rather pay for a client and gain the support of a commercial product. By agreeing to the license, you also "grant permission for the Skype Software to utilize the processor and bandwidth of Your computer for the limited purpose of facilitating the communication between Skype Software users" - a "limited purpose" with quite a broad remit!

Defend the network

With potential security problems like these, it would be wise to run Skype with caution, if at all. A NAT firewall would mitigate direct attacks against your client or server, for example. Unfortunately, some Skype nodes are more vulnerable than others, offering more by way of connectivity to untrusted parties. These are the ‘Supernodes’, used for routing calls and allowing two NAT restricted ‘skypers’ to converse. Any attacker would see a ‘Supernode’ as an obvious target – after all this is access to a network service, and traditional network services like HTTP, FTP and DNS have always seen huge potential for worms such as code red. HTTP servers are easy to find, but what of Skype ‘Supernodes’? Well, you have but to ask. The Skype server will, with a little coaxing, happily provide a list of IPs currently known to be running as ‘Supernodes’. This is to allow the NAT-ed Skype client who's built-in ‘Supernode’ list is outdated to easily find a ‘Supernode’ via which to route calls. This list of easy targets is unavoidable, and clearly poses considerable risk.

As Skype gains popularity it will come under greater scrutiny by both the security industry and those with less benign intentions. Threats could range from lawsuits, through misuse akin to the productivity losses incurred by spurious web browsing prior to the introduction of effective content filters and logging, right through to serious security breakdowns. What can we do about this? Locking down client PCs, limited roll-out where necessary and intelligent security polices are among the best defences when implemented with the right perimeter firewall and proxy suite. This technology is inevitable, and it looks like Skype may ‘VHS’ the world with a possibly inferior, but ubiquitous, cheap and effective product. Don't say you weren’t warned.

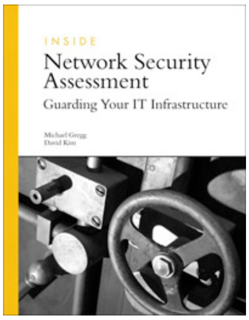
Tom Newton is the product development manager at SmoothWall (www.smoothwall.net), an Internet security provider now protecting over a million networks worldwide.

Latest additions to our bookshelf

Inside Network Security Assessment: Guarding Your IT Infrastructure

by Michael Gregg, David Kim

Sams, ISBN: 0672328097

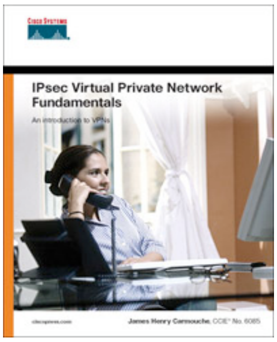


Inside Network Security Assessment: Guarding Your IT Infrastructure is a collection of utilities and templates that will take you through the assessment process. Written by two highly qualified authors with close ties to the International Information Systems Security Certification Consortium, this book was developed with the goal of being a text for the CISSP continuing education class on Network Security Assessment. You will be provided with step-by-step training on assessing security, from paperwork to penetration testing to ethical hacking.

IPsec Virtual Private Network Fundamentals

by James Henry Carmouche

Cisco Press, ISBN: 1587052075

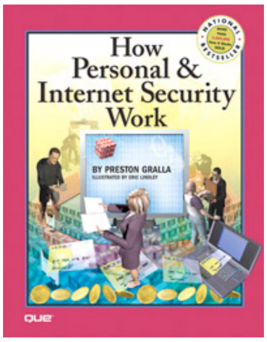

Cisco Systems
IPsec Virtual Private Network Fundamentals
An introduction to VPNs
ciscopress.com
James Henry Carmouche, CCIE® No. 6085

IPsec Virtual Private Network Fundamentals provides a basic working knowledge of IPsec on various Cisco routing and switching platforms. It provides the foundation necessary to understand the different components of Cisco IPsec implementation and how it can be successfully implemented in a variety of network topologies and markets (service provider, enterprise, financial, government). This book views IPsec as an emerging requirement in most major vertical markets, explaining the need for increased information authentication, confidentiality, and non-repudiation for secure transmission of confidential data.

How Personal & Internet Security Works

by Preston Gralla

Que, ISBN: 0789735539



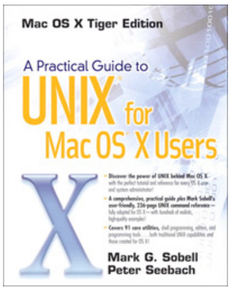
How Personal and Internet Security Works illustrates in vivid detail the many dangers faced by those who use the Internet to send or receive email, surf the Web, conduct personal business, use a credit card, or even travel to airports and how those dangers can be solved.

You'll also get detailed explanations of Internet privacy issues such as spyware, phishing, identity theft, data mining, biometrics, and security cameras, as well as Homeland Security issues such as airport scanning and terrorist screening.

Practical Guide to UNIX for Mac OS X Users

by Peter Seebach, Mark G. Sobell

Prentice Hall, ISBN: 0131863339

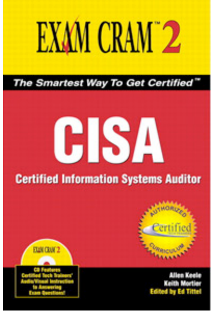


This book explains UNIX for the Mac OS X user–giving you total control over your system, so you can get more done, faster. Building on Mark Sobell's highly praised A Practical Guide to the UNIX System, it delivers comprehensive guidance on the UNIX command line tools every user, administrator, and developer needs to master–together with the world's best day-to-day UNIX reference. This book is packed with hundreds of high-quality examples. From networking and system utilities to shells and programming, this is UNIX from the ground up–both the "whys" and the "hows"–for every Mac user.

CISA Exam Cram: Certified Information Systems Auditor

by Allen Keele, Keith Mortier

Que, ISBN: 0789732726

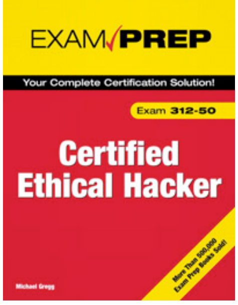


Want an affordable yet innovative approach to studying for the Certified Information Systems Auditor (CISA) 2005 exam? CISA 2005 Exam Cram 2 is your solution. You will have the essential material for passing the CISA 2005 exam right at your fingertips. All exam objectives are covered and you'll find practice exams, exam alerts, notes, tips and cautions to help guide you through your exam preparation. A CD also provides you with a video introduction to the exam and complete explanations of answers to the practice questions from Certified Tech Trainers (CTT).

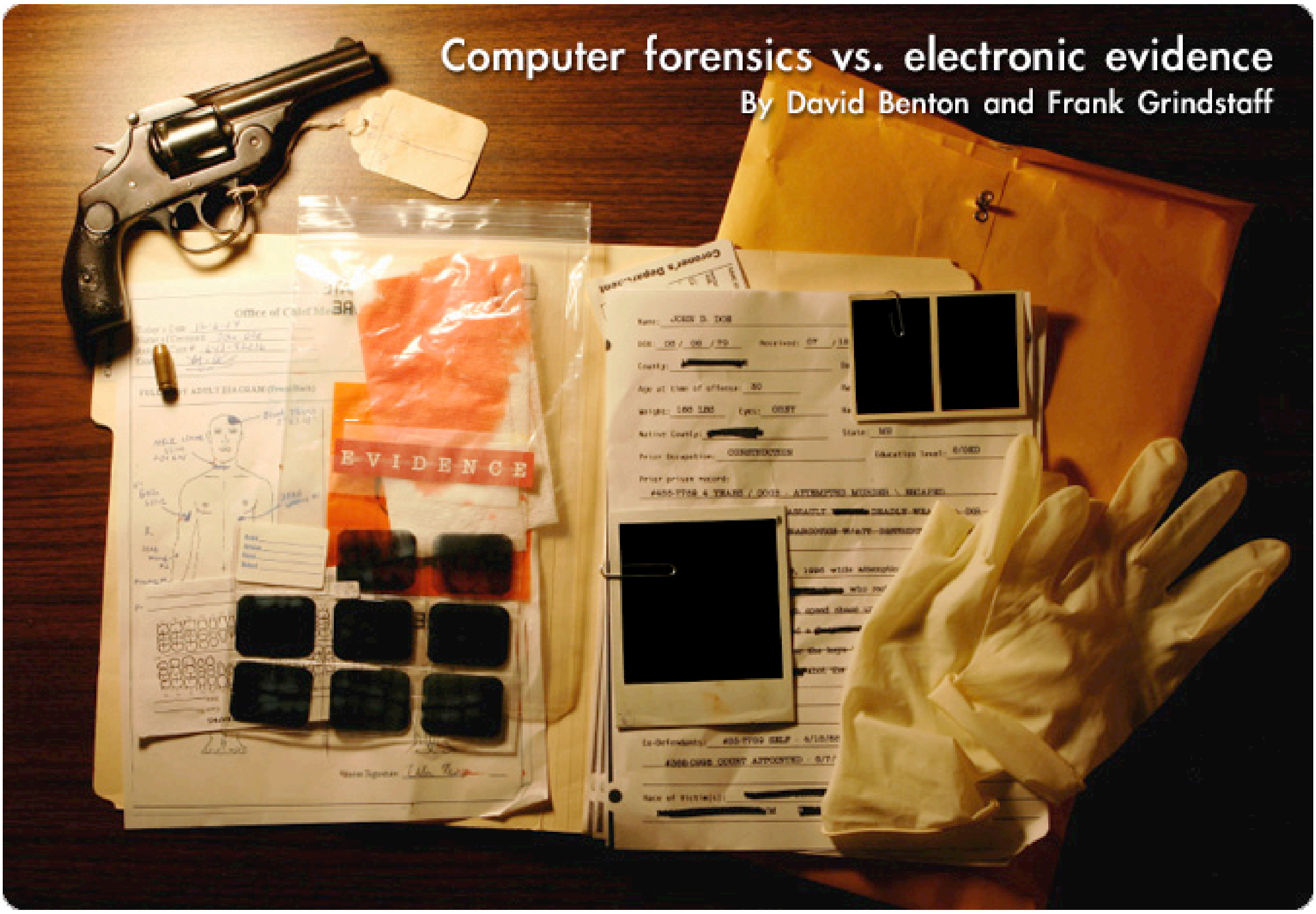
Certified Ethical Hacker Exam Prep

by Michael Gregg

Que, ISBN: 0789735318



Certified Ethical Hacker Exam Prep is the perfect solution for the CEH exam, giving you the solid, in-depth coverage you'll need to score higher on the exam. Along with the most current CEH content, the book also contains the elements that make Exam Preps such strong study aides: comprehensive coverage of exam topics, end-of-chapter review, practice questions, Exam Alerts, Fast Facts, plus an entire practice exam to test your understanding of the material. The book also features MeasureUp's innovative testing software, to help you drill and practice your way to higher scores.



Computer forensics vs. electronic evidence

By David Benton and Frank Grindstaff

Electronic Evidence is changing the scope and face of many regulatory and judicial investigations. People may wonder why they need computer forensics in an investigation if they are already using an electronic evidence specialist. Why should they pay twice for what they perceive as being the same service?

In an investigation if there is a large amount of items like documents and emails from a large number of computers, an electronic evidence firm can effectively and efficiently gather the files and organize them. If the documents are not in electronic format they can be scanned and included in the process. Once these items are in electronic format they can be filtered, searched, and reviewed with relative ease. In a small investigation where there is only one or two personal computers involved, you use a computer forensics specialist for this. While there is some truth to this there is also a lot wrong with it.

In a large investigation it is common to use a firm specializing in electronic evidence to handle the electronic discovery needs in the investigation. The electronic discovery could cover ten's to thousand's of hard drives depending on the scope of the investigation. If this is the only type of electronic discovery being utilized, your investigation could be missing a lot. While it may be impractical and cost prohibited to forensically review all of the hard drives at a company, it may also be seen as negligence to not forensically review a few selective hard drives in an investigation/ discovery process.

When do you need a computer forensics specialist and when do you need Electronic Discovery services?

First it is perhaps helpful to define computer forensics and EDiscovery. Computer Forensics is the application of the scientific method to digital evidence during an investigation in order to establish fact, which may be used in judicial proceeding. EDiscovery is the providing of electronic document(s) pursuant to a request or order from a regulatory or judicial authority.

A forensic review of selective computers can help an e-discovery team work more efficiently by helping them narrow their scope in its time frame, number of locations, number of computers (email servers, network servers) and number of people. Another item to consider is do you want to review deleted items? If so, a forensic review is a must for that computer. Below is a table comparing electronic discovery and computer forensics on some of the key points.

Computer Forensics	Electronic Discovery
Investigate and Detail Analysis Typically targets selected hard drives Searches everything on the hard drive, “deleted” and active items Determine who, what, and when Creation of a timeline of events Reporting and expert testimony Breaking of passwords/encryption May include backup tapes, email servers, other servers Includes meta-data Normally reviewed by one person at a time, in one location Searches can take hours or days	Gathering, searching, filtering, and producing large amounts of information for review Can cover thousands of hard drives Active and archived data, normally does not include deleted, discarded, hidden, or encrypted data Data is accessed, but not analyzed Can include backup tapes, email servers, other servers May or may not include meta-data Can be reviewed by numerous people in several locations Searches can take minutes or hours

You may notice that searches in computer forensics can take days, compared to minutes for electronic discovery. This seems odd until you look at the way searches are done using computer forensic software.

Consider that a typical personal computer has an 80 GB hard drive can have 18,181,820 pages of data on it. Electronic discovery may only look at a small fraction of this data, and the search is a text search (byte by byte). In computer forensics every bit of the hard drive is searched bit by bit, (note: eight bits equals one byte). In general, the bit by bit search algorithm is much slower than the text search. This speed difference and the searching by bits instead of bytes requires much more time.

At one time computer forensics was very expensive and was viewed as unaffordable for the average case. This meant that if any electronic evidence was reviewed it was done through electronic discovery, not computer forensics. Now, with innovations in computer forensic software a forensic examination of a hard drive is reasonably affordable. This has caused more and more cases to include electronic evidence that just a few years ago would have ignored it. This has caused some interesting developments as there was very little case law to guide attorneys and judges in these matters. The past few years have seen more and more rulings on items found using computer forensics and more conferences and work groups formed to publish guidelines on electronic discovery and computer forensics. One such organization is The Sedona Conference (thesedonaconference.org), which is a non-profit, non-partisan law and policy think-tank.

One of the Work Groups, WG1: Electronic Document Retention and Production, purpose is to develop principles and best practice guidelines concerning electronic evidence retention and production. These guidelines were developed as a joint collaboration between attorneys in the public and private sector, judges, and other experts. Here are the 14 proposed guidelines:

1. Electronic data and documents are potentially discoverable under Fed. R. Civ. P. 34 or its state law equivalents. Organizations must properly preserve electronic data and documents that can reasonably be anticipated to be relevant to litigation.

2. When balancing the cost, burden and need for electronic data and documents, courts and parties should apply the balancing standard embodied in Fed. R. Civ. P. 26(b)(2) and its state-law equivalents, which require considering the technological feasibility and realistic costs of preserving, retrieving, producing and reviewing electronic data, as well as the nature of the litigation and the amount in controversy.

3. Parties should confer early in discovery regarding the preservation and production of electronic data and documents when these matters are at issue in the litigation, and seek to agree on the scope of each party's rights and responsibilities.

4. Discovery requests should make as clear as possible what electronic documents and data are being asked for, while responses and objections to discovery should disclose the scope and limits of what is being produced.

5. The obligation to preserve electronic data and documents requires reasonable and good-faith efforts to retain information that may be relevant to pending or threatened litigation. However, it is unreasonable to expect parties to take every conceivable step to preserve all potentially relevant data.

6. Responding parties are best situated to evaluate the procedures, methodologies and technologies appropriate for preserving and producing their own electronic data and documents.

7. The requesting party has the burden on a motion to compel to show that the responding party's steps to preserve and produce relevant electronic data and documents were inadequate.

8. The primary source of electronic data and documents for production should be active data and information purposely stored in a manner that anticipates future business use and permits efficient searching and retrieval. Resort to disaster recovery backup tapes and other sources of data and documents requires the requesting party to demonstrate need and relevance that outweigh the cost, burden and disruption of retrieving and processing the data from such sources.

9. Absent a showing of special need and relevance, a responding party should not be required to preserve, review or produce deleted, shadowed, fragmented or residual data or documents.

10. A responding party should follow reasonable procedures to protect privileges and objections to production of electronic data and documents.

11. A responding party may satisfy its good-faith obligation to preserve and produce potentially responsive electronic data and documents by using electronic tools and processes, such as data sampling, searching or the use of selection criteria, to identify data most likely to contain responsive information.

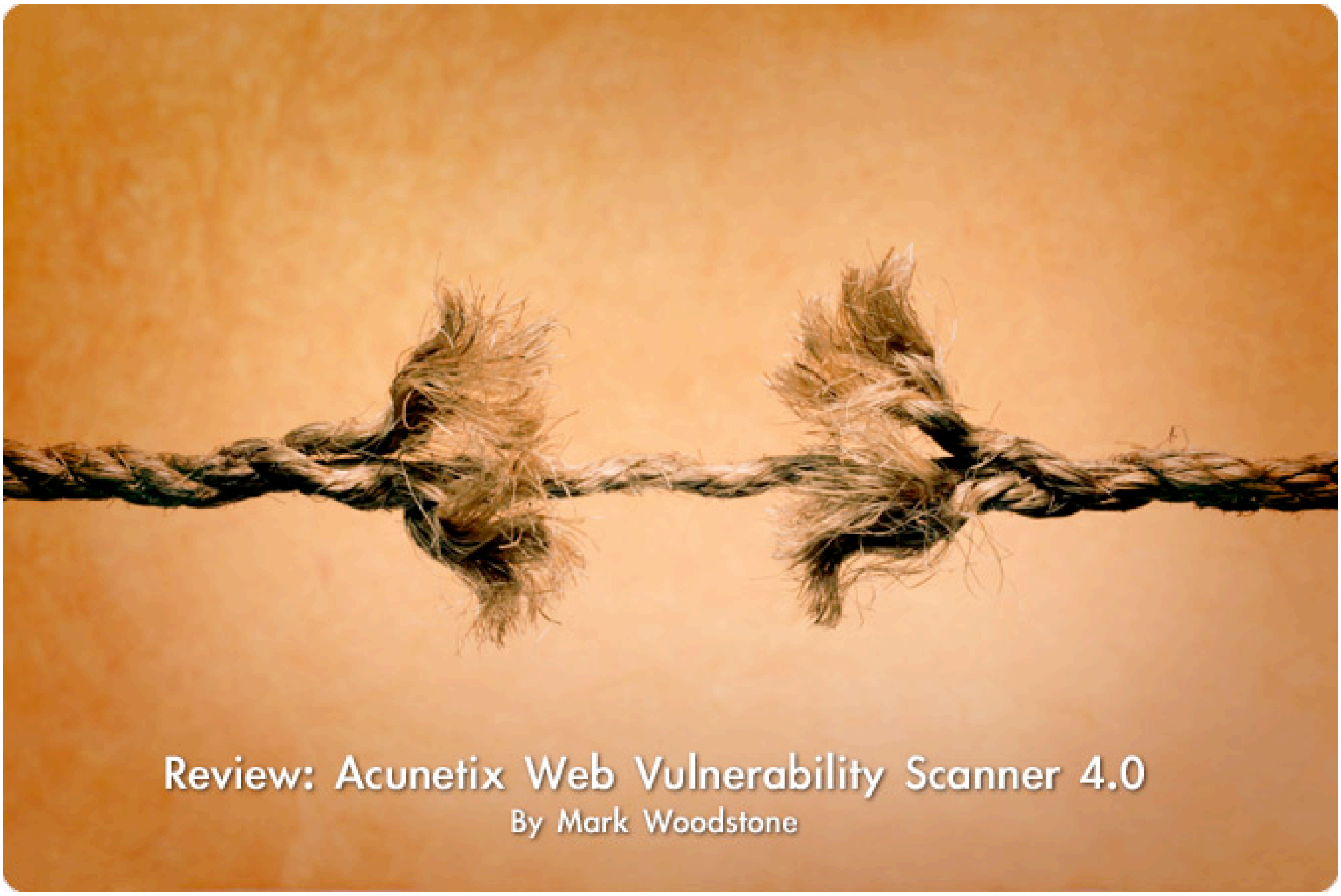
12. Unless it is material to resolving the dispute, there is no obligation to preserve and produce metadata absent agreement of the parties or order of the court.

13. Absent a specific objection, agreement of the parties or order of the court, the reasonable costs of retrieving and reviewing electronic information for production should be borne by the responding party, unless the information sought is not reasonably available to the responding party in the ordinary course of business. If the data or formatting of the information sought is not reasonably available to the responding party in the ordinary course of business, then, absent special circumstances, the costs of retrieving and reviewing such electronic information should be shifted to the requesting party.

14. Sanctions, including spoliation findings, should only be considered by the court if, upon a showing of a clear duty to preserve, the court finds that there was an intentional or reckless failure to preserve and produce relevant electronic data and that there is a reasonable probability that the loss of the evidence has materially prejudiced the adverse party.

Over the last year or so there has been more merging of electronic evidence tools with computer forensic tools. Where electronic evidence tools would search the storage media on a computer or network, it generally would only look at undeleted or active files. If you thought the file you needed had been deleted, then you called in the computer forensic person. They would get the deleted files, file fragments, and other artifacts left on the computer storage media. As electronic evidence becomes more prevalent in court, vendors are beginning to develop more sophisticated tools which will become increasingly important as companies must now be sure they comply with the new Federal laws such as Sarbanes-Oxley.

J. Frank Grindstaff, Jr., (CPA, CISA, CIA, CCE, EnCE) is on the computer forensics team of a Fortune 500 company. Frank is a past president of the Atlanta Chapter of Information Systems Audit & Control Association (ISACA) and is active in several professional organizations including the High Tech Crime Investigation Association (HTCIA), ISACA, and the Georgia Society of CPA's. Frank can be contacted at www.gsforensics.com.



Review: Acunetix Web Vulnerability Scanner 4.0

By Mark Woodstone

Ten years ago I started working for a small San Francisco based startup that was offering consulting services for financial institutions. One of my first duties there was to be a part of a small penetration testing team.

Back then we had some good pieces of code that was helping us to test modem connections, file servers and different networking equipment.

At my current job position, my employer often sends me to information security conferences all over the States. From the lectures I attend and companies exhibiting, it is very obvious that the current hot trend is web application security.

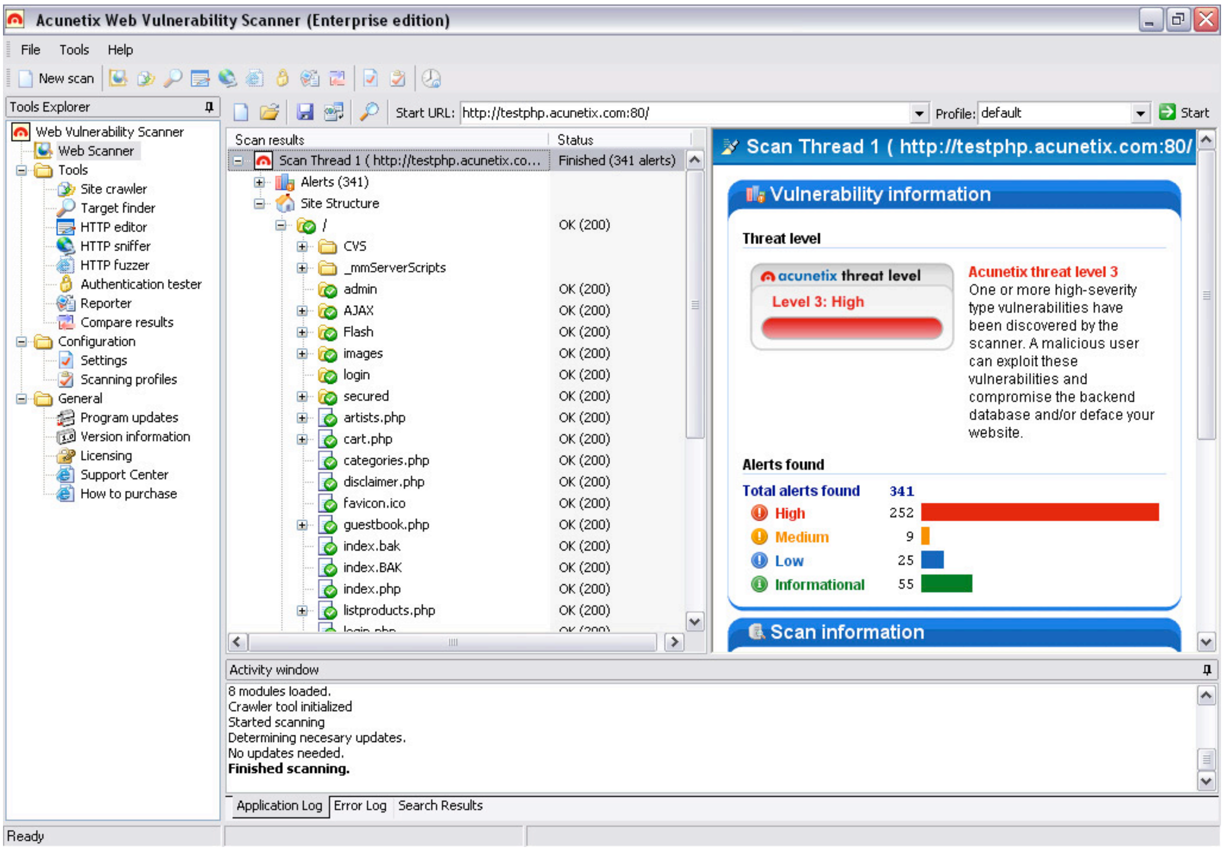
With a growing number of businesses going online, web applications became one of the biggest security issues. The types of scanners we used back then evolved to another level following the latest threats.

Acunetix Web Vulnerability Scanner is one of the rather new products in the evolving web application security market. Before I start this review, I must give you a disclaimer - because of company policy, some of the screenshots accompanying the review will be obfuscated or even taken from a scan of Acunetix test web servers.

For the purpose of this review I used the latest version of Acunetix Web Vulnerability Scanner available - 4.0. With an installation file of just above 8 MB, the software will take approximately 28 MB of space.

As you can see from the screenshot on the following page, a straightforward software GUI offers an optimized three-column structure. From left to right we have a main set of options and tools, scan results and a window containing details of a selected vulnerability alert.

The bottom of the screen hosts a real time activity window that shows the progress of the scanning process.



Start URL: http://testphp.acunetix.com:80/ Profile: default

Scan results	Status
Scan Thread 1 (http://testphp.acunetix.co...	Finished (341 alerts)
Alerts (341)	
Site Structure	
/	OK (200)
CVS	
_mmServerScripts	
admin	OK (200)
AJAX	OK (200)
Flash	OK (200)
images	OK (200)
login	OK (200)
secured	OK (200)
artists.php	OK (200)
cart.php	OK (200)
categories.php	OK (200)
disclaimer.php	OK (200)
favicon.ico	OK (200)
guestbook.php	OK (200)
index.bak	OK (200)
index.BAK	OK (200)
index.php	OK (200)
listproducts.php	OK (200)
login.php	OK (200)

Scan Thread 1 (http://testphp.acunetix.com:80/

Vulnerability information

Threat level

acunetix threat level
Level 3: High

Acunetix threat level 3
One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

Alerts found

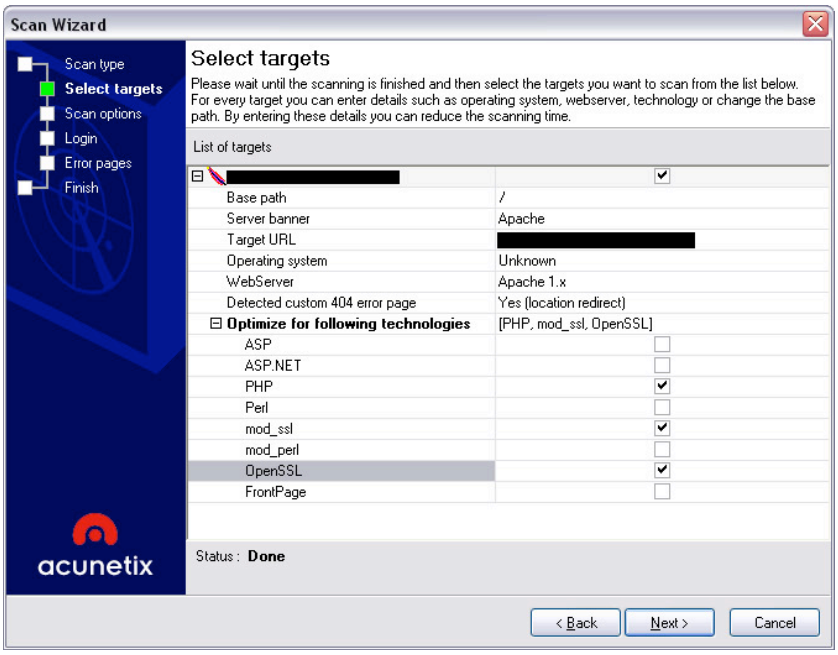
Total alerts found	341
High	252
Medium	9
Low	25
Informational	55

Scan information

```
8 modules loaded.
Crawler tool initialized
Started scanning
Determining necesary updates.
No updates needed.
Finished scanning.
```

Figure 1. Acunetix Web Vulnerability Scanner main screen.

There are four different scan types. The default one offers a normal procedure where one web site gets all the attention. If the user wants to scan multiple sites, there is an option to select a file that contains the list of URls. If you already used the software's built-in crawler module, you can also act upon its results. The final scan type offers scanning of a range of IP addresses with web servers running on ports specified by the user. I mostly used the default option for scanning a single web site. After choosing this option, user is able to use predefined set of scanning profiles and to set specific crawling options. If in any case the target web server is located behind a HTTP authentication window, you will be able to fill in your credentials. When you setup the initial scan settings, hitting the finish button will fire away the scanner.



Select targets

Please wait until the scanning is finished and then select the targets you want to scan from the list below. For every target you can enter details such as operating system, webserver, technology or change the base path. By entering these details you can reduce the scanning time.

List of targets

[redacted]	☑
Base path	/
Server banner	Apache
Target URL	[redacted]
Operating system	Unknown
WebServer	Apache 1.x
Detected custom 404 error page	Yes (location redirect)
Optimize for following technologies	[PHP, mod_ssl, OpenSSL]
ASP	☐
ASP.NET	☐
PHP	☑
Perl	☐
mod_ssl	☑
mod_perl	☐
OpenSSL	☑
FrontPage	☐

Status : Done

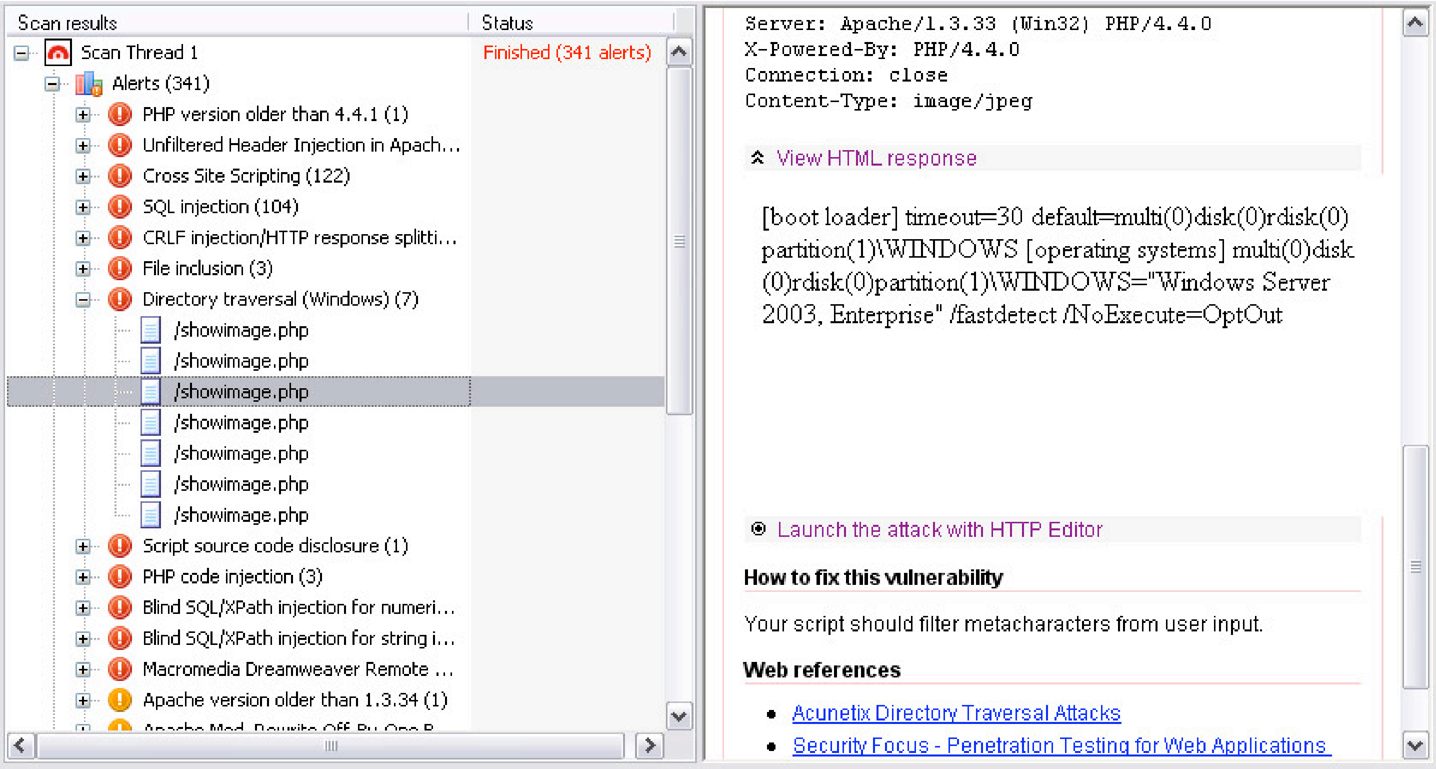
Figure 2. The Scan Wizard.

Although the automatic scan finds a huge amount of specific information that could result in a possibly vulnerable application, the "Manual browsing window" that opens during the scan is surely a nice touch by the developers. In the window, the user can browse the site that is being scanned so the software crawler can identify the files that are not directly accessible or were not discovered by the crawling process. This option is especially interesting with web sites that use JavaScript navigation.

Time consumption is an important aspect of vulnerability scanners. Both on a simple PHP based blog, as well as a large multi-user web application, Acunetix Web Vulnerability Scanner was a bit slow. Because of connection differences, there is no point of mentioning specific timeframes in which the software was able to scan the systems, but the performance is directly connected to the complexity of the tests. I have set it up to check all the possible details on both scanning scenarios, so I expected a longer scanning period.

Acunetix Web Vulnerability Scanner offers its users real time reporting. For instance, when the software was in the middle of lenghty scan of a complex PHP web application scenario, I was able to check the issues that were already discovered.

Alert breakdown is done with four colors, each of the representing attack severity - red (high), orange (medium), blue (low) and green (information).



- Scan Thread 1 — Finished (341 alerts)
  - Alerts (341)
    - PHP version older than 4.4.1 (1)
    - Unfiltered Header Injection in Apach...
    - Cross Site Scripting (122)
    - SQL injection (104)
    - CRLF injection/HTTP response splitti...
    - File inclusion (3)
    - Directory traversal (Windows) (7)
      - /showimage.php
      - /showimage.php
      - /showimage.php
      - /showimage.php
      - /showimage.php
      - /showimage.php
      - /showimage.php
    - Script source code disclosure (1)
    - PHP code injection (3)
    - Blind SQL/XPath injection for numeri...
    - Blind SQL/XPath injection for string i...
    - Macromedia Dreamweaver Remote ...
    - Apache version older than 1.3.34 (1)
    - Apache Mod_Rewrite Off By One B

```
Server: Apache/1.3.33 (Win32) PHP/4.4.0
X-Powered-By: PHP/4.4.0
Connection: close
Content-Type: image/jpeg
```

[boot loader] timeout=30 default=multi(0)disk(0)rdisk(0)partition(1)\WINDOWS [operating systems] multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="Windows Server 2003, Enterprise" /fastdetect /NoExecute=OptOut

How to fix this vulnerability

Your script should filter metacharacters from user input.

Web references

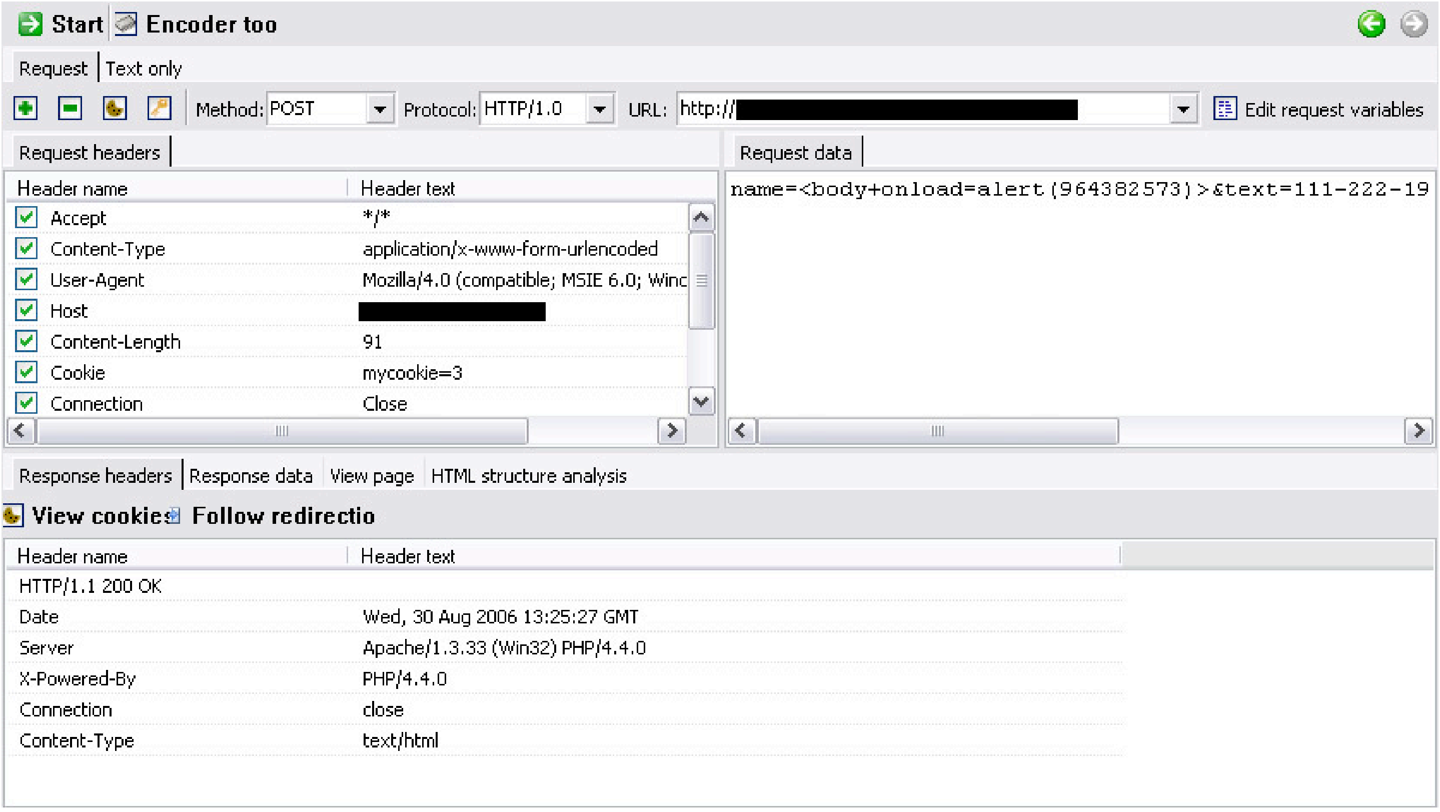
- Acunetix Directory Traversal Attacks
- Security Focus - Penetration Testing for Web Applications

Figure 3. The scan results.

The alerts are presented to the user in an easy to manage format: vulnerability type -> vulnerability item -> description. Under the vulnerability description, the most interesting thing is to check out attack details.

For every detected vulnerability, the user can see the actual HTTP headers that triggered the vulnerability as well as the HTML response given by the tested server.

Besides this, the software uses an innovative approach allowing the user to modify and replicate the same attack via a built-in HTTP Editor module. Within this GUI, users can craft specially structured attacks and analyze the server response.



Method: POST Protocol: HTTP/1.0 URL: http://[redacted]

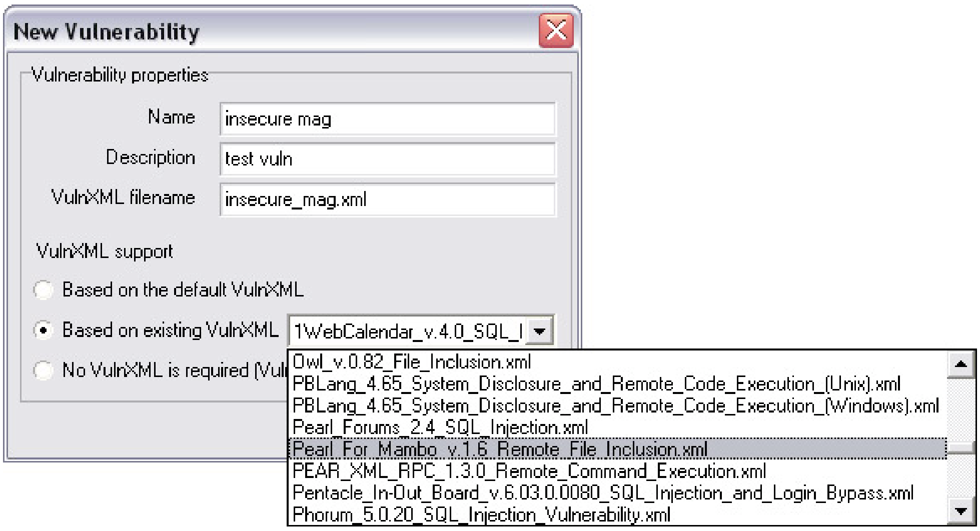
Header name	Header text
☑ Accept	*/*
☑ Content-Type	application/x-www-form-urlencoded
☑ User-Agent	Mozilla/4.0 (compatible; MSIE 6.0; Winc
☑ Host	[redacted]
☑ Content-Length	91
☑ Cookie	mycookie=3
☑ Connection	Close

```
name=<body+onload=alert(964382573)>&text=111-222-19
```

Header name	Header text
HTTP/1.1 200 OK	
Date	Wed, 30 Aug 2006 13:25:27 GMT
Server	Apache/1.3.33 (Win32) PHP/4.4.0
X-Powered-By	PHP/4.4.0
Connection	close
Content-Type	text/html

Figure 4. The HTTP Editor.

There is a slight bug with the attack launching that manifests in vulnerability items that are clearly not exploitable. For instance, inside a blue alert that says "Broken link", the user can try to launch this attack. There is obviously no attack related to this, but the software AI doesn't understand the difference. I didn't come across any other buggy issues with the software, so I thought about mentioning this one.



Name: insecure mag
Description: test vuln
VulnXML filename: insecure_mag.xml

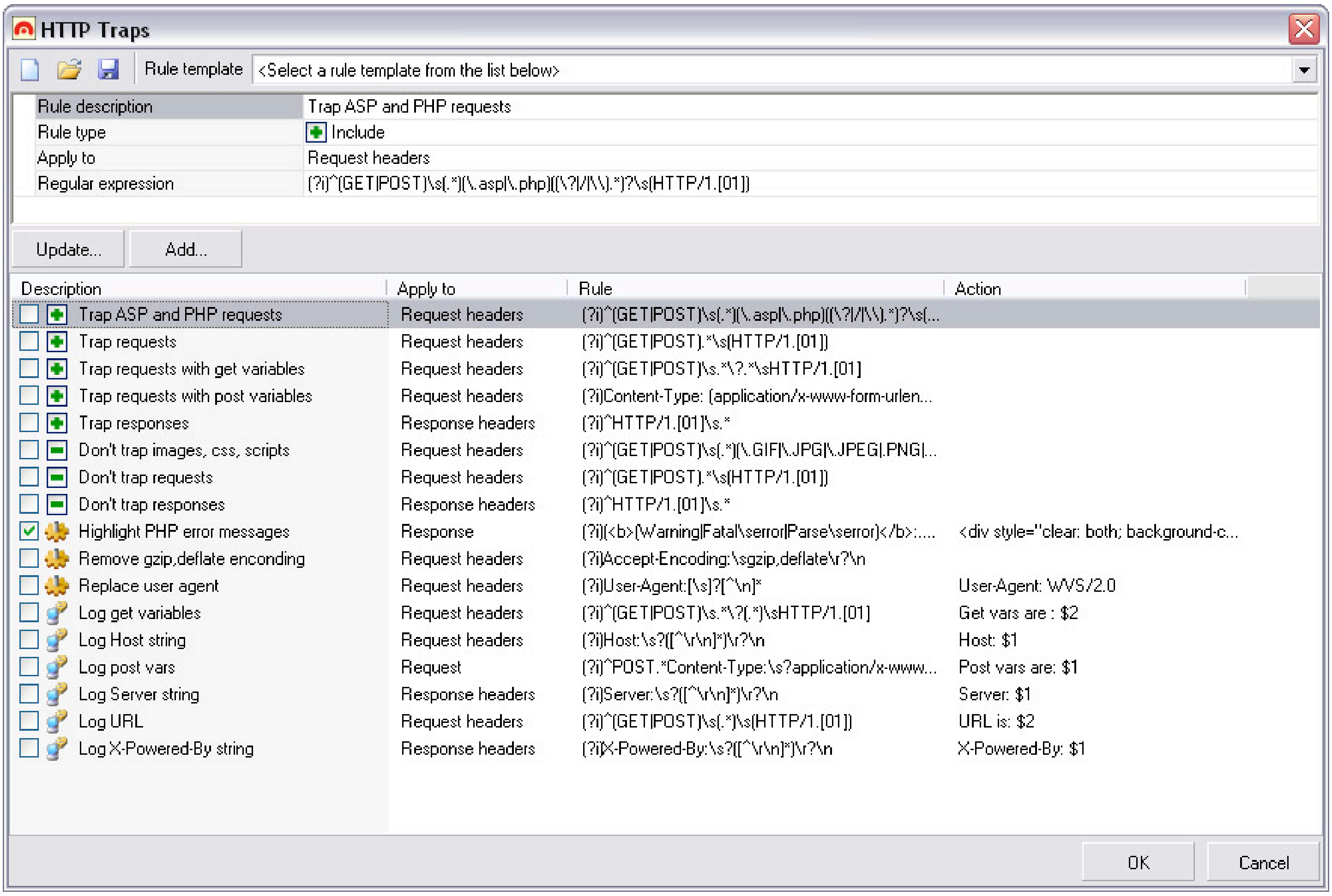
VulnXML support

○ Based on the default VulnXML
● Based on existing VulnXML 1WebCalendar_v.4.0_SQL_I
○ No VulnXML is required (Vul

Owl_v.0.82_File_Inclusion.xml
PBLang_4.65_System_Disclosure_and_Remote_Code_Execution_(Unix).xml
PBLang_4.65_System_Disclosure_and_Remote_Code_Execution_(Windows).xml
Pearl_Forums_2.4_SQL_Injection.xml
Pearl_For_Mambo_v.1.6_Remote_File_Inclusion.xml
PEAR_XML_RPC_1.3.0_Remote_Command_Execution.xml
Pentacle_In-Out_Board_v.6.03.0.0080_SQL_Injection_and_Login_Bypass.xml
Phorum_5.0.20_SQL_Injection_Vulnerability.xml

Figure 5. The vulnerability editor.

Advanced users will find the "Vulnerability Editor" option very interesting. There you can list and edit all the vulnerability types and specific items that Acunetix uses for scanning. I was really satisfied with the way how users can create new items by cloning existing vulnerability information. This way, users develop custom sets of vulnerability scanning actions that would be optimized for their servers, as well as manually update sections of the current vulnerabilities.



HTTP Traps

Rule template <Select a rule template from the list below>

Rule description	Trap ASP and PHP requests
Rule type	Include
Apply to	Request headers
Regular expression	(?i)^(GET|POST)\s(.*)(\.asp|\.php)((\?|/|\\).*)?\s(HTTP/1.[01])

Description	Apply to	Rule	Action
☐ Trap ASP and PHP requests	Request headers	(?i)^(GET|POST)\s(.*)(\.asp|\.php)((\?|/|\\).*)?\s(...	
☐ Trap requests	Request headers	(?i)^(GET|POST).*\s(HTTP/1.[01])	
☐ Trap requests with get variables	Request headers	(?i)^(GET|POST)\s.*\?.*\sHTTP/1.[01]	
☐ Trap requests with post variables	Request headers	(?i)Content-Type: (application/x-www-form-urlen...	
☐ Trap responses	Response headers	(?i)^HTTP/1.[01]\s.*	
☐ Don't trap images, css, scripts	Request headers	(?i)^(GET|POST)\s(.*)(\.GIF|\.JPG|\.JPEG|.PNG|...	
☐ Don't trap requests	Request headers	(?i)^(GET|POST).*\s(HTTP/1.[01])	
☐ Don't trap responses	Response headers	(?i)^HTTP/1.[01]\s.*	
☑ Highlight PHP error messages	Response	(?i)(<b>(Warning|Fatal\serror|Parse\serror)</b>:....	<div style="clear: both; background-c...
☐ Remove gzip,deflate enconding	Request headers	(?i)Accept-Encoding:\sgzip,deflate\r?\n	
☐ Replace user agent	Request headers	(?i)User-Agent:[\s]?[^\n]*	User-Agent: WVS/2.0
☐ Log get variables	Request headers	(?i)^(GET|POST)\s.*\?(.*)\sHTTP/1.[01]	Get vars are : $2
☐ Log Host string	Request headers	(?i)Host:\s?([^\r\n]*)\r?\n	Host: $1
☐ Log post vars	Request	(?i)^POST.*Content-Type:\s?application/x-www...	Post vars are: $1
☐ Log Server string	Response headers	(?i)Server:\s?([^\r\n]*)\r?\n	Server: $1
☐ Log URL	Request headers	(?i)^(GET|POST)\s(.*)\s(HTTP/1.[01])	URL is: $2
☐ Log X-Powered-By string	Response headers	(?i)X-Powered-By:\s?([^\r\n]*)\r?\n	X-Powered-By: $1

Figure 6. The HTTP sniffer in action.

Besides HTTP Editor, Acunetix Web Vulnerability Scanner offers a couple of other invaluable tools:

- With HTTP Sniffer users can create a custom set of traps that would be recorded in the sniffing period. By the way, by enabling the sniffing option, the software starts a proxy on port 8080.

- HTTP Fuzzer is a nice addition that is used for crafting specific requests and tracking the server's response. The option is especially worthy when used with one of the predefined number/character generators which append their output to the requests.

- The last tool I actively used inside Acunetix WVS is an Authentication Tester, a brute force module that can be configured for testing both HTTP and HTML form authentication methods.

The verdict

The bottom line is that Acunetix Web Vulnerability Scanner 4 is a powerful and versatile scanner that proves to be an important piece of a web application-testing arsenal.

As always with penetration testing, some things must be done manually, but from the perspective of an automated web vulnerability scanning procedure, you cannot miss with Acunetix WVS.

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

SSH port forwarding: security from two perspectives, part two

By Andrew J. Bennieston and Liam A. Fishwick

Part 1, published in issue 7 of (IN)SECURE, looked at the technicalities of port forwarding, covering local, remote and dynamic port forwarding. Part 2 looks at the security implications, and makes some recommendations for securing port-forwarding solutions on a network.

Policies and Configuration

This part of the article looks at firewall policies and SSH server configuration issues, in an attempt to secure a LAN (Local Area Network) whilst still allowing flexible port-forwarding solutions. At the end of the article is a table of port-forwarding related SSH client command-line options for quick-reference.

Firewall Policies For Inbound SSH

As SSH typically operates on port 22, the inbound filtering on a firewall should be set such that it allows packets to port 22 only on systems where there is a reason for external users to access SSH. For instance, if the company server runs SSH to allow roaming users to pick up their email on the road, access to that service should be allowed through the firewall. Access to arbitrary computers, on port 22, should be denied. This prevents a user running an sshd on their own computer with standard settings, and connecting in from a remote location.

Of course, the user could run an sshd on a different port; 2222 for instance. A well designed set of firewall rules will block inbound connection attempts to any port except those specifically allowed, and with destination addresses specific to the server machines running those services. In addition, if the firewall performs network address translation (NAT) then the firewall's IP address would be the only externally accessible address, and port 22 on the firewall would be forwarded to the internal SSH server. This solution, however, does not scale easily for multiple SSH servers.

Using the above policies, inbound SSH connections can be effectively limited to servers which may be locked down for security. Such server hardening is the topic of the next section.

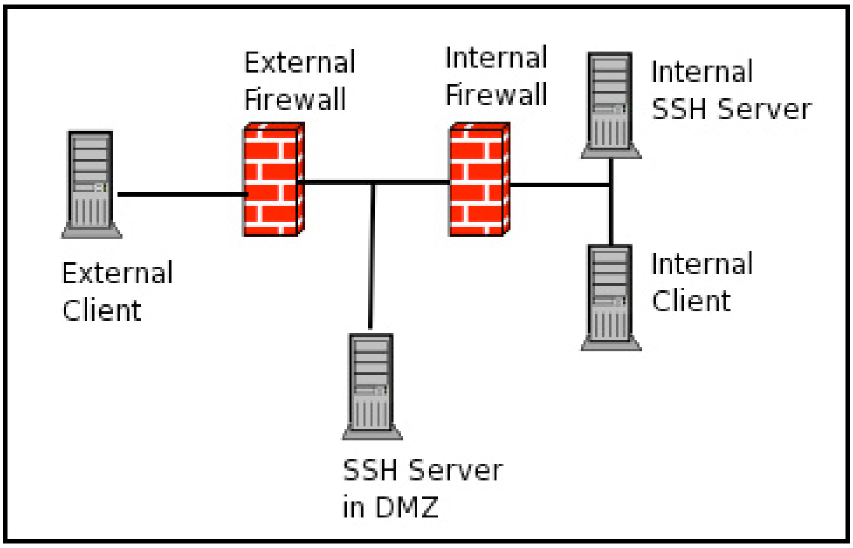
Internal SSH Server Configuration

Most SSH servers default to allowing port forwarding. Where there is no reasonable use for this feature, it should be disabled. This instantly protects against many of the possible circumventions of firewall rules or security policies.

Where port forwarding is required, or useful, two options exist to provide some extra security to this system. The first option is to reduce the number of users with accounts on this system to only those that need port forwarding capabilities. Users who only need shell access should be able to use a different `sshd`, which has had port forwarding disabled entirely. Reducing the number of users with access to the system reduces the number of users with the capability to subvert the security policy.

The `sshd config` keywords `AllowTcpForwarding`, `AllowTcpForwardingForUsers` and `AllowTcpForwardingForGroups` control TCP forwarding, and allow the server administrator to specify users and groups for which TCP port forwarding is allowed. When using public-key authentication, port forwarding may be turned off on a per-key basis by using the `~/.ssh/authorized_keys` file.

The second option is to put the server with port forwarding enabled into a more secure zone of the network, a DMZ (demilitarized zone), for instance, where there is a second firewall protecting the internal network, and allowing connections only to services specifically allowed. If you need to allow port forwarding to one or two well-defined services running on your LAN, this may well be a secure and practical solution (see Figure 1 below).



In the network example above, an external client may access the SSH server in the DMZ, with full port forwarding capabilities. The internal firewall only allows certain inbound connections to pass, however, and so the flexibility of the port forwarding is limited by the internal firewall. This allows secure solutions to retain some of the flexibility of port forwarding. Other security concerns exist with the use of SSH, and it is of course always recommended to change the default settings of an SSH server to increase the security. The use of public-key authentication, and increasing the verbosity of the logging (the `LogLevel` server configuration option) are important considerations in a secure environment. Lowering the time an `sshd` waits for login to complete is also useful on secure servers, as Denial of Service attacks could flood the server with connection requests and resources would be tied up until this time has passed and the connection is closed. The `LoginGraceTime` keyword is responsible for setting this time period.

Firewall Policies For Outbound SSH

In a perfectly secure environment, outbound SSH would be disabled entirely; it is not possible to guarantee the security of systems you do not have direct control over. In many environments, it is sufficient to allow outbound SSH only to certain addresses; remote office servers and other systems which are considered to be secure, and for which access is needed on a daily basis. For all other outbound SSH, one solution is to put an SSH server into the DMZ. This server would accept connections from only a limited number of users, and allow outbound SSH from that system to anywhere on the Internet. In this way, it is possible to restrict which users have such access in much the same way as discussed above for inbound SSH.

Outbound SSH Client Configuration

If your SSH client program allows port forwarding to be disabled at compile-time, and the users have no means of compiling or using their own SSH clients, using this feature would be a powerful way to restrict user port forwarding. You do, however, lose a lot of flexibility in this method. An administrator can no longer go to a user machine and use the same SSH client to perform activities which require port forwarding. This loss of flexibility is only worth the security gain in a highly secure environment. In all other cases, comprehensive firewall rules and SSH server configuration should suffice.

Option	Syntax	Comments
-L	-L lport:address:port	Local forwarding. Listen on lport and forward to address:port via encrypted channel.
-R	-L rport:address:port	Remote forwarding. Listen on remote server on rport and forward to address:port via encrypted channel.
-D	-D port	Dynamic port forwarding. Listen on local host on port, as a SOCKS5 proxy. The data is transmitted over the encrypted channel to the remote server, then on to its destination.
-g	-g -L lport:address:port -g -R rport:address:port	Gateway ports. Allow systems other than localhost to connect into a local or remote forwarded port.
+g	+g -L lport:address:port +g -R rport:address:port	No gateway ports. Prevent systems other than localhost from connecting into a local or remote forwarded port.

Keyword	Value	Comments
AllowTcpForwarding	Yes / No	Determines whether TCP port forwarding is allowed on a server-wide basis.
AllowTcpForwardingForUsers	List of allowed users	Lists the users which are allowed to use TCP port forwarding on this server.
AllowTcpForwardingForGroups	List of allowed groups	Lists the groups which are allowed to use TCP port forwarding on this server.
DenyTcpForwardingForUsers	List of denied users	Lists the users which are to be denied port forwarding access on this server.
DenyTcpForwardingForGroups	List of denied groups	Lists the groups which are to be denied port forwarding access on this server.

Andrew J. Bennieston contributes to leading computer security websites and forums. His writing efforts include articles, tutorials and book/software reviews. His skillset includes C/C++, PHP, Python and Linux administration. His personal website is located at http://stormhawk.coldblue.net.

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

"An informative insight into mobile security and the opportunity to speak to key people within the industry." CR, Icstis, Mobile Security 2005

12 Operator Case Studies

mobile security 2006

Combating Mobile Security Threats & Exploiting the Revenue Generating Potential of Pre-emptive Security Measures

3rd – 5th October 2006
Crowne Plaza, St James, London

Learn from the experience of12 Operator Case Studies to inform your mobile security strategy.

- **SWISSCOM,** Switzerland
- **VODAFONE,** UK
- **T-MOBILE,** International
- **ORANGE,** UK
- **o2,** Germany
- **BT,** UK
- **TELEFÓNICA MÓVILES,** Spain
- **TELIASONERA,** Finland
- **TMN,** Portugal
- **MOBILKOM,** Austria
- **VODACOM,** South Africa

Content Provider Presentation from **Universal Mobile Music**

M-commerce Case Study from **RaboBank**

Sponsored by
McAfee Proven Security™ ArcSight

THE WORLD'S MOST COMPREHENSIVE MOBILE SECURITY EVENT:

- □ **Learn** from **12 operator presentations** to inform your mobile security strategic planning
- □ **Develop** your understanding of how to **combat** current mobile security threats
- □ **Discover** the **revenue generating opportunities** mobile security presents through **M-commerce & DRM**
- □ **Gain** unrivalled insight into **Next Generation** mobile security
- □ **Understand** the impact of **regulation** on the mobile security business case
- □ **Network** with key figures in the mobile security industry to discuss the issues and **build strategic partnerships**

"Malware for smart phones is now evolving, and seems likely to become a growing threat as smart phones gain popularity." eWEEK.com

PRE-CONFERENCE WORKSHOP

2nd October 2006

Effectively Securing Premium Content through Interoperable DRM: Examining in Detail the Latest DRM Technologies, Trends and Strategies

Led by: CoreMedia

Produced by:
informa
telecoms & media

To register please visit www.informatm.com/security or call +44 (0) 20 7017 4202 or email Emma.Abrahamson@informa.com Please quote (IN) Secure to claim a 10% discount.

www.informatm.com

informa
telecoms & media

WINDOWS - Eraser
http://www.net-security.org/software.php?id=155

Eraser is a secure data removal tool for Windows. It completely removes sensitive data from your hard drive by overwriting it several times with carefully selected patterns.

LINUX - strongSwan
http://www.net-security.org/software.php?id=643

strongSwan is a complete IPsec and IKEv1 implementation for Linux 2.4 and 2.6 kernels. It interoperates with most other IPsec-based VPN products.

MAC OS X - Password Gorilla
http://www.net-security.org/software.php?id=661

Password Gorilla helps you manage your logins. It stores all your user names and passwords, along with login information and other notes, in a securely encrypted file. A single "master password" is used to protect the file.

POCKET PC - eWallet
http://www.net-security.org/software.php?id=553

Have your most important personal information backed up for safekeeping, encrypted and password-protected for security, but right with you when you want it. Plus, you can enter your information on your Windows PC and synchronize it with your handheld.

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

Log management in PCI compliance

By Dr. Anton Chuvakin

Security professionals have come to realize that ensuring data security and integrity is critical to business continuity and risk mitigation. However, with increasing amounts of data flooding our ever more complex networks, the risk of stolen or lost - with you unable to prove that it was not stolen - information continues to rise.

Online merchant networks are particularly at risk from both classic computer attacks and more insidious fraud. At the same time, the more customer data is collected, the more dangerous the situation becomes. In response to this trend and to prodding from major credit card companies, new security measures are being implemented by merchants and other businesses to protect the data their customers trust them with (or don't even know they have…).

Today, all credit card merchants, service providers and retailers who process, store and transmit cardholder data have a responsibility to protect that data and must comply with a diverse range of regulations and industry mandates as well as a growing list of voluntary "best practices" frameworks. These include the venerous Sarbanes-Oxley bill (better known as SOX or SarbOx), the Payment Card Industry (PCI) data security standard, the Gramm-Leach-Bliley Act of 1999 and even HIPAA (healthcare providers take credit cards too!). Not complying with the above might result in fines, legal exposure, or both, although it is widely known that the regulation differ wildly in regards to their "teeth." For instance, it was reported that nobody was ever fined for being out of compliance with HIPAA.

But this is easier said than done. Immense volumes of log data are being generated on such payment networks, necessitating more efficient ways of managing, storing and searching through log data, both reactively – after a suspected incident – and proactively – in search of potential risks. For example, a typical retailer generates hundreds of thousands of log messages per day amounting to many terabytes per year. An online merchant can generate upwards of 500,000 log messages every day. One of America's largest retailers has more than 60 terabytes of log data on their systems at any given time. At the same time, unlike other companies, the retailed often have no option of not caring for logging.

The importance of effective and efficient log data management in payment networks cannot be underemphasized. In fact, the result of data mismanagement can be devastating. Retail Ventures Inc., for example, lost personal customer information from 108 stores in its DSW Shoe Warehouse subsidiary, an incident that involved 1.4 million credit cards used to make purchases. The lost data consisted of account numbers, names, and transaction amounts. Similarly, CardSystems was sued in a series of class action cases alleging it failed to adequately protect the personal information of 40 million consumers. At an individual cost of $30 per consumer the costs of repairing the damage could be as high as $1.2 billion. What is interesting is that in a latter case, only a smaller number of cards was "confirmed stolen", while the rest were not "confirmed safe," since there were no logs to prove that they were not.

Addressing PCI not only protects businesses and merchants from cardholder fraud, but also satisfies a broader mandate for information protection and security. Several retailed stated that complying with PCI makes them automatically compliance with SOX, due to more stringent and more specific requirements described in the PCI standard. Additional benefits include improved operational efficiencies through broad compliance (even likely with future regulations!), reduced IT administration and maintenance costs, reduced IT labor costs and greater IT productivity. At the same time, some see complying with PCI as another compliance burden for companies, especially if IT resources are limited and focused on a day-to-day grind of "firefighting." To cost-effectively and efficiently comply with PCI, companies should look at log management and intelligence (LMI) solutions to simplify the process of collecting, storing and managing log data to both satisfy the reporting and monitoring requirements, audit log collection requirements as well as enable better incident response and forensics.

Addressing PCI not only protects businesses and merchants from cardholder fraud, but also satisfies a broader mandate for information protection and security.

PCI Compliance Combats Fraud and Improves Security

In most cases, when a customer clicks the "buy" button on a web site, a number of things happen on the backend. An application server connects to a database, multiple records are updated and sometimes a connection to a separate payment application is initiated.

All those activities generate log files in various places: on the servers, applications, databases as well as on network and security infrastructure components.

At the same time, the attackers know that there might be vulnerabilities in these processes and technologies that leave data unprotected. Internal threats such as insider misuse are of even greater concern in this case, since there are no perimeter defenses stopping such attackers.

According to recent FBI survey, financial fraud is the second-largest category of hacking events on the Internet today. Similarly, Gartner estimates that 20-30% of Global 1000 companies suffer losses due to mismanagement of private and confidential information.

The costs to recover from these mistakes could reach up to $5-20 million per company, as it happened in a few recent cases affecting both commercial and government entities.

PCI Requirements Center on Security and Authorized Access

Complying with PCI, merchants and service providers not only meet their obligations to the payment system but create a culture of security that benefits everyone, including the top executives.

The security requirements of PCI extend to all system components that are connected to the cardholder data environment:

• Network components: firewalls, switches, routers, intrusion prevention and detection systems, proxies and content filters, wireless access points as well as other network and security appliances
• Servers: web, database, authentication, domain name service (DNS), mail, network time protocol (NTP), directory and others
• Applications: all purchased and custom apps, internally and externally facing web applications, Intanet applications, etc

What is even more important is that companies must be able to verify and demonstrate their compliance status and to do so rapidly, whenever an audit takes place. Such proof of compliance is a fundamental and critical function that identifies and corrects potential pitfalls in the network, and ensures that appropriate levels of cardholder information security are maintained.

PCI requirements revolve around the following goals:

• Build and maintain a secure network
• Protect cardholder data in transit and at rest
• Maintain a vulnerability management program
• Implement strong access control measures and audit them on a regular basis
• Continuously monitor networks and systems
• Maintain an information security policy
* Maintain audit trails of all of the above activities

Log data plays a central role in meeting several of these goals. Specifically, without log data, companies cannot verify and audit access controls, other security safeguards and policies or even monitor their networks and systems as well as conduct incident response activities.

The PCI specification highlights the necessity of log data collection and management for meeting the key requirements. For example, Requirement 10 specifies that companies should “track and monitor all access to network resources and cardholder data.” The requirement specifies that companies “implement automated audit trails to reconstruct events for all system components.” These events include user access, actions taken, invalid logical access attempts, use of identification and authentication mechanisms, initialization of audit logs and creation or deletion of system-level objects. It also recommends recording audit trail entries for each event, including user ID, type of event, date and time, success or failure, origination of event, and the identity of the affected data or component.

The PCI standard goes on to say that companies should “review logs for all system components at least daily,” and the review should include servers that handle intrusion detection, authentication, authorization and accounting.

The interesting thing is that, in the mind of many retailers, “review logs daily” does not mean that a person would be poring through the logs every single day. An automated system can do this just as well, and in fact better. In case of such “automated review,” alerts would be generated in case traces of malicious, suspicious or fraudulent activity are seen in logs. At the same time, a human analyst might review reports and alerts that highlight such activity as needed.

In addition, PCI specifies that “an audit trail should be retained for a period consistent with its effective use, as well as legal regulations,” and that the “audit history usually covers a period of a t least one year, with a minimum of 3 months available online.” Thus there are also log data retention (and the corresponding log data destruction requirements!) requirements.

One should not that log data is implicitly present in many other PCI requirements, not only the directly relevant Requirement 10. For instance, just about every claim that is made to satisfy the requirements, such as data encryption or anti-virus updates, requires log files to actually substantiate it. So, even the requirement to “use and regularly update anti-virus software” will likely generate requires for log data during the audit, since the information is present in anti-virus audit logs.

It is also well-known that failed anti-virus updates, also reflected in logs, expose the company the malware risks, since anti-virus without the latest signature updates only creates a false sense of security and undermine the compliance effort.

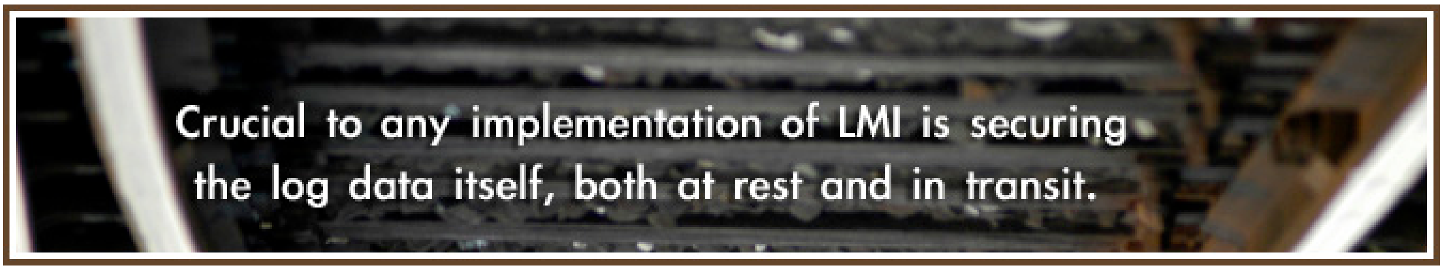
Similarly, the requirement to “establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations” is unthinkable to satisfy without effective collection and timely review of log data.

Thus, logs value to PCI program goes much beyond Requirement 10. Only through careful log data collection and management can companies meet the broad requirements of PCI. Such detailed log data management requires embedded intelligence in the log management solution to make the data secure, accessible and easy to organize and to automate many of the required tasks, such as monitoring, analysis and retention.

LMI for PCI Compliance

A comprehensive LMI solution that can collect, aggregate and centrally store all data from these network entities is essential to meet the goals of the PCI standard. LMI enables satisfying the audit, monitoring, data protection, log data collection and retention, identity access and change management cited in PCI requirement documents.

Let’s look at some of the above requirements in more detail.



Crucial to any implementation of LMI is securing the log data itself, both at rest and in transit.

Data Protection

To provide the necessary data protection measures, companies should implement an LMI solution that enables administrators to set alerts on and report on all applications, devices, and systems.

This enables them to provide evidence that infrastructure has been configured properly and are misconfigured systems are not providing a backdoor for intruders – or a front door to insiders through which vital information can leak.

Alerts can provide administrators with early warning of misuse and attacks, allowing them to isolate and fix the problem before damage occurs or data is lost. And, of various data access policies and processes not being followed.

Crucial to any implementation of LMI is securing the log data itself, both at rest and in transit. This not only serves to reduce the risk of this vital information leaking, but also prevents it from being altered or lost thereby reducing its relevance, immutability and forensic quality.

Identity access and change management

Access and change management are critical to meeting PCI compliance as well as other regulations and IT governance frameworks, such as ITIL, COBIT or ISO. Strong access and change control measures ensure that only authorized users can access or take action on critical data.

The PCI standard mandates that companies maintain a complete record of access (both failed and successful), activity, and configuration changes for applications, servers and network devices. Such log data allows IT to set up alerts to unusual or suspicious network behavior and provide information to auditors with complete and accurate validation of security policy enforcement and segregation of duties.

LMI allows administrators to monitor who has permission to access or make changes to devices and applications in the network. It also enables administrators to create a complete audit trail across devices and protect network resources from unauthorized access or modifications.

An effective LMI solution will support centralized, automated storage of collected data allows for faster, more reliable data retrieval during an audit or while investigating suspicious behavior.

Network and System Monitoring

PCI compliance necessitates ongoing monitoring of network activity to validate that processes and policies for security, change and access management, and user validation are in place and up to date.

Logging and monitoring allow for fast problem isolation and thorough analysis when something goes or is about to go wrong. With the automated monitoring capabilities delivered by an LMI solution, companies can better mitigate risk and reduce downtime, because they can address data critical for problem resolution and threat mitigation rapidly, before damage spreads. Ongoing and automated monitoring gives administrators greater insight into the payment network at all times so that unusual user activity, unauthorized access or even risky insider behavior can be identified—and stopped—immediately.

Components of an Effective LMI Solution

To use log data to unleash its full value for compliance, operations excellency and security, companies should implement a log management solution that provides the following critical capabilities:

- Collection and aggregation 100% of all log data from enterprise data sources including firewalls, VPN concentrators, web proxies, IDS systems, email servers and all of the other systems and applications mentioned in the PCI standard.
- Creation of reports that organize the log data quickly and automatically, so that administrators can deliver detailed network activity information and proof of compliance to auditors.
- Setting of alerts based on changes to individual devices, groups of devices or the network, to minimize network downtime and loss of data due to malicious attacks, security breeches, insider misuse or performance issues.
- Fast data retrieval from securely stored, unaltered raw log files. Immutable logs are critical in litigation and attestation.
- Integration with existing network management and security solutions to reduce maintenance and administration and leverage existing architecture.
- The ability to contextualize log data (comparing application, network and database logs) when undertaking forensics and other operational tasks.

By now the reader should be convinced that it is impossible to comply with PCI requirements without log data management processes and technologies in place.

Complete log data is needed to prove that security, change management, access control and other required processes and policies are in use, up to date and are being adhered to. In addition, when managed well, log data can protect companies when legal issues arise; for example, when processes and procedures are in question or when a discovery process is initiated as a part of an ongoing investigation.

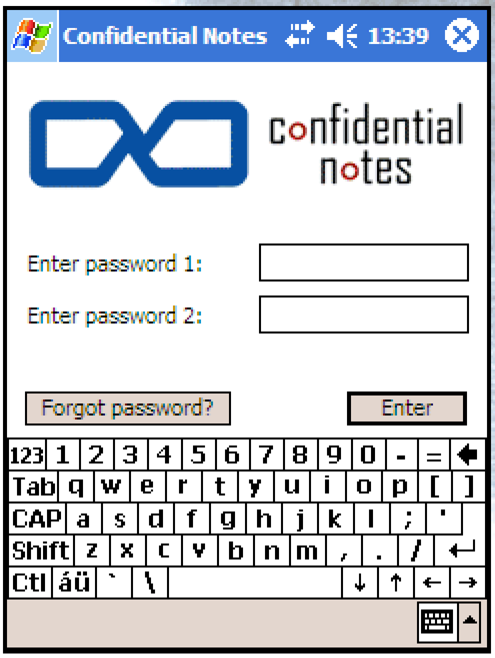
Not only does log data enable compliance, but it allows companies to prove that they are implementing and continuously monitoring the processes outlined by the requirements. In fact, that is the ONLY way to prove it!

Dr. Anton Chuvakin, GCIA, GCIH, GCFA (www.chuvakin.org) is a recognized security expert and book author. A frequent conference speaker, he also represents the company at various security meetings and standard organizations. He is an author of a book "Security Warrior" and a contributor to "Know Your Enemy II", "Information Security Management Handbook" and the "Hacker's Challenge 3".

Anton also published numerous papers on a broad range of security subjects, such as incident response, intrusion detection, honeypots and log analysis. In his spare time he maintains his security portal www.info-secure.org and several blogs.

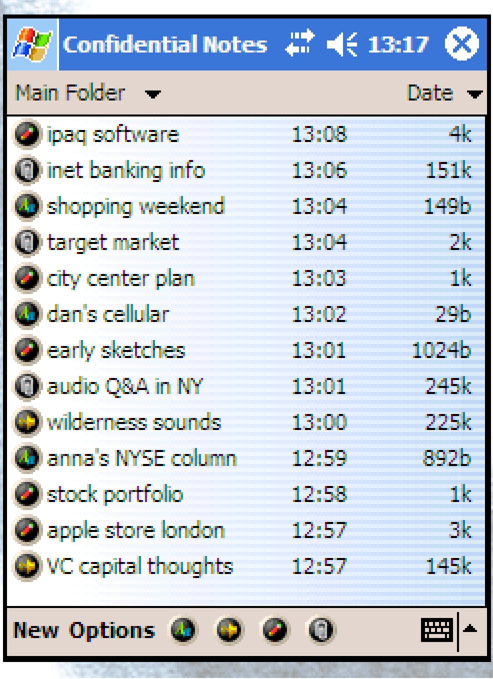
Confidential Notes is a practical and easy to use solution that instantly provides you with a high level of security for your mobile data.

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

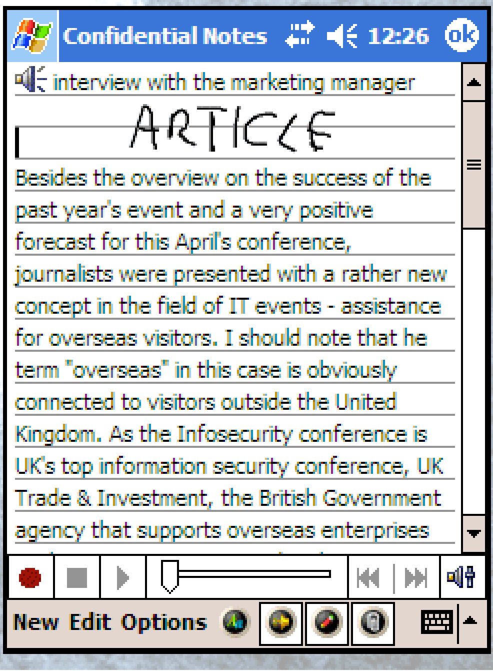


Enter password 1:

Enter password 2:



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



interview with the marketing manager

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 he 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

Airscanner vulnerability summary: Windows Mobile security software fails the test

By Seth Fogie

Microsoft claims that the Windows Mobile operating system is secure enough for the enterprise. That's not quite true, since unlike Windows XP, handhelds don't have advanced security architecture. For example, Pocket PC has no Kerberos authentication, Encrypting Filesystem, or a built-in firewall. In fact, even the much-touted Mobile2Mobile "secure" signing process for .DLLs and .exes can be bypassed with a simple buffer overflow, thus potentially allowing malware to take over your device.

However, once you understand limitations, you can then plan your Windows Mobile rollout more carefully. Fortunately, there is a great deal of 3rd party security software out there. Unfortunately, much of it is completely insecure. Sadly, Windows Mobile developers have not yet been held up to the same scrutiny as desktop software developers. For instance, you may think your 'encrypted' or 'secure' data is safe on a Pocket PC because the vendor stated as much, when in reality the data is insecure.

In this paper, we expose some weaknesses in 3rd-party security software for Pocket PC. Note that we are not assigning blame to any of the developers; in fact, some of them responded quickly and were eager to get feedback and to fix the bugs. On the other hand, some were angry, threatening, and even dismissive. For us, it doesn't matter if software has bugs. All software has flaws; that's why you should always use "layered" security. It is the responsiveness of a developer, and their willingness to fix the product, that helps us define a quality developer.

This is not an attempt to criticize any vendors. We selected the target applications at random using the search engines provided by reseller websites. We are also not disparaging the Windows Mobile platform. In fact, we love it and use it every day. We simply want to make it stronger, and more secure. And by raising user awareness, perhaps more people will pay more attention to how their data is stored. The principle of "security through obscurity" has long been a discredit.

Background

According to the 2005 Pointsec Mobile Usage Survey, an estimated 22% of PDA owners have lost their devices. Combine this with the statistic that 81% of those lost devices had no protection (e.g. PIN or encryption), and the problem just got worse. Yet the same survey indicates that 37% of PDAs have sensitive information on them, such as passwords, bank account information, corporate data and more.

If you think PDA security isn't a real subject, just consider the possibility that there is someone out there right now with your name, email, phone number, and birth date and more stored on a digital device that was just left in a taxi cab – not a comforting thought.

Thankfully, a security conscious person can find, download, and install a plethora of software that will help them remain productive, yet keep their data secure inside an encrypted file in the event the device is lost or stolen. On the surface, these programs are an excellent idea.

Financial information, passwords, credit card numbers, and even project files can all be locked up and secured. In addition, passwords that are entered into the PDA for service oriented programs (e.g. remote access, email, chat, etc.) are protected from prying eyes using masking techniques so an attacker can learn that information. Unfortunately, as we discovered, more often than not the security mechanisms are nothing but an illusion at worst, or terribly flawed at best. The end result is that the user is placing their trust in a broken program that is insecure. This paper will address many of the issues we found and what you can look for when investigating the quality of your 'secure' program.

THERE ARE NUMEROUS WINDOWS MOBILE VENDORS THAT STORE SENSITIVE INFORMATION IN THE REGISTRY WITH FLAWED ENCRYPTION SCHEMES, OR EVEN IN PLAINTEXT! IF THE END USER KNEW ANYONE COULD SEE THIS DATA, WHAT WOULD THEY SAY?

The Windows Mobile Obfuscation Shell

Before we examine the details of the flaws, it is important to understand the nature of the operating system. The reason for this is because it is our belief that Windows Mobile platform creates an environment conducive to poorly designed security software.

In contrast, if there is a problem on the Windows XP (desktop) operating system, it is fairly easy for you to find out what is happening. For starters, a Ctrl-Alt-Del will allow you access to an informative Windows Task Manager that provides all sorts of information about the programs running on the computer. In addition, it is simple to find out what is configured to run at startup via the 'msconfig' command. Next, you can look inside the registry with 'regedit' or use the command line to quickly access and view files. And if this isn't enough, there are many free tools available that can expose almost anything about the operating system to its owner. All in all, thanks to certain tools, Windows XP is a fairly open operating system.

Now, what kind of details can you find out on the Windows Mobile 5 platform? For starters, the Task List only mentions the names of the open applications that have graphical interfaces. All others are not listed! How can a user find out if there is a hidden program that is eating up memory? Is there a way to find out what executes when the device is rebooted? Not for the average user.

In fact, the only way a user can examine what is occurring behind the scenes is via the Visual Studio 2005 program that runs on a desktop system – and only if the PDA is synced up to that same system. There are some third party programs that give access to some of this data, but these are not free or as informative as Visual Studio.

The point is this – average Windows Mobile users are relatively blind about what their device is doing. As this paper will illustrate, there are numerous Windows Mobile vendors that store sensitive information in the registry with flawed encryption schemes, or even in plaintext! If the end user knew anyone could see this data, what would they say?

History has taught the security community that software vendors will not code secure software unless forced to do so by consumers. The Pocket PC software market is a prime example of this ‘law’, which is why Airscanner performed this research. No more excuses…

The rest of this paper will be examining many different programs and their flaws. As you will see, blindly trusting a software vendor to keep you data safe is very risky. We hope that our research will help convince you to thoroughly research a product before relying on it to keep you secure.

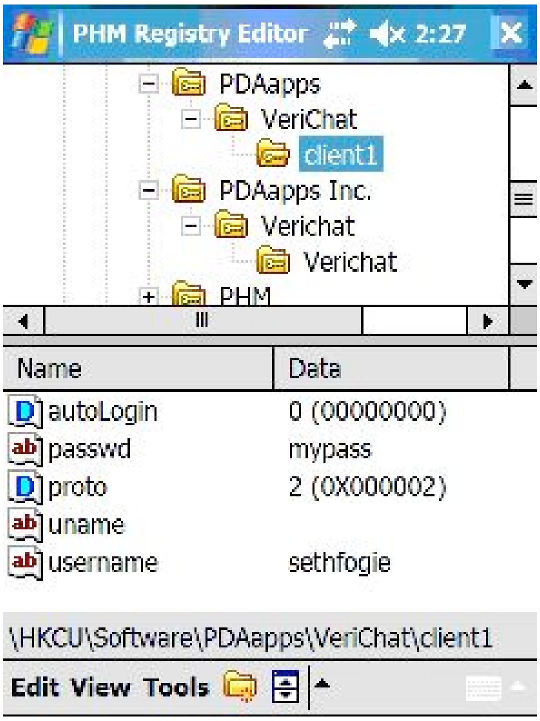
Protecting the Passwords

When you use a program that requires a password, you assume it will be kept secure. This assumption is dangerous, especially on a Windows Mobile device. Typically, third party passwords are not encrypted. If they are, then it is a fairly simple matter to crack many of the encryption methods, thus exposing the original value. In this section we will highlight how you can find these passwords, with numerous examples to prove the point.

There are several tools that will assist in your registry viewing. The first is the registry viewer included with Visual Studio. This program is not free, but you can obtain a 120 day trial version from Microsoft’s website. To augment this program, we also used an internal (Airscanner) tool that dumps the entire registry, and a free program called PHM Registry Editor (phm.lu/Products/PocketPC/RegEdit/).

Plaintext Passwords

The first group of examples stores the user account information in plaintext right under their registry key in the HKLM\Software or HKCU\Software branch. Figure 1 illustrates how a program called Verichat stores your user information.



Name	Data
autoLogin	0 (00000000)
passwd	mypass
proto	2 (0X000002)
uname	
username	sethfogie

\HKCU\Software\PDAapps\VeriChat\client1

Figure 1: VeriChat User/Pass storage

If you note, both the username and password are very simple to read.

The following is a list of programs that were examined and found to have similar issues. Some store the information in the registry, and others simply keep it hidden in a configuration file.

- Verichat – Chat program
  - HKCU\Software\PDAapps\VeriChat\client#
- IM+PPC – Chat program
  - \Program Files\IMPlus\implus.cfg
- Agile – Chat program
  - \HKCU\Software\AgileMessenger
- MSN Messenger Force
- Imov Messenger – Chat program (Enterprise version is encrypted)
- File Transfer Anywhere – File transfer program
  - \HKLM\Software\TTXN\File Transfer Anywhere
- NeoFTP – FTP client
  - \Program Files\neoFTP\FTP_Hosts.lst
- Thunderhawk – Web browser
  - thconfig.txt
- RemoteKeyboard – PC to PDA keyboard
  - \HKCU\Software\TransCreative\RemoteKeyboard\PassCode

The above list represents those products that do not protect the user information. The key thing to realize is if someone was able to gain access to a PDA for even a few seconds, the listed registry entries could be quickly viewed or copied out to an external memory card.

Password Exposure Bugs

To help protect against such easy attacks, some programs do encrypt the user information. Unfortunately, these protections are sometimes flawed, which results in exposed account information. This can occur either through a software bug, or by implementing a weak/flawed proprietary method of encryption. The following illustrates a few examples.

BullGuard Antivirus

BullGuard is an antivirus program that requires a valid account to update the virus database. Each time the update occurs, the AV software sends the email address and password used to register the software via an encrypted channel to their server. This protects that information during transmission. Unfortunately, a weak encryption scheme is used to protect that password that is stored on the local device.

In addition to being able to decrypt existing passwords, we discovered that certain passwords are 'shortened' thanks to a flawed encryption algorithm. Figure 2 illustrates this bug. The highlighted data is where the encrypted password of 'ssssssss' should be posted. Note that there is nothing between the semicolon and the 0x0D and 0x0A. As you can see, the password is basically blank! Unfortunately, this represents just one of many such defunct passwords that could be selected.

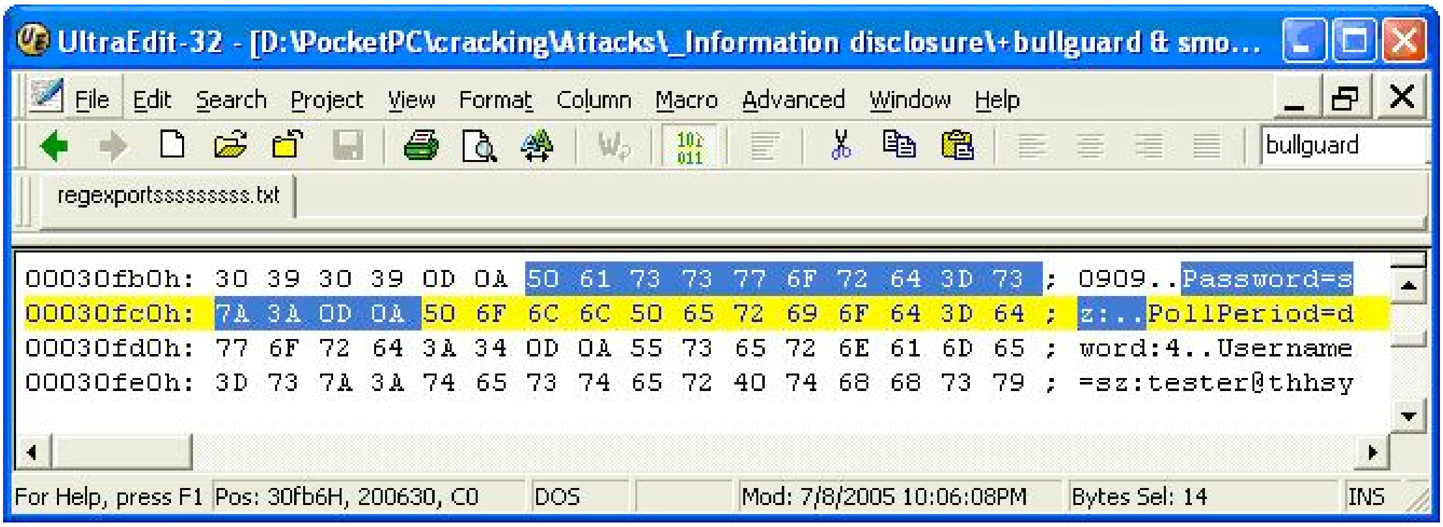
Although not related to password storage, it is important to note BullGuard stores its virus pattern matching information in a plaintext file that lists the virus and its pattern. For example, the following is the entry for the WinCE Duts virus.

```
WinCE-Duts.A(frk)=04001be50fe0a0e128f01b
e508001be50fe0a0e128f01be53380bde85468
6973
```

The reason this is a bad idea is because a malicious program can simply patch the virus definition file with an incorrect value, thus ensuring it won't be considered a virus. Secondly, BullGuard includes an auto delete function that could become an attack tool if malicious program inserted a pattern that matched all executable and dll files on the PPC (i.e. ReallyBadVirus=4d5a9000).

Abidia and OAnywhere

The mobile device is an excellent tool for remotely monitoring services. In the case of Abidia and OAnywhere, this service is eBay.com and Overstock.com account monitoring.


UltraEdit-32 - [D:\PocketPC\cracking\Attacks_Information disclosure\+bullguard & smo...
File Edit Search Project View Format Column Macro Advanced Window Help
bullguard
regexportsssssssss.txt
For Help, press F1
Pos: 30fb6H, 200630, C0
DOS
Mod: 7/8/2005 10:06:08PM
Bytes Sel: 14
INS

```
00030fb0h: 30 39 30 39 0D 0A 50 61 73 73 77 6F 72 64 3D 73 ; 0909..Password=s
00030fc0h: 7A 3A 0D 0A 50 6F 6C 6C 50 65 72 69 6F 64 3D 64 ; z:..PollPeriod=d
00030fd0h: 77 6F 72 64 3A 34 0D 0A 55 73 65 72 6E 61 6D 65 ; word:4..Username
00030fe0h: 3D 73 7A 3A 74 65 73 74 65 72 40 74 68 68 73 79 ; =sz:tester@thhsy
```

Figure 2: Bullguard Registry Entry

Once the PDA software is installed and configured, the application will poll the online auction websites for updates on items selling, buying, etc. The dangers for this type of program are three fold. First, the user account information must be securely stored on the device. Second, if the program ever has to handle the sensitive data, then it must be able to ensure the confidentiality of that information during program execution. Third, the program must securely transmit the data to the service provider.

In the case of Abidia, the user information is stored in an XML file in the program directory. Fortunately, the eBay account data is encrypted (e.g. ebaypass="2F6DD0EEDA61 68A7FE2A3AC47436A8720399FB4797D E422E"). After reviewing the encryption scheme, we determined that it appeared to be secure enough given the time involved to crack it. However, during this investigation, we discovered that the executable file itself could be used to decrypt the password. As previously mentioned, if a program stores a password it must maintain the confidentiality of the data at all times. In the case of Abidia, it was fairly simple to follow the execution path and hook into the program after it decrypted the password, which we then were able to display on the PDA's screen.

Finally, we examined the data communication process to ensure the user account information was securely transmitted. We discovered that the program interacts with an API interface on Abidia's servers, which serves as a proxy to eBay. The following is an actual capture of the plaintext HTTP POST request send from our Windows Mobile device.

```
POST
/api/get.php?user=sethfogie&pass=mypassword&serial=&imei=22363230F8403111
1800%2D0050BFE45CE5&site=US&dbg=y&name=buy HTTP/1.1
Host: api.abidia.com
User-Agent: Abidia-Wireless/2.5.3 (PocketPC; 240x320; WindowsMobile/5.1.70)
Accept: text/html
Content-Language: en-US
Connection: Close
Content-Length: 93
Content-type: application/x-www-form-urlencode
```

In case you missed it, take a close look at the POST string. Abidia does not encrypt the user or password. Since this was all performed over a regular HTTP session, anyone in the data transmission path (including Abidia) can capture the account information.

It is dangerous enough to trust a third party company with user account information, but the fact the username and password are sent as plaintext is very insecure; particularly if you are using a wireless connection and/or a public hotspot.

Windows Mobile WEP Key

The Odyssey client included with the original (WM2003) Dell X50v stores the WEP keys as an encrypted strings in the registry. When the network connection is made to the secure network, the driver pulls these values from the registry, decrypts them, and then incorporates the key into the communication process. However, during this process, the driver writes the decrypted value back into the registry. The problem is not Odyssey's, as that program does encrypt the key, but is instead a flaw in how all three (Windows Mobile, Dell wireless driver, Odyssey) work together.

The following illustrates: Byte 5 - 9 list my entered WEP keys for each entry.
KEY1=aabbccddee

```
"HTCWEPDefaultKey1"=hex:
01,00,00,00,aa,bb,cc,dd,ee,8c,f6,36,1d,af,90,
17,5b,00,f6,36,1d,af,00,00,00...
```

After we notified the vendors, this problem has been fixed in current versions of Windows Mobile and there is a ROM update that will correct the problem for the Dell Axim X50v.

PocketMoney

According to the website, "PocketMoney is the most robust financial management tool for the Pocket PC." With it, you can "Store the institution, phone, account number, expiration date, limit, fee for each account. Now you can even password protect your PocketMoney data from prying eyes!"

To keep the information safe, PocketMoney requires a user to enter a password before opening its data file. An 'encrypted' version of the password is stored in the registry at the HKLM\SOFTWARE\Handmark\PocketMoney\Password key. Unfortunately, the password is protected via a ROT-N function using the following seed value:

0x21 0x70 0x6d 0x6f 0x6e 0x65 0x79 0x21 ⇒

NAK p m o n e y NAK.

In other words, the protection of the password (and the financial data) is tied directly to the word 'pmoney' (sound familiar?). Despite the key selection, a ROT-N scheme is always a bad idea because it is trivial to do a pattern analysis on the encrypted data and deduce the key.

In this section we looked at several examples of how not to protect user account information. Unfortunately, this problem is wide spread through out Windows Mobile programs. Be sure you understand the dangers associated with trusting a program to keep your user account information secure, and always use unique passwords.

Data Protection Programs

This next section takes a look at programs that implement password protection schemes that are meant to keep data secure. Unlike the previous section that focused only on user account information, this section targets programs that were designed to store sensitive data such as banking transactions, stock information, credit card numbers, and lists of passwords. In this case, an attacker would have access to a much larger chunk of sensitive data that the user is assuming is secure.

Financial Management Programs

This section addresses a common problem that exists in numerous 'secure' programs. Although some programs obscure the issue, all of the following titles can all have their security mechanisms bypassed by a small change in the registry. Note how some companies try to hide this fact by placing the registry key in unusual locations, or by burying the flag inside a large registry string.

It should also be mentioned that a malicious user can often just copy the 'protected' data file off the target device and onto a device that has no protection enabled. Since the data itself is not truly protected, an alternate device will be able to open it without the need of a password.

PocketKeeper

PocketKeeper is program to manage daily out-of-pocket expenses with multiple accounts different currencies, intuitive register, customizable categories, budget, multiple report charts, and password protection. It has two levels of security – a global level that restricts access to the program, and an account level that secures each account.

Upon reviewing the files associated with this program, it was discovered that both passwords are stored as plaintext in the .dat files of the program directory. Specifically, the global password is stored in config.dat and each account password is stored in its relative account file.

PocketMoney

PocketMoney not only uses a weak encryption scheme to protect the password (discussed in previous section), but the protection scheme itself can be easily disabled by setting the following key in the registry to a 0.

HKLM\SOFTWARE\Handmark\PocketMoney\Active Password = 0

In response to this issue, PocketMoney's vendor rather alarmingly states, “The password in PocketMoney wasn't designed to encrypt data or prevent anyone other than a casual browser from being able to access the data. I suggest the user turn on the Palm's (sic) password protection if they want their palm (sic) secure.” We, the users, beg to differ!

WebIS Money

WebIS Money states it includes “…secure password protection to your data to safeguard it in case your PDA is lost or stolen.” Unfortunately, this protection can be disabled by removing the following key from the registry.

HKLM\SOFTWARE\Microsoft\Pim\Outlook\I-MAP Folders\H11

MoneyTracer

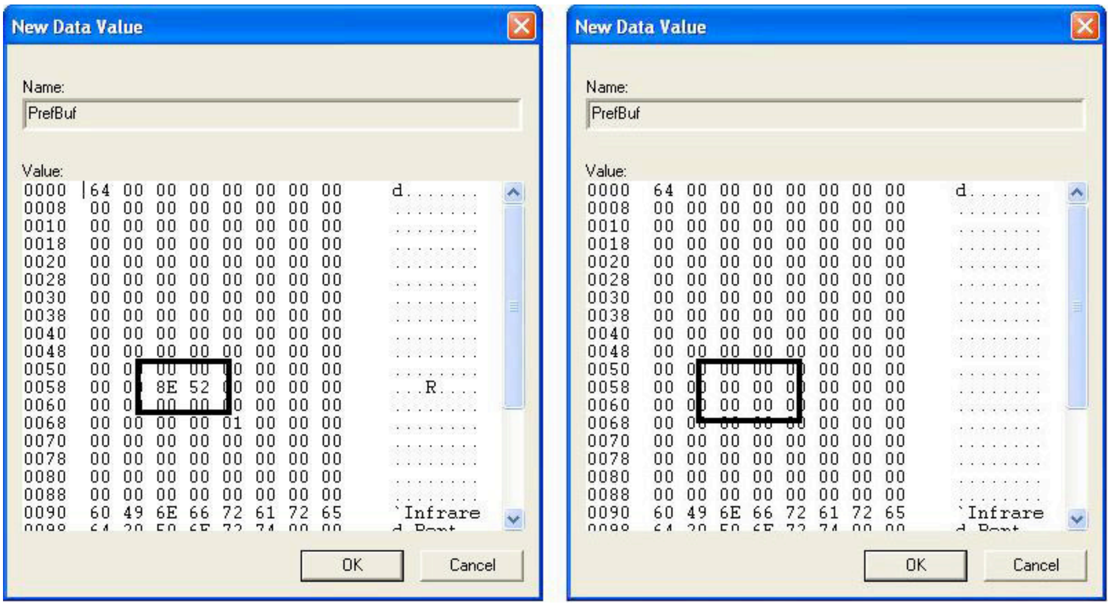
MoneyTracer claims “Encryption of your data by your own password.” While the password option is available, it only authenticates the user and does not actually encrypt any of the data, as claimed. To disable the ‘encryption’, set the following key to ‘0’.

\HKLM\SOFTWARE\Maction\MoneyTracer\bEnablePassword = 0

TinyStocks Stock Manager

TinyStocks states “Stock Manager can be protected with a 4-digit PIN number.” This PIN is stored as a four byte value within a preferences string in the registry. The following lists the location and provides a screen shot of the key with the password set/unset.

HKCU\Software\TinyStocks\Stock Manager\



Name: PrefBuf

Value:

```
0000 |64 00 00 00 00 00 00 00   d.......
0008  00 00 00 00 00 00 00 00   ........
0010  00 00 00 00 00 00 00 00   ........
0018  00 00 00 00 00 00 00 00   ........
0020  00 00 00 00 00 00 00 00   ........
0028  00 00 00 00 00 00 00 00   ........
0030  00 00 00 00 00 00 00 00   ........
0038  00 00 00 00 00 00 00 00   ........
0040  00 00 00 00 00 00 00 00   ........
0048  00 00 00 00 00 00 00 00   ........
0050  00 00 00 00 00 00 00 00   ........
0058  00 00 8E 52 00 00 00 00   ...R....
0060  00 00 00 00 00 00 00 00   ........
0068  00 00 00 00 01 00 00 00   ........
0070  00 00 00 00 00 00 00 00   ........
0078  00 00 00 00 00 00 00 00   ........
0080  00 00 00 00 00 00 00 00   ........
0088  00 00 00 00 00 00 00 00   ........
0090  60 49 6E 66 72 61 72 65   `Infrare
0098  64 20 50 6F 72 74 00 00   d Port
```

Name: PrefBuf

Value:

```
0000  64 00 00 00 00 00 00 00   d.......
0008  00 00 00 00 00 00 00 00   ........
0010  00 00 00 00 00 00 00 00   ........
0018  00 00 00 00 00 00 00 00   ........
0020  00 00 00 00 00 00 00 00   ........
0028  00 00 00 00 00 00 00 00   ........
0030  00 00 00 00 00 00 00 00   ........
0038  00 00 00 00 00 00 00 00   ........
0040  00 00 00 00 00 00 00 00   ........
0048  00 00 00 00 00 00 00 00   ........
0050  00 00 00 00 00 00 00 00   ........
0058  00 00 00 00 00 00 00 00   ........
0060  00 00 00 00 00 00 00 00   ........
0068  00 00 00 00 00 00 00 00   ........
0070  00 00 00 00 00 00 00 00   ........
0078  00 00 00 00 00 00 00 00   ........
0080  00 00 00 00 00 00 00 00   ........
0088  00 00 00 00 00 00 00 00   ........
0090  60 49 6E 66 72 61 72 65   `Infrare
0098  64 20 50 6F 72 74 00 00   d Port
```

Figure 3: Screenshot of the StockManager registry key

When asked about this issue, TinyStocks replied, “The password protection in Stock Manager is not meant to be secure but to stop casual access to the program. The data itself is unencrypted and so it's quite easy to just look at it.”

PocketExepense Pro

PocketExpense Pro creates a .vol file that contains all its financial information. Included in the file are the settings associated with the password option. In this program, all the preferences are stored in a large hex string in the registry. However, it is possible to disable the password by changing the hex at 0x7D94 from 0xF4 to 0xD4.

Inspiration

Inspiration is a project management program that uses ‘built-in security features’ to “…keep files from accidentally being modified when handhelds are shared between multiple users.” Therefore, it is fair to say that the password was never meant to offer any true security.

However, if an attacker wanted to remove the password requirement, they would only have to overwrite the encrypted password value that is stored in the project header. Specifically, bytes 0x95 – 0xA3 need to be set to 0x20 0x00 0x20 0x00 etc.

Microsoft Money for Windows Mobile 2006

MS Money for Windows Mobile 2006 is a financial tracking program that can be used independently or with the MS Money application that runs on many desktops.

The program can be configured to require a password when it is launched. However, this password does not encrypt the data, which stored as plaintext in data stores in the Databases folder.

The password is stored in the registry at HKLM\SOFTWARE\Microsoft\Money2000 CE\Options\Display in an encrypted format. However, the encryption scheme used to protect the password from viewers is a weak proprietary algorithm and can be cracked using the following equation:

(((encrypted byte - A0)/4) * 8) + 24h) – encrypted byte = password byte (all hex calcs)

Finally, the password requirement can be nullified by deleting the key from the registry, which will cause the program to think the password option is not set.

Password\Credit Card\PIM Management Programs

The following programs are used to store sensitive information, such as password lists, web site login information, credit card numbers and more. Due to the nature of the data, these programs need to be secure. If an attacker can access the ‘protected’ information, they will have gained access to a wealth of information.

As illustrated, the previous financial programs do not protect your data. Although most vendors use security as a selling point, in reality a simple registry tweak will allow anyone access to this sensitive data. Even the vendors admit their software is insecure and recommend alternative steps to secure the data.

Password Master 1.0 – Free version

Password Master 1.0 allows you to “Keep all your passwords, Credit Card Numbers and other details in a single place. Carry your money or details virtually everywhere.” According to their website, “Since all the details you enter are sensitive data, the Password Manager helps you to create a Secure Login to the records. You can create a Master Password, which will work as your Master key for all the virtual locks you know.”

Unfortunately, if someone deletes the following key from the registry, the master key will be reset, thus allowing full access to the data.

\HKEY_CURRENT_USER\Software\Data\Password Master\Pref\dt

This version of the program is free. The vendor’s website provides this tool, but also advertises their Password Master 3.5 version that requires a payment. We look at this version later in this section.

Passman 1.2

Passman 1.2 is a password management program that can create and store a list of passwords. It includes an option for a startup password and also provides for ‘512bit encryption’ of the data. Both protection measures can be cracked.

To bypass the startup password, a malicious user only has to set the startpasswdenabled registry key to ‘0’.

\HKEY_CURRENT_USER\Software\passman
\preferences\startpasswdenabled.

However, if the database is encrypted, the actual data will still be secure. Unfortunately, the password used to encrypt the database is itself not properly protected. The following equation will decrypt the password stored in the registry, thus giving an attacker full access to the database.

Assume:
B is byte of password in hex
P is position of target byte (0-5 for this example)

B-(25-(3*P)) = Bplaintext
⇒ 26 23 20 1D 1A 17 = 111111

The end result is that the password option can be disabled, the password can be cracked, and the database can be decrypted by an unauthorized user.

Password Master 3.5

Password Master 3.5 states it will “Keep all your passwords, Credit Card Numbers and other secured details in a single place. Carry your money or details virtually everywhere. Now includes a Free Desktop Companion!” In other words, it performs much the same function as CodeWallet Pro.

Ironically, like the previous example, Password Master 3.5 also does not encrypt its information using a unique password. Instead it relies on the user provided password to authenticate the operator to the file, and then decrypts the data using an internal algorithm. Therefore, using the same technique outlined previously, an attacker only has to obtain the secure file and overwrite a few bytes of hex in the header to gain access to that file, and the ‘secured’ contents within. In this case, the hex range is from 0x2A - 0x5B.

In addition to the overwrite vulnerability, this program also was found to have a bug in the ‘hint’ feature that enables a user to obtain their password if they forget it based on a question/answer. However, if the user never configures the hint option, the program will give up the password regardless of a correct hint/answer combination. While this is a security risk, it is based on a software bug – not a broken security model.

It is important to note that Password Master 3.5 also includes a desktop companion that operates in the exact same way as its mobile counterpart. This desktop based program also suffers from the header overwrite bug.

CodeWallet 6.0.5

CodeWallet is one of the premier programs that fall into the category of Secure Information Manager. It will protect your sensitive information, including credit cards, passwords, etc., in an encrypted file that a user decrypts with a password when opening.

During testing, we initially thought that CodeWallet used the same dysfunctional method of ‘encryption’ used by Password Master. However, CodeWallet looked into our report and commented that the while it was possible to open a file, all the data was still encrypted.

After further research, we found that when a Wallet file is created, its encryption is tied to the original password used to create the file. If the password is changed after this, it will only change the authentication requirements, and not affect the encryption.

Unfortunately, the My Sample Wallet included with the program comes with a known password, which an attacker can use against other files based on the Sample Wallet. As a result, anyone who used the Sample Wallet as a template to build their own secure Wallet is vulnerable to the header over write attack.

Miscellaneous Information Disclosure Bugs

Not all Windows Mobile related security problems are related to failed protection schemes. This section will outline several other program and bugs that were found during the research project.

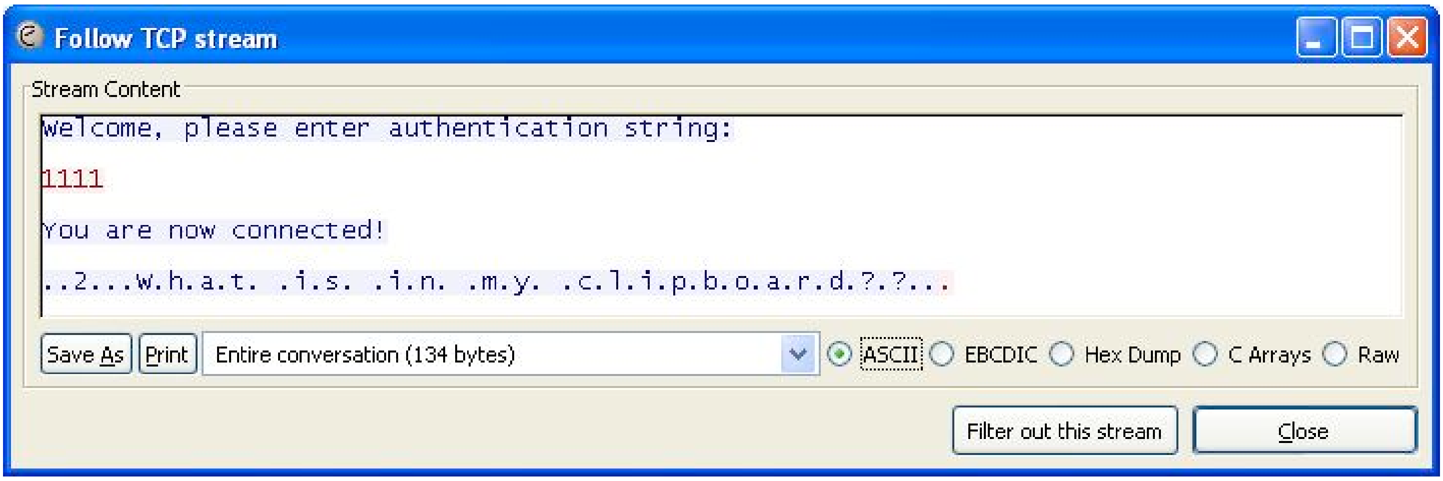
Remote Keyboard

From the vendors website, “Remote Keyboard is a program that connects PC keyboard and mouse to your Pocket PC over ActiveSync connection or TCP/IP network.” This is a handy program for power users who need to enter a lot of text into the PDA.

Once installed, the client on the PC sends out UDP packets containing an IP address to port 23 that are detected by a listener on the PDA. Upon detection, the PDA will connect back to port 8123 on the specified IP address. At this point the PC will query for the correct password, which is provided by the PDA application. Finally, the connection is made and the user can control the PDA remotely from the PC client.

We discovered a few problems with this program that can expose the password used to authenticate the connection as well as capture the clipboard contents of the PC. The first issue was discovered when we created a custom UDP packet that contained our “server’s” IP address and passed it onto the network. The Remote Keyboard listener on the PDA detected this packet, and immediately tried to connect to our computer on port 8123. Upon seeing this, we then created a small and simple ‘server’ that emulated the login process. As guessed, once the PDA had connected to the ‘server’ and negotiated the connection, it sent the ‘server’ the authentication password.

Using this captured password, we then telneted to the PC service running on port 8123 and discovered that the program dumped the entire contents of the clipboard onto the wire after a successful login. The following provides a screenshot of this bug.



```
welcome, please enter authentication string:

1111

You are now connected!

..2...w.h.a.t. .i.s. .i.n. .m.y. .c.l.i.p.b.o.a.r.d.?.?...
```

Entire conversation (134 bytes)

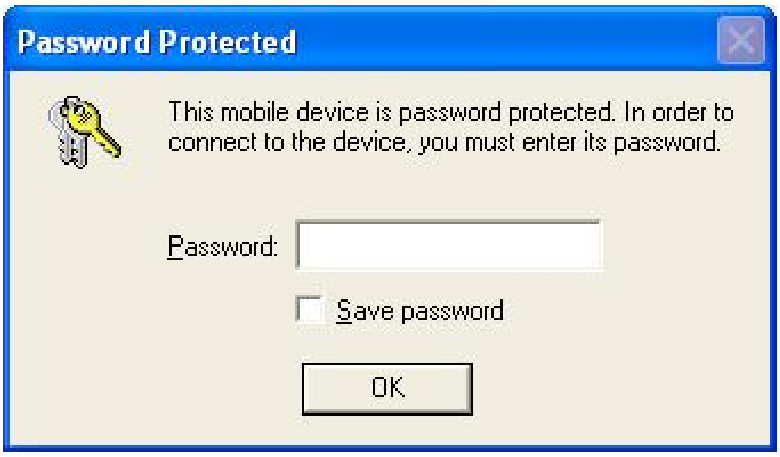
● ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ○ Raw

Figure 4: Remote Keyboard capture

ActiveSync 3.8

ActiveSync is ‘the’ program used to sync a Windows Mobile device to a PC. It is the most-downloaded Windows Mobile software application of all time. Contained in this program are functions used to upload software, sync up emails, and much more. Version 4.0 and above have restricted any form of network based synchronization; however, as many users rely on this feature for their day to day synchronization needs, Microsoft still provides AS 3.8 as a download.

As we discovered in mid-2005, the AS3.8 service on the PC opens up port 990 on any existing interface (i.e. wired, wireless, PPP, etc.). This port allows access to the ActiveSync service, which can be abused to spawn a password box on the PC users screen (figure 5). If a user enters a value in this dialog box, the characters of the password are returned to the attacker, who can then use this data to gain access to the protected PDA or create a connection between an attacker's PDA and the target PC.



Password Protected

This mobile device is password protected. In order to connect to the device, you must enter its password.

Password:

□ Save password

Figure 5: Spoofed spawned password dialog box

Suggested Fixes

As this document illustrates, there is a serious problem with regard to sensitive information and the handheld device. The following provides several suggestions as to how you can mitigate the risks we discussed.

Password protect your device

Windows Mobile comes with a password protection feature that will lock the device to unauthorized users. There are also third party vendors who provide a lock and wipe program that incorporates password protection with a memory wipe feature if the wrong password is used. However, it is important to note that a logon will not protect the data on external memory cards.

Encryption

All sensitive data must be secure using a known and proven encryption scheme/ program. This is especially important for external media cards often used in PDA's. It only takes a second to remove a card from a PDA. We recommend you inquire as to the encryption scheme used. Windows Mobile includes a MS Crypto API that has so far proven to be solid. While there could be others, programs that use this API are probably going to be secure.

Limit exposure

Given the statistics, it is recommended that PDA users limit the amount and type of data found on a device. Store files on different media cards, based on their function and only carry them with you when they are needed. By combine preventative security actions with reactive security fail safes (i.e. data wiping password programs), you can mitigate the security dangers even if the device is lost.

Use computer security common sense

The PDA is a hand held computer, and should be treated as one: do not download and execute untrusted software, use antivirus programs to scan/protect your device regularly, use a strong password and change it regularly, and disable unwanted services like Bluetooth. In short, employ the same precautions you would apply to your PC usage.

Seth Fogie is a former United States Navy Nuclear Engineer and one of the most widely read technical information security authors in the world.. At the present time he's a member of the Airscanner Mobile Security Team. They focus on exploring security threats and on reverse engineering malware for embedded and handheld wireless platforms.

HITBSecConf2006 - Malaysia

September 18th - 21st 2006 : Kuala Lumpur, Malaysia

DEEP KNOWLEDGE SECURITY CONFERENCE

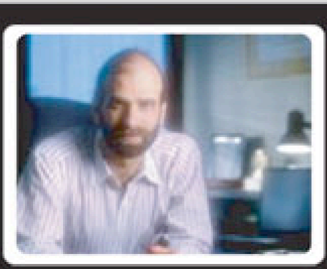
18th – 21st September 2006 • The Westin KL, Kuala Lumpur • Malaysia

An event not to be missed!

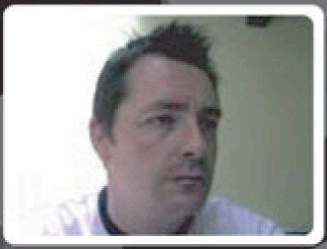
ASIA'S LARGEST NETWORK SECURITY CONFERENCE

2-Days 7 Tracks Hands-On Technical Training
2-Days Dual Track Conference
Capture The Flag "Live Hacking" Competition
30+ Network Security Specialists and Researchers Speakers
Panel discussions

Keynote Speakers



Bruce Schneier
Chief Technical Officer
Counterpane Internet Security, Inc.



Mark Curphey
Vice President of Consulting
Foundstone

John Viega
Chief Security Architect
McAfee Inc.

* Network Security Assessment and Latest Attack Methods
* Fundamental Defense Methodologies
* Close Look At the Latest Computer and Network Security Technologies
* Advanced Computer and Network Security Topics

Brought to you by:

hack in the box — Keeping Knowledge Free

Supported & Endorsed by:

Suruhanjaya Komunikasi dan Multimedia Malaysia — Malaysian Communications and Multimedia Commission

MAMPU

Official Airline Partner

malaysia AIRLINES

Main Sponsors:

Cisco Systems

Foundstone — A Division of McAfee

Microsoft

Media Partners

(IN)SECURE — OPEN. INFORMATIVE. TO THE POINT.

vb 2006 DUBLIN

phrack Magazine

hakin9

Supporting Organizations

HERT — Hacker Emergency Response Team

zone-h — the internet thermometer

Xfocus Team

xatrix security

Chaos Computer Club — KABELSALAT IST GESUND

SyScan'05

IT UNDERGROUND

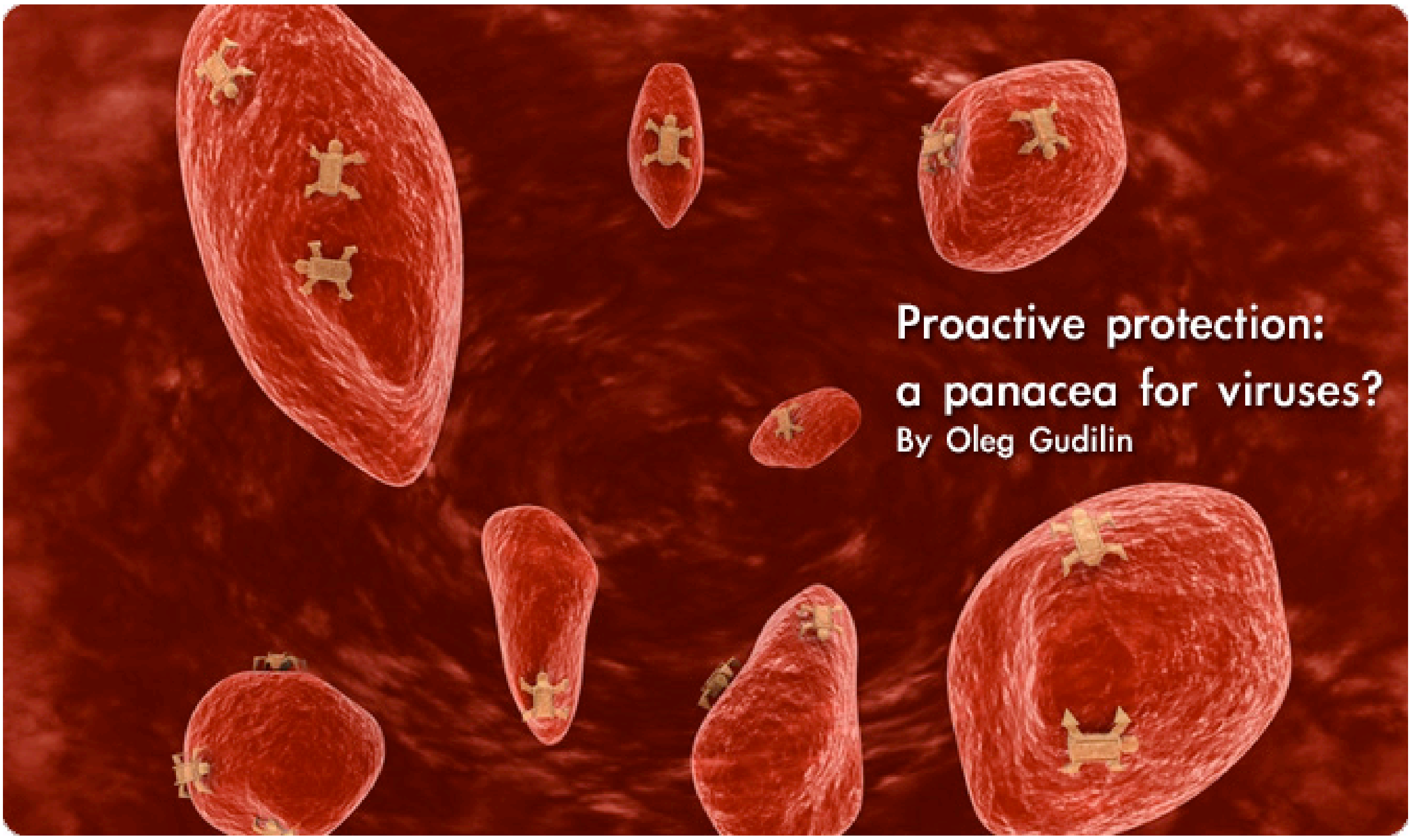
SIG²

Our Speakers are supported by:

CORE SECURITY TECHNOLOGIES

BELLUA

Conference URL:
http://conference.hackinthebox.org or http://conference.hitb.org



Proactive protection: a panacea for viruses?

By Oleg Gudilin

Virus attacks have firmly established themselves as the leading IT security threat. Not only do they result in financial losses, but they also serve as a vehicle for many other security threats, such as the theft of confidential information and unauthorized access to sensitive data. The antivirus industry has responded by coming up with a number of new approaches to protecting IT infrastructures - to name a few, these include proactive technologies, emergency updates during outbreaks, significantly more frequent antivirus database updates, etc. This article will provide more information on the newest technologies used by antivirus companies and help users to judge the effectiveness of these technologies more objectively. In this article, we will focus on proactive technologies.

Virus attacks cause enormous damage and, equally important, the number of types of malicious code is growing at an increasing rate. In 2005, growth in the number of malicious programs exploded: according to Kaspersky Lab, the average number of viruses detected monthly reached 6,368 by the end of the year. Overall growth for the year reached 117% compared with 93% for the previous year.

Likewise, the nature of the threat itself has changed. Malicious programs are not only much more numerous, but also significantly more dangerous than ever before. The antivirus industry has responded to the challenge with a number of new approaches to antivirus protection, including proactive technologies, shorter response times to new threats that can cause outbreaks, as well as more frequent antivirus database updates. This article provides a detailed analysis of the proactive protection, often promoted by vendors as a panacea for all existing and even all possible viruses.

An Introduction to Proactive Technologies

Contemporary antivirus products use two main approaches to detect malicious code - signature-based and proactive/heuristic analysis. The first method is sufficiently simple: objects on the user's computer are compared to templates (e.g., signatures) of known viruses. This technology involves continually tracking new malicious programs, and creating their descriptions, which are then included in the signature database. Therefore, an antivirus company should have an effective service for tracking and analyzing malicious code (that is, antivirus lab). The main criteria used to evaluate how effectively the signature-based approach is implemented include new threat response times, frequency of updates and detection rates.

The signature-based method has a number of obvious shortcomings. The primary disadvantage is the delayed response time to new threats. There is always a time lag between the appearance of a virus and the release of its signature. Contemporary viruses are capable of infecting millions of computers in a very short time.

Thus, proactive/heuristic methods of virus detection are becoming increasingly popular. The proactive approach does not involve releasing signatures. Instead, the antivirus program analyzes the code of objects scanned and/or the behavior of the applications launched and decides whether the software is malicious based on a predefined set of rules.

In principle, this technology can be used to detect malicious programs that are as yet unknown, which is why many antivirus software developers were quick to advertise proactive methods as a panacea for the rising wave of new malware. However, this is not the case. To judge the effectiveness of the proactive approach and whether it can be used independently from signature-based methods, one must understand the principles upon which proactive technologies are based.

There are several approaches which provide proactive protection. We will look at the two which are the most popular: heuristic analyzers and behavior blockers.

Heuristic Analysis

A heuristic analyzer (or simply, a heuristic) is a program that analyzes the code of an object and uses indirect methods of determining whether it is malicious. Unlike the signature-based method, a heuristic can detect both known and unknown viruses (i.e., those created later than the heuristic).

An analyzer usually begins by scanning the code for suspicious attributes (commands) characteristic of malicious programs. This method is called static analysis. For example, many malicious programs search for executable programs, open the files found and modify them. A heuristic examines an application’s code and increases its “suspiciousness counter” for that application if it encounters a suspicious command. If the value of the counter after examining the entire code of the application exceeds a predefined threshold, the object is considered suspicious.

The advantages of this method include ease of implementation and high performance. However, the detection rate for new malicious code is low, while the false positive rate is high.

Thus, in today’s antivirus programs, static analysis is used in combination with dynamic analysis. The idea behind this combined approach is to emulate the execution of an application in a secure virtual environment (which is also called an emulation buffer or “sandbox”) before it actually runs on a user’s computer. In their marketing materials, vendors also use another term - “virtual PC emulation”.

A dynamic heuristic analyzer copies part of an application’s code into the emulation buffer of the antivirus program and uses special “tricks” to emulate its execution. If any suspicious actions are detected during this “quasi-execution”, the object is considered malicious and its execution on the computer is blocked.

The dynamic method requires significantly more system resources than the static method, because analysis based on this method involves using a protected virtual environment, with execution of applications on the computer delayed according to the amount of time required to complete the analysis. At the same time, the dynamic method offers much higher malware detection rates than the static method, with much lower false positive rates.

The first heuristic analyzers became available in antivirus products sufficiently long ago, and all antivirus solutions now take advantage of more or less advanced heuristics.

Behavior Blockers

A behavior blocker is a program that analyzes the behavior of applications executed and blocks any dangerous activity. Unlike heuristic analyzers, where suspicious actions are tracked in emulation mode (dynamic heuristics), behavior blockers work in real-life conditions.

First-generation behavior blockers were not very sophisticated. Whenever a potentially dangerous action was detected, the user was prompted to allow or block the action. Although this approach worked in many situations, “suspicious” actions were sometimes performed by legitimate programs (including the operating system) and users who didn’t necessarily understand the process were often unable to understand the system’s prompts.

New-generation behavior blockers analyze sequences of operations rather than individual actions. This means that determining whether the behavior of applications is dangerous relies on more sophisticated analysis. This helps to significantly reduce the number of situations in which the is prompted by the system and increases the reliability of malware detection.

Today’s behavior blockers are able to monitor a wide range of events in the system. Their primary purpose is to control dangerous activity – that is, analyze the behavior of all processes running in the system and save information about all changes made to the file system and the registry. If an application performs dangerous actions, the user is alerted that the process is dangerous. The blocker can also intercept any attempts to inject code into other processes. Moreover, blockers can detect rootkits - i.e., programs that conceal the access of malicious code to files, folders and registry keys, as well as make programs, system services, drivers and network connections invisible to the user.

Another feature of behavior blockers that is particularly worth mentioning is their ability to control the integrity of applications and the Microsoft Windows system registry. In the latter case, a blocker monitors changes made to registry keys and can be used to define access rules to them for different applications. This makes it possible to roll back changes after detecting dangerous activity in the system in order to recover the system and return it to its state before infection, even after unknown programs have performed malicious activity.

NEW-GENERATION BEHAVIOR BLOCKERS ANALYZE SEQUENCES OF OPERATIONS RATHER THAN INDIVIDUAL ACTIONS. THIS MEANS THAT DETERMINING WHETHER THE BEHAVIOR OF APPLICATIONS IS DANGEROUS RELIES ON MORE SOPHISTICATED ANALYSIS.

Unlike heuristics, which are used in nearly all contemporary antivirus programs, behavior blockers are much less common. One example of an effective new-generation behavior blocker is the Proactive Defence Module included in Kaspersky Lab products.

The module includes all of the features mentioned above and also, importantly, a convenient system that informs the user of the dangers associated with any suspicious actions detected. Any behavior blocker requires input from the user at some point; so the user must be sufficiently competent. In practice, users often do not have the knowledge required, and information support (in effect, decision-making support) is an essential part of any contemporary antivirus solution.

To summarize, a behavior blocker can prevent both known and unknown (i.e., written after the blocker was developed) viruses from spreading, which is an undisputed advantage of this approach to protection.

On the other hand, even the latest generation of behavior blockers has an important shortcoming: actions of some legitimate programs can be identified as suspicious. Furthermore, user input is required for a final verdict regarding whether an application is malicious, which means that the user needs to be sufficiently knowledgeable.

Proactive Protection & Software Flaws

Some antivirus vendors include statements in their advertising and marketing materials that proactive/heuristic protection is a panacea for new threats, which does not require updating and therefore is always ready to block attacks, even for those viruses that do not as yet exist. Moreover, brochures and datasheets often apply this not only to threats that use known vulnerabilities, but to so-called “zero-day” exploits as well. In other words, according to these vendors, their proactive technologies are capable of blocking even malicious code which uses unknown flaws in applications (those for which patches are not yet available).

Unfortunately, either the authors of these materials are insincere or they don’t quite understand the technology well enough. Specifically, combating malicious code is described as a fight between virus writers and automatic methods (proactive/heuristic). In reality, the fight is between people - virus writers versus antivirus experts.

The proactive protection methods described above (heuristics and behavior blockers) are based on “knowledge” about suspicious actions characteristic of malicious programs. However, this “knowledge” (i.e., a set of behavior-related rules) is input into the program by antivirus experts and is obtained by analyzing the behavior of known viruses. Thus, proactive technologies are powerless against malicious code that uses completely new methods for penetrating and infecting computer systems, which appeared after the rules were developed – this is what zero-day threats are all about. Additionally, virus writers work hard to find new ways of evading behavior rules used by existing antivirus systems, which in turn significantly reduces the effectiveness of proactive methods.

Antivirus developers have no choice but to update their set of behavior rules and upgrade their heuristics in response to the emergence of new threats. These types of updates are certainly less frequent than in the case of virus signatures (code templates), but still need to be performed regularly. As the number of new threats increases, the frequency of such updates will inevitably rise as well. As a result, proactive protection will evolve into a variant of the signature method, albeit based on “behavior” rather than code patterns.

By concealing the need to update proactive protection from users, some antivirus vendors in effect deceive both their corporate and personal clients and the press. As a result, the public has a somewhat erroneous idea of the capabilities of proactive protection.

BY CONCEALING THE NEED TO UPDATE PROACTIVE PROTECTION FROM USERS, SOME ANTIVIRUS VENDORS DECEIVE BOTH THEIR CLIENTS AND THE PRESS.

Proactive vs. Signature-Based Methods

Despite their shortcomings, proactive methods do detect some threats before the relevant signatures are released. An example of this can be seen in the response of antivirus solutions to a worm called Email-Worm.Win32.Nyxem.e (Nyxem).

The Nyxem worm (also known as Blackmal, BlackWorm, MyWife, Kama Sutra, Grew and CME-24) can penetrate a computer when a user opens an email attachment containing links to pornographic and erotic sites or a file on open network resources. It takes the virus very little time to delete information on the hard drive. Up to 11 different file formats are affected (including Microsoft Word, Excel, PowerPoint, Access, Adobe Acrobat). The virus overwrites all useful information with a meaningless set of characters. Another distinctive characteristic of Nyxem is that it only becomes active on the third of each month.

A research group from Magdeburg University (AV-Test.org) carried out an independent study to assess the time it took different developers to respond once Nyxem emerged. It turned out that several antivirus products were able to detect the worm using proactive technologies, i.e. before the signatures were released:

Proactive detection of Nyxem by behavior blockers

Kaspersky Internet Security 2006 (Beta 2)	DETECTED
Internet Security Systems: Proventia-VPS	DETECTED
Panda Software: TruPrevent Personal	DETECTED

Proactive detection of Nyxem by heuristics

eSafe	Trojan/Worm [101] (suspicious)
Fortinet	Suspicious
McAfee	W32/Generic.worm!p2p
Nod32	NewHeur_PE (probably unknown virus)
Panda	Suspicious file

Overall, eight antivirus products detected Nyxem using proactive methods. Does this, however, mean that proactive technologies can replace the “classical” signature-based approach? Certainly not. To be valid, analysis of the effectiveness of proactive protection should be based on tests involving large virus collections, not individual viruses, however notorious.

One of the few widely acknowledged independent researchers who analyze proactive methods used by antivirus products on large virus collections is Andreas Clementi (www.av-comparatives.org). To find out which antivirus programs are capable of detecting threats that do not as yet exist, solutions can be tested on viruses that appeared recently, e.g., within the past three months. Naturally, antivirus programs are run with signature databases released three months ago, so that they are confronted with threats that were then “unknown” to them. Andreas Clementi’s focus is on the results of this type of testing.

Based on the results of testing conducted in 2005, the heuristics used in the Eset, Kaspersky Anti-Virus and Bitdefender solutions were the most effective.

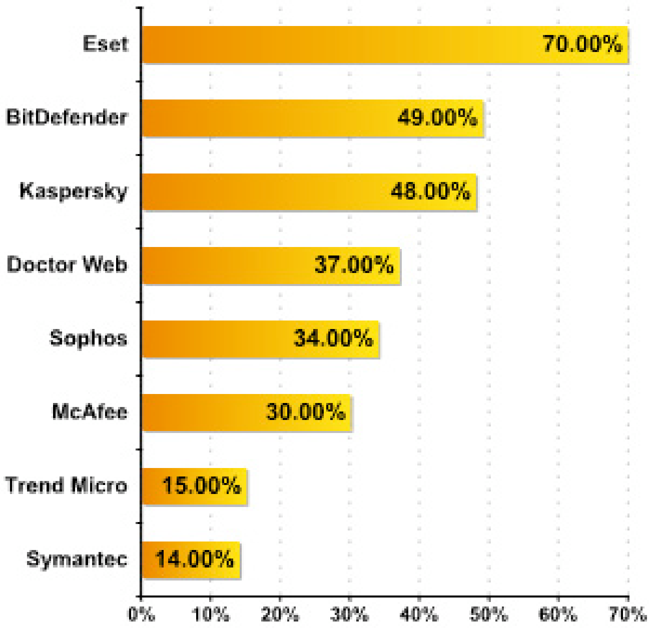


Figure 1. Proactive (heuristic) detection rates - Source: AV-comparatives.org

The test used a collection that included 8,259 viruses. From the results above, we see that the highest detection rate in the test was about 70%. This means that each of the solutions tested missed at least 2,475 viruses, hardly an insignificant figure.

In another test of the effectiveness of heuristic analyzers conducted by experts from Magdeburg University (AV-Test.org) in March 2006 for PC World magazine, detection rates achieved by leaders of the test did not exceed 60%. Testing was conducted using one-month old and two-month old signatures.

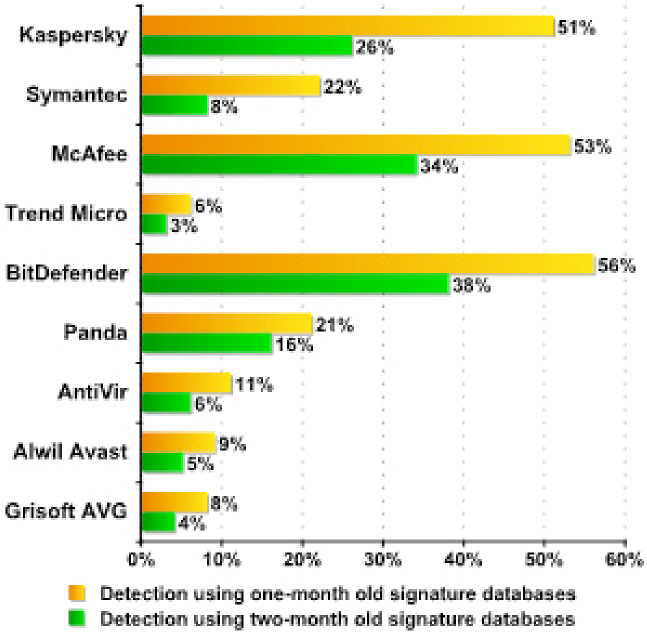


Figure 2. Proactive (heuristic) detection rates - Source: PC World, AV-Test.org

It should be noted that the high detection rates demonstrated by heuristic analyzers have a downside: their false positive rates are also very high. To operate normally, an antivirus program should strike a balance between detection rates and false positive rates. This is also true of behavior blockers.

The results of the analyses conducted by AV-comparatives.org and AV-Test.org provide a solid illustration of the fact that proactive methods alone are incapable of providing the necessary detection rates.

Antivirus vendors are perfectly aware of this and, for all their rhetoric on proactive technologies, continue to use classical signature-based detection methods in their solutions. Tellingly, developers of purely proactive solutions (Finjan, StarForce Safe'n'Sec) must purchase licenses for “classical” signature-based technologies from third parties and to use in their products.

Naturally, signature-based methods have shortcomings as well, but so far, the antivirus industry has been unable to come up with anything capable of replacing this classic approach. Consequently, the primary criteria to measure the effectiveness of antivirus solutions will continue to include not only the quality of proactive protection, but response time to new virus threats (the time it takes to add the relevant signature to the database and deliver the update to users) as well.

On the following page you’ll find information on average response times demonstrated by leading antivirus vendors for major antivirus threats during 2005. The Magdeburg University research group (AV-Test.org) analyzed the time it took developers to release updates containing the relevant signatures.

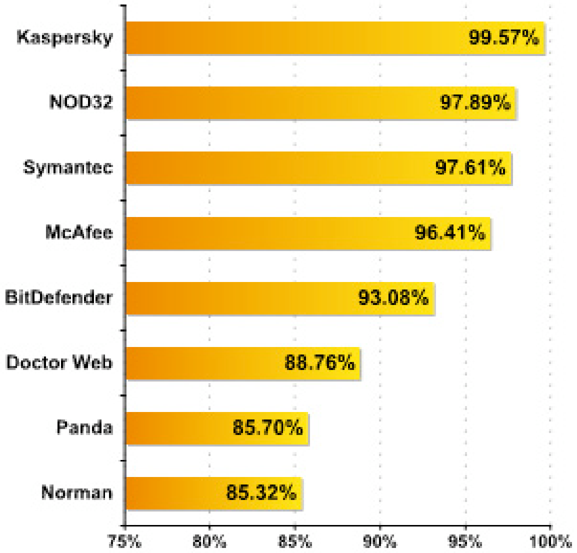
The analysis covered different variants of 16 worms that were most common in 2005, including Bagle, Bobax, Bropia, Fatso, Kelvir, Mydoom, Mytob, Sober and Wurmark.

Average response time	2005
0 to 2 hours	Kaspersky Lab
2 to 4 hours	BitDefender, Dr. Web, F-Secure, Norman, Sophos
4 to 6 hours	AntiVir, Command, Ikarus, Trend Micro
6 to 8 hours	F-Prot, Panda Software
8 to 10 hours	AVG, Avast, CA eTrust-InocuLAN, McAfee, VirusBuster
10 to 12 hours	Symantec
18 to 20 hours	CA eTrust-VET

Source: Ranking Response Times for Anti-Virus Programs (Andreas Marx of AV-Test.org)

In summary, a number of important conclusions can be made from the above. First of all, the proactive approach to combating malicious programs is the antivirus industry's response to the ever-growing stream of new malware and increasing rates at which it spreads. Existing proactive methods are indeed helpful in combating many new threats, but the idea that proactive technologies can replace regular updates to antivirus protection is a fallacy. In reality, proactive methods require updating as much as signature-based methods. Existing proactive techniques alone can not ensure high malicious program detection rates. Furthermore, higher detection rates are in this case accompanied by higher false positive rates. In this situation, the new threat response time remains a solid measure of antivirus program effectiveness. For optimal antivirus protection, proactive and signature-based methods should be used together, given that top detection rates can be achieved only by combining these two approaches. The figure below shows results of testing conducted by www.av-comparatives.org to determine the overall (signature-based + heuristic) malicious program detection levels. It may seem that the differences between programs that performed well in tests are small. Yet, it should be kept in mind that the test was performed on a collection of over 240,000 viruses and a difference of 1% accounts for about 2,400 missed viruses.

Users of antivirus solutions should not place too much trust in the information they find in vendor marketing materials. Independent tests that compare the overall capabilities of products are best suited to assessing the effectiveness of available solutions.



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

Events around the world

Gartner IT Security Summit 2006
18 September-19 September 2006 - Royal Lancaster Hotel, London, UK
http://www.gartner.com

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

IT Security World Conference & Expo 2006
25 September-27 September 2006 – San Francisco, USA
http://www.misti.com

IBM SecureWorld 2006
17 October-19 October 2006 – Montpellier, France
http://www.ibm.com

Storage Expo 2006
18 October-19 October 2006 – Olimpia, London, UK
http://www.storage-expo.com

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

If you want your event included in the HNS calendar e-mail us at press@net-security.org

Introducing the MySQL Sandbox

By Giuseppe Maxia

Installing a side instance of MySQL for testing purpose is a task that many administrators can perform without breaking a sweat. If you need to do that only once in a while, you need just to read the manual carefully, or to have some experience in this matter, and the task is accomplished quite easily.

If, however, your skills are below the Guru level, even to get this task done just once you may find yourself in trouble. And, let's face it, even experienced administrators, when they need to do this several times, with different versions of MySQL, may have trouble doing it right. It would be nice to have a tool that takes care of the dirty details for you and gets the job done quietly, without interfering with existing installations, and without side effects.

Such a tool exists, it's The MySQL Sandbox (sourceforge.net/projects/mysql-sandbox/). It is a framework for testing features under any version of MySQL from 3.23 to 5.1. Without fuss, it will install one server under your home directory, and it will provide some useful commands to start and stop it, and to use it within the sandbox.

There are many reasons for installing a side server. One is testing a potentially dangerous application, and you don't want to try it on a production server. Another reason is to try different versions of MySQL on a piece of code when hunting a bug. Or you are a consultant, your customers are all using different versions of the DBMS, and you need to test your procedures in an environment that is as close as possible to the your clients are using. I don't know about you, but in my job I have all the above needs, sometimes all at once.

After having performed the task of installing a side instance of MySQL dozens of times, I realized that I was perhaps wasting too much time, especially in terms of responsiveness, since I could not answer to emergency problems as quickly as I would like. Therefore, I forced myself to put together most of my expertise into a Perl script, and the MySQL Sandbox was born. Now, when I need to test something in any version of MySQL from the ancient 3.23 to the bleeding edge one in the Beta branch, I can do that in a few seconds. Literally.

With this package you can play with MySQL 5.x without need of using other computers. The server installed in the sandbox use non-standard ports and sockets, so that they won't interfere with existing MYSQL installations.

Getting started

To use MySQL Sandbox you need a few things:

- The Sandbox package itself;
- Linux or FreeBSD operating system (it may work in other *NIX OSs, but has not been tested);
- a binary package of MySQL 3.23 or later;
- Perl 5.8.1 or later (for installation only);
- a Bash compatible shell.

Installation

To show you the simplest installation, let's assume that you have already a MySQL binary installation, in its default location of `/usr/local/mysql`.

Unpack the distribution package in one empty directory and run the install script. For example:

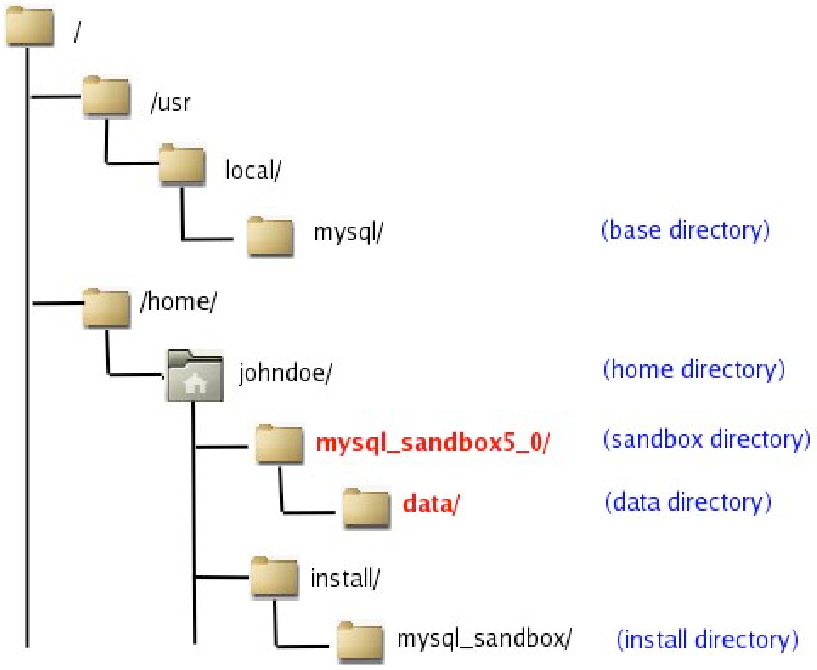
```
$ ./install.pl
```

Now, assuming that `johndoe` is your username, (I sincerely hope it is not), you got MySQL 5.0 in `/usr/local/mysql`, and the directory from which you are installing is `/home/johndoe/install/mysql_sandbox`, you will be greeted by the following confirmation screen:

```
The MySQL 5 Sandbox,  version 1.4 17-May-2006
    (C) 2006 Giuseppe Maxia, Stardata s.r.l.

installing with the following parameters:
sandbox_directory              = mysql_sandbox5_0
sandbox_port                   = 3310
datadir_from                   = archive
install_version                = 5.0
basedir                        = /usr/local/mysql
home_directory                 = /home/johndoe
my_file                        =
operating_system_user          = johndoe
db_user                        = datacharmer
db_password                    = datacharmer
force                          = 0
version_after_name             = 1
verbose                        = 0
do you agree? ([Y],n)
```

To better understand the options, look at Figure 1. below - Basic Sandbox directory organization



Putting aside the other options for now, let's focus on the directories. **basedir** is where you get the binaries from, i.e., in this case `/usr/local/mysql`.
home_directory is your `$HOME`, (`/home/johndoe`). It could be anywhere, but it should be a place where you've got all necessary writing privileges. Your `$HOME` is just a safe assumption. Under this directory, the installation process is going to create the **sandbox_directory** (red colored in the figure) and the **data directory** is just below it.

If you type **Y**, or just press ENTER, the installation progra will create `/home/johndoe/mysql_sandbox5_0/`, which will contain everything you need to work with this side instance.

Just cd to that directory, and use the `./start.sh` command. You will see the following:

```
$ ./start.sh
/usr/local/mysql ~/mysql_sandbox5_0
~/mysql_sandbox5_0
sandbox server started
sandbox server started
```

Your server is now installed and ready for use. Go ahead and try it out..

```
$ ./use.sh
Welcome to the MySQL monitor.  Commands end with ; or g.
Your MySQL connection id is 1 to server version: 5.0.22

Type 'help;' or 'h' for help. Type 'c' to clear the buffer.

mysql [localhost] {datacharmer} ((none)) >
```

After that, you may look around. There is a configuration file `my.sandbox.cnf`, containing the starting options for you server. There is a `USING` file, containing a reminder of which version and basedir you were using. And there is a `current_options.conf`, containing the options used by the installation to create your sandbox. Should you need to recreate it, use the installation script again with this file as a parameter.

```
$ cd /install_directory
$ ./install.pl -f current_options.conf
```

When you are done, you may stop the server.

```
$ ./stop.sh
```

The server will go down quietly. You may erase the whole directory if you wish. There are some more interesting things that you can do.

Advanced installation

The above installation was easy. But actually I don't recommend installing a sandbox from `/usr/local/mysql`.

The reason is that in such a location you install the current production release, and if you upgrade it, the sandbox will point to a version that is different from the one you originally intended.

I keep different versions grouped in a directory, conveniently named so that they can be easily accessed.

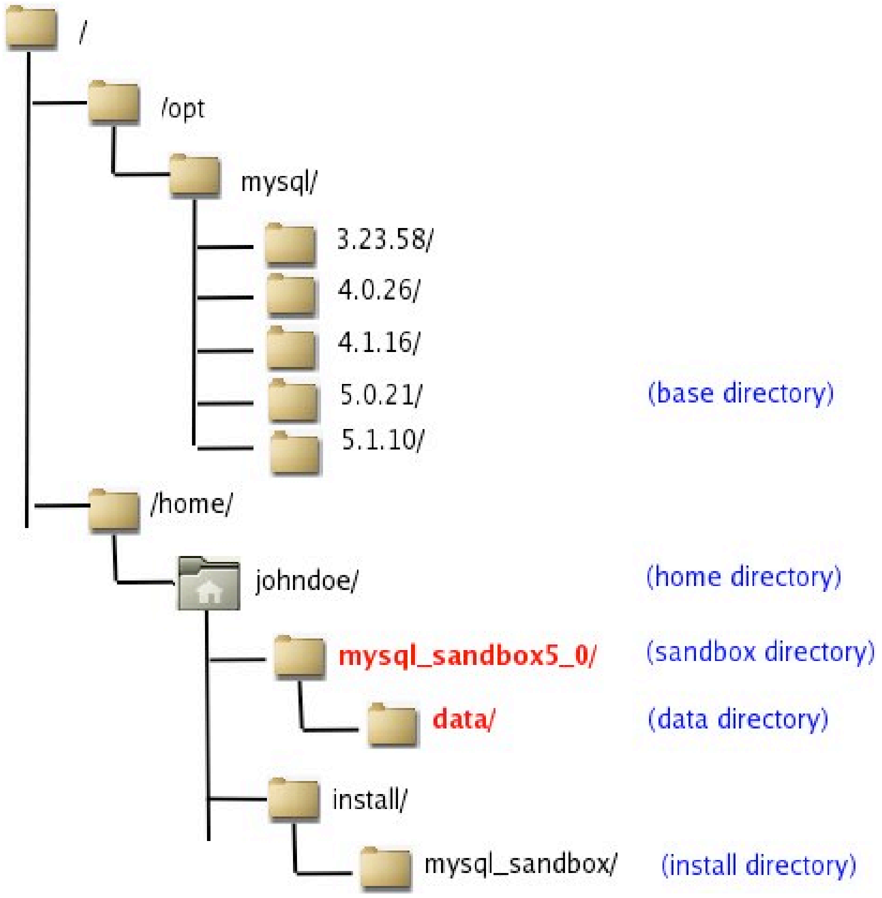


Figure 2. Advanced Sandbox directory organization

Usually I unpack the max package, and rename the unpacked directory to the simple version name so `mysql-max-5.0.21-linux-i686.tar.gz` becomes 5.0.21. If I have several packages of the same version (it happens when testing the source code) I add a letter to the end.

My side servers organization is something like the one shown in Figure 2.

If you want to get the same organization, just download the binary packages for your operating system (or compile it if you must) and for each version you may need to use, and unpack them in the same directory. Rename them appropriately, so that each directory is named after a version number, and you are ready to install.

If you want to achieve the same result as in the default installation, you should specify where the basedir option, so that the installation program will create appropriate configuration files and scripts.

```
./install --basedir=/opt/mysql/5.0.21
```

Should you run this command, though, you will get a different result.

```
/home/johndoe/mysql_sandbox5_0 already exists.
'--force' option not specified.
Installation halted
```

As a security measure the Sandbox installer will refuse to overwrite existing directories, unless you instruct it explicitly to do so with the –force option.

But let’s take a look at some of the more interesting features. The complete list is always available using `./install.pl --help`.

Building the data directory

By default, the `mysql` database comes with two users. The `datacharmer` user has been granted all privileges except `grant`. This user can connect from any host. The `root` user has got all privileges, including `grant`. This user can connect only from `localhost`.

You can control the creation of the mysql database with the `-datadir_from=[source]`.

The default value for [source] is `archive`, and this will use the packaged `mysql` database that was just described:

```
--datadir_from=archive
```

Use `dir:[name]` to import an existing `mysql` database:

```
--datadir_from=dir:/home/johndoe/my_default_mysql_db
```

To create the grant tables from scratch, use `script`:

```
--datadir_from=script
```

If you change the way your data directory is created, you should also modify the username and password you want to use. The installer will make a `grants.mysql` file containing the commands you should run as root to instantiate them. In this case, you can start using your sandbox by typing:

```
$ ./use.sh -u root -p
Enter password:
```

and then pressing `ENTER` for an empty password. Once inside the client, run **source grants.mysql**, and your users will be created with their appropriate passwords.

```
Welcome to the MySQL monitor.  Commands end with ; or g.
Your MySQL connection id is 1 to server version: 5.0.22

Type 'help;' or 'h' for help. Type 'c' to clear the buffer.

mysql [localhost] {root} ((none)) > source grants.mysql

Database changed
Query OK, 0 rows affected (0.00 sec)
Query OK, 0 rows affected (0.00 sec)
Query OK, 0 rows affected (0.01 sec)
Query OK, 0 rows affected (0.00 sec)

mysql [localhost] {root} (mysql) >
```

After that, you can run the script without additional arguments.

```
$ ./use.sh
Welcome to the MySQL monitor.  Commands end with ; or g.
Your MySQL connection id is 2 to server version: 5.0.22

Type 'help;' or 'h' for help. Type 'c' to clear the buffer.

mysql [localhost] {datacharmer} ((none)) >
```

Using the installation wizard

There are a few more options worth mentioning, but I won't get into detail about them now. You would not remember them all (heck, I don't remember them, even though I wrote the whole thing!). I will mention the only one you're going to need if you want to fine tune your sandbox installation without memorizing too many things. Just run this one:

```
./install.pl --interactive
```

Then the installation program will turn into a wizard (a text-based one, but a wizard nonetheless) that will guide you step-by-step through all the available options. The output looks like this:

```
~/install/mysql_sandbox ~/install/mysql_sandbox/docs
Enter the values for each option
To leave the interactive choice and accept default values
for the remaining options, enter 'default'
To go to the previous item, enter 'back'
To quit the installation without any action, enter 'quit'

-----------------------------------------------------------------
home_directory
   The home directory. (default: $HOME (/home/johndoe))
Your choice: (default value [/home/johndoe])
-----------------------------------------------------------------
sandbox_directory
   Where to install the sandbox, under home-directory
Your choice: (default value [mysql_sandbox])
-----------------------------------------------------------------
sandbox_port
   The port number to use for the sandbox server.
   (Default: 3310)
Your choice: (default value [3310])
```

Thirteen more options follow (and possibly more, depending on how much time has elapsed between my writing and your reading this piece). For each option, you could either press `ENTER`, accepting the default value, which is shown in brackets, or insert the value that is appropriate for your needs. If you have already changed what you wanted, and don't want to go through the rest of the options list, you could enter **default**, and you leave the wizard, accepting default values for the remaining options.

If you want to cancel the installation, just enter **quit** and the program is terminated without performing any action at all. To re-enter the previous option, type **back**.

Testing recent software on an older version

Let's say you developed an application, you tested it with the current production ready version (5.0), and it works fine. Before releasing to the wide public, though, you want to test it with earlier versions, to prevent unpleasant surprises to your support department.

Using the Sandbox, the task is easy. For example, to install the latest release from version 4.0, you should enter:

```
$ ./install.pl --basedir=/opt/mysql/4.0.27
            --sandbox_directory=mysql_sandbox_4_0_27
            --install_version=4.0 --sandbox_port=4027
            --no_ver_after_name
```

That will create a sandbox directory with a distinct name, and a port with the same number as the version itself. If that does not sound easy, you are right. It's easier than doing it manually, but the task can become even easier. Starting from Sandbox 1.5, there is an additional installing program, called **`express_install.pl`**. To accomplish exactly the same result, you can enter

```
$ ./express_install.pl /opt/mysql/4.0.27
```

If you are using **`/opt/mysql/`** as your binary repository, you can even omit the path. The express install will generate for you the necessary options for you.

```
$ ./express_install.pl 4.0.27
Executing ./install.pl --basedir=/opt/mysql/4.0.27
            --sandbox_directory=mysql_sandbox_4_0_27
            --install_version=4.0
            --sandbox_port=4027
            --no_ver_after_name

    The MySQL Sandbox,  version 1.5 23-May-2006
    (C) 2006 Giuseppe Maxia, Stardata s.r.l.
installing with the following parameters:
home_directory                 = /home/johndoe
sandbox_directory              = mysql_sandbox_4_0_27
sandbox_port                   = 4027
datadir_from                   = archive
install_version                = 4.0
basedir                        = /opt/mysql/4.0.27
my_file                        =
operating_system_user          = johndoe
db_user                        = datacharmer
db_password                    = datacharmer
force                          = 0
no_ver_after_name              = 1
verbose                        = 0
do you agree? ([Y],n) n
```

If you want, you may add some options to **`express_install.pl`**. Everything after the version (or the complete basedir) is passed to install.pl. For example:

```
$ ./express_install.pl 4.0.27 --interactive
Executing ./install.pl --basedir=/opt/mysql/4.0.27
                --sandbox_directory=mysql_sandbox_4_0_27
                --install_version=4.0
                --sandbox_port=4027
                --no_ver_after_name
                --interactive

Enter the values for each option
* To leave the interactive choice and accept default values
     for the remaining options, enter 'default'
* To go to the previous item, enter 'back'
* To quit the installation without any action, enter 'quit'

-----------------------------------------------------------------
home_directory
   The home directory. (default: $HOME (/home/johndoe))
Your choice: (current value [/home/johndoe]) quit
```

Using the Sandbox to perform a main MySQL installation

If you want to mimic a normal binary installation using the Sandbox, you can do it, by supplying the following options during to the installation program.

```
home_directory              = /usr/local/
sandbox_directory           = mysql
sandbox_port                = 3306
datadir_from                = script
install_version             = 5.0
basedir                     = /usr/local/mysql
my_file                     = large
operating_system_user       = johndoe
db_user                     = datacharmer
db_password                 = datacharmer
force                       = 1
no_ver_after_name           = 1
verbose                     = 0
```

The `force` option is necessary because it will overwrite existing files. Running `install.pl` with the above parameters will get you an installation very close to the default one. In addition to that, you will have three bash scripts (`_start.sh_`, `stop.sh`, `use.sh`), but you can also start and stop the server using the normal `mysql.server` script.
So why would you do that? Actually, you shouldn't. I am showing you how to do it so that you would get acquainted with the tool's flexibility. The main reason why you shouldn't do that is that putting your data under the `/usr/` directory is seldom a good idea. You may use a symbolic link for the data directory, but in general you should avoid having your data in the same place where you keep your applications.

So the best usage for the Sandbox would be to install a new data directory in an appropriate partition with enough free storage. It will save time and you'll get the same result as if you'd done it manually. Only neater.

Creating a sandbox using an existing my.cnf with a given version

When you are testing an existing application, or hunting for a bug, it's often important to setup a server with a specific `my.cnf`.
You know already that the `myfile` option will accept a `{small|large|huge}` keyword, and it will find a sample configuration file from `$BASEDIR/support-files`. Something that is also stated in the help text, but you may overlook, is that you can instead supply the full path of an existing my.cnf. For example:

```
$ ./express_install.pl /opt/5.0.21 --my_file=/opt/mysql/4.1.19/my.cnf
```

The installation program will skip from the given installation file those options that are indispensable to setup a proper sandbox, and will include all remaining options in the final `my.sandbox.cnf`, inserting a comment in the file to remind you the origin of such options.

Troubleshooting

Nothing is perfect and MySQL Sandbox is no exception. There are a couple of things that can go wrong.

a) Sandbox server not started yet

When you enter `./start.sh`, usually you see the welcoming message sandbox server started, and your are ready to use it. Sometimes you see a message saying sandbox server not started yet. That may be bad news, but it may only mean that the server is still building the files that are necessary for its functioning. For example, if your setup calls for a huge InnoDB tablespace, it may take a while before the server is up and running.

In these cases, have a look at the `hostname.err` file in the data directory. If the last message is along the line of “file such and such did not exist. new to be created”, it means that you have to wait a few seconds.

Look at the data directory, if you see a .pid file, everything was fine. If you don’t, than back to the error log, and try to figure out what was wrong.

b) Character set information not found

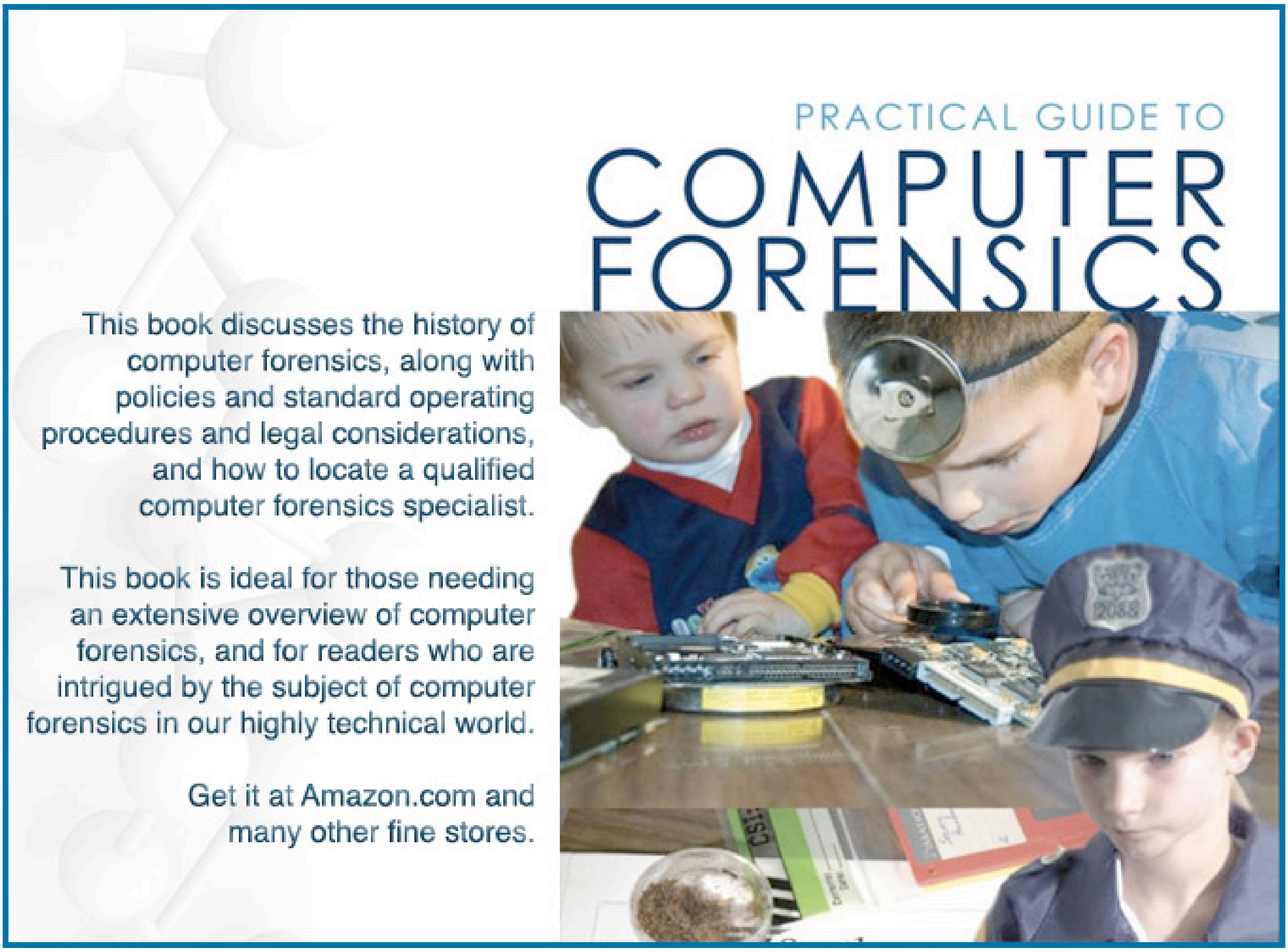
One of the cases that may happen, but only in some Linux distributions, is that a old version sandbox will complain about something along the lines of not finding a file that actually exists.

The message may say: Character set information not found in ‘`/opt/mysql/x.x.xx/share/mysql/english/errmsg.sys`’

You look at `/opt/mysql/x.x.xx/share/mysql/english/`, and indeed the `errmsg.sys` file is there. I think it’s a bug, but since it only happens in older versions, and only in Debian distributions, I will let it at that. The workaround that I found needs a root intervention. You need to set a symbolic link between your basedir and `/usr/local/mysql`. After that, the server will start.

I never had this problem on a non-Debian system.

Giuseppe Maxia is a systems analyst and database designer with 20 years of IT experience. He deals with data analysis and migration, performance optimization, general wizardry and is the founding partner and CTO of Stardata s.r.l.. Giuseppe has spoken at several Open Source conferences (MySQL UC 2003, 2004, OSDBCon 2005, Linux Expo, Webbit and more), in his home country and abroad. He is a well known contributor to PerlMonks and several mailing lists on MySQL and databases. You can find out more about him at www.datacharmer.org



Continuous protection of enterprise data: a comprehensive approach

By Ulf Mattsson

How to keep sensitive data locked down across applications, databases, and files, including ETL data loading tools, FTP processes and EDI data transfers.

Many consider the insider threat to represent the greatest vulnerability and exposure to enterprise resources. Database attacks are on the rise even as the risks of data breaches are increasing. Several industries must deal with legislation and regulation on data privacy.

This article will review how to protect sensitive data wherever the data resides: at application-level; within databases, files and operating systems; and in storage. We will address the management of associated encryption keys, access control and reporting - helping organizations mitigate risk and reduce costs, while protecting consumer, employee and partner information. The approach safeguards information by cryptographic protection from point-of-creation to point-of-deletion, to keep sensitive data locked down across applications, databases, and files - including ETL data loading tools, FTP processes and EDI data transfers. This design principle optimizes placement of functions for encryption and security enforcement among the modules of a distributed computer system.

The guiding concept, continuous protection of data, suggests that encryption functions placed at low levels, and typically implemented with native platform-based toolkits, may be redundant and of little value when compared with the cost of supporting them at that low level. The principle suggests that Enterprise levels of Data Protection and Key Management may be cost effective in many configurations. We also include a set of best practices that ensure not only a successful PCI audit, but a sustained improvement in the security and protection of sensitive data, and the limiting of theft and its costly aftermath.

Whether you decide to implement encryption inside or outside the data store, we recommend that:

- encrypted information be stored separately from encryption keys,
- strong authentication should be used to identify users before they decrypt sensitive information,
- access to keys should be monitored, audited and logged,
- sensitive data should be encrypted end-to-end, while in transit in the application and while in storage in enterprise data stores.

We introduce a system-solution example that complies with these requirements and provides a cost-effective implementation.

The business problem

The business problem of IT security is, however, more severe than the technical problems. Because current user access control solutions involve different components for authentication, authorization and administration (AAA), a solution can fail at any of these components. For example, one required component upgrade may no longer interoperate with another component, alienating users, leading to lost business, and perhaps, to security breaches. The result is that IT managers face continual, onerous cycles of development and maintenance. In short, the business problem of IT security is to prioritize that which simplifies and enhances the user experience, to support revenue and revenue growth, while reducing enterprise liability and expenditure

Today’s IT security solutions will need to be continually updated, however, in ever faster cycles, to remain effective - more frequent patches, upgrades, support, and perhaps replacement - to provide the same level of value tomorrow. To date initiatives have focused on data in backup and storage systems. However regional and vertical mandates - such as U.S. state breach notification laws (e.g., California Senate Bill 1386), the European Union Data Privacy Directive, Japan's Personal Information Protection Act and the Payment Card Industry standard - are driving companies to take an aggressive stance on protecting data-at-rest. Organizations are seeking to avoid the financial and brand integrity costs associated with compromised data, while positioning themselves to take advantage of "safe harbors” which often protect companies from penalties if appropriate steps have been taken to protect sensitive information.

The business problem of IT security is more severe than the technical problems.

Security gaps in enterprise security

Continual development and maintenance not only make IT security more expensive than it appears, they also make IT security solutions less secure, by increasing the number and the potential extent of security gaps that may exist at any time.

In a broad generalization, two types of attacks can exploit security gaps: network and data attacks. A network attack tries to interfere with client and/or server systems in transactions, in terms of their communication processes. For example, an attack may try to gain or deny access, read files, or insert information or code that affects communication.

Data attacks try to tamper with, and/or read, data in files or messages, by deleting, changing, reading, or inserting false data.

Trust, risk and the weakest link

The conventional risk model used in IT security is that of a linked chain - the system is a chain of events, where the weakest link is found and made stronger. We should question this approach because it fails to solve the problem of how to provide a secure IT system, even when a recognized weak link is made stronger. The strengthening of any link, even if made much stronger, would not make the system less vulnerable, and might make the system more vulnerable, because the security of the system would still depend on a weakest link (which might be the newly “hardened” link). Further, such solutions are actually based on the illogical presumption that "no part will fail at any time" - if a critical part fails, the system fails. In short, there is an inevitable single point-of-failure - that weakest link.

Making the link stronger will not make the single point-of-failure go away - at most it may shift it.

The need to know and the segregation of duties

The technical objective of information security may be stated as: “avoid unnecessary concentration of information and power; allow enough concentration to make a task possible to execute." An all-knowing, all-powerful entity would be the perfect attacker and could break any security measure. This is why we oftentimes talk about "need to know" and "separation of powers." We name these principles, respectively, information granularity and power granularity.

These concepts mean that information should not be provided in its entirety to a single entity. This is the reason business information and power should be carefully distributed, for example, among local employees, the office management, the enterprise management and the customer. And, contrary to what many advocate for IT security solutions, there should be no single point of control in an IT security system. This can be the single point of failure - no matter how trustworthy a single point of control is, its failure or compromise leaves no recourse for recovery.

A comprehensive approach to enterprise data protection

New business models rely on open networks with multiple access points to conduct business in real time, driving down costs and improving response times to revenue generating opportunities. By leveraging the ability to quickly exchange critical information and improve their competitive position, enterprises are introducing new vulnerabilities that can be exploited to gain unauthorized access to sensitive information. By establishing appropriate enterprise architecture key management, with encryption at application-, database- and file-level, the organization maximizes benefits while minimizing potential pitfalls to operational processes farther down the line. Each type of application and storage method may need a different approach to lock down data. This paper reviews a practical implementation of a transparent approach to keep sensitive data locked down, utilizing policy driven encryption and key management for data-at-rest and in-transit across enterprise systems. The encryption solution operates at the field, record and file levels to suit the operational needs for each type of application and data storage system.

The primary vulnerability of the database and file level encryption

The primary vulnerability of database- and file-level encryption is that they do not protect against application-level attacks - the encryption function is solely implemented within the DBMS. The application protection solution institutes policies and procedures that enable software developers to effectively build security into enterprise applications, employing external filters to block attacks.

Hackers, crackers, internal attacks and business evolution are facts of life; as a result, security threats, leaks and lack of scale will constantly plague user access control solutions based on password lists, access control databases, and shared secrets. With more users, more applications and more revenue depending on Web resources, it is more important than ever before to provide remote user access while protecting the enterprise's resources. With multiple administrative domains and the need for quick response to market changes, managers often need centralized user administration and control delegation to be effective. For end-to-end web security, consider implementing application-layer encryption security to protect PINs and other sensitive data in communications between web browsers and hosts. App-level protection ensures sensitive information is protected from its point of entry until it is validated or used by the target applications. This addresses an inherent limitation in most Secure Socket Layer (SSL) implementations that terminate encryption at the web servers and create the potential exposure of clear text in the form of sensitive user credentials and business transactions.

PROTECTING CUSTOMER DATA IS MUCH LESS EXPENSIVE THAN DEALING WITH A SECURITY BREACH.

A framework that includes the following components

This security solution helps companies protect themselves through a framework that includes the following components:

1. Encryption key management: enables organizations to manage encryption keys generated by disparate enterprise applications helping to guarantee the seamless flow of protected information, with minimal intrusiveness.

2. Application protection: institutes policies and procedures that enable enterprise software developers to effectively build security into applications and use external filters to block attacks.

3. Data protection: helps ensure that data is encrypted wherever it resides, including databases, files/OSs, and in storage, with minimal intrusiveness and most granular separation of duties.

According to Gartner, Inc.: "Protecting customer data is much less expensive than dealing with a security breach in which records are exposed and potentially misused." Specifically, Gartner estimates that compromises involving more than 1 million accounts will be close to $50 per account. Smaller breaches carry significant costs, as well -- in 2002, Gartner estimated that the cost per account will be closer to $1,500 per account, not including market cap fluctuation, when about 5,000 accounts were compromised. (Source: "Data Protection is Less Costly than Data Breaches," John Pescatore and Avivah Litan. September 16, 2005).

The challenge to get the parts together

The challenge is to get the parts together - expertise in database encryption, application security and file encryption to be applied in the integrated solution:

1. Protection of sensitive data in any place where data reside will include an enterprise key management and crypto support (or remote access to crypto support) on all major OS platforms.

2. Sensitive data should be encrypted end-to-end will include an enterprise key management and crypto support (or remote access to crypto support) on all major OS platforms. Partner solution will extend the support to additional platforms, including mobile devices.

3. The distribution and protection of encryption keys in all different environments is the foundation for enforcing authentication and non-repudiation. The protection of encryption keys is linked to the authentication and authorization that supports the non-repudiation of each cryptographic operation. Each environment presents a unique level to enforce or not enforce authentication and non-repudiation, based on the support provided by the combination of OS and DBMS.

Consolidation of policy management

There is a real need, thus, to bring together policy, management and implementation considerations influencing security assurance for each particular IT solution. Other security principles such as redundancy, diversity, no single point of failure, and least-privilege also need to be used in defining the specific requirements for a secure IT system.

Such requirements need to be clearly formulated, decidable and, as much as possible, complete. An end-to-end design is important to assure effectiveness, because attacks and errors are hard to detect and prevent at interface points. Because there are no paper trails, non-repudiation is also essential for Internet and IT security systems. Non-repudiation is often defined as providing proof that a particular act had actually been performed - example, as demonstrated by a trusted time-stamp. However, we may view the concept of non-repudiation much more strictly - as in preventing the effective denial of an act. The first definition describes the component quality used in the IT system, where a weak component may compromise the whole system. The stricter definition focuses on the need to continuously evaluate all potential and existing threats, verifying any additional security design features that might be necessary to mitigate risks stemming from the most likely or most damaging threats to the customer environment, and eventual changes in that environment.

An effective data protection solution

An effective data protection solution needs to deal with an extensive list of security properties. A secure IT system must not "pop" like a balloon when subjected to an attack, or fail silently, leaving no trace of the attack. There should be no single point of failure. There must be multiple channels of communication and correction, even if the channels are not 100% independent. We intuit an increase in reliability by using multiple channels of information. This correlates well with our perception of how trust may be defined - we know from experience that we trust more when we have more evidence to support trust. In an IT security system, we define trust as qualified reliance on information, based on factors independent of that information. More precisely, trust is that which is essential to a communication channel but cannot be transferred using that channel.

A true end-to-end encryption solution

To cope with the accelerated risks and obsolescence typical of IT security solutions, enterprises need an End-To-End IT security solution that can provide shorter, less expensive, deployment, development and maintenance cycles. The solution should minimize the probability of patches, upgrades and support during the lifetime of an IT security system. The solution also needs to integrate core security services and eliminate known or costly weak links such as password lists, access control databases, shared secrets, and client-side PKI.

What are these core security services, what else is required in order to solve both the technical and business problems of IT security? We first need to look at the security gaps that can be exploited, and what security services are necessary to prevent such breaches. Second, we need to realize that it is the combination, and interoperation, of security properties that can provide the resiliency required of a secure IT system. An IT security system needs to have the equivalent of several independent, active barriers, controlling different security aspects but complementing each barrier's function. Lastly, an IT security solution needs to be highly scalable, supporting anywhere from hundreds to millions or tens of millions of users, compatible with the current infrastructure and standards, and extensible.

Security management must be based on a security policy

Several key elements of a comprehensive security policy:

- Trust - qualified reliance on information, based on factors independent of that information
- Access control - granting access to information objects based on the trusted identity of users - limiting access to system resources to authorized users, processes or systems - validated before decryption of data items is authorized
- Audit and maintenance of historical logs of all transactions, reviewed to maintain accountability for all security relevant events. This covers archived data with support for adding strong encryption over time.
- Authentication - corroboration of a credential or claim; the ability to establish and verify the validity of a user, user device or other entity - also, the integrity of the information stored or transmitted. This should cover integration with LDAP, X.500, i500 product, Active Directory

implementation, and other derivations and implementations of user directories.

- Authorization - conveyance of rights, power or privilege to see, do or be something, including The Open Group, OASIS, and other XML-based authorization standard.
- Confidentiality - ensuring that data is not available or disclosed to unauthorized individuals, entities or processes, to include separation of duties/power/roles.
- Integrity - ensuring that data is not altered or destroyed in an unauthorized manner.
- Non-repudiation - the ability to prevent the effective denial of an act; the ability to prove the origin and delivery of transactions and data-at-rest changes.
- Security management - a defined process to perform system security functions such as audit, credential management and configuration management. Security management must be based on a security policy - the set of laws, rules, and practices that regulate how an enterprise manages, protects, and distributes sensitive information.

Encryption should be implemented to leverage the existing high-performance infrastructure and scale, not impede overall performance.

Centralized administration of security policies

In short, with centralized user administration, security policies can remain consistent, easy-to-manage and audit. Centralized administration of users is, thus, a common operational requirement in networked environments. However, the need for centralized user administration does not mean the absence of delegation.

Delegated or distributed administration is a requirement for medium-size to large enterprises, where administrative domains within an organizational unit or divisional lines are common. It is unrealistic to have one group responsible for administration for the entire enterprise. Delegated administration is also necessary for B2B/partner e-business models (e.g., a partner company administers its own employees in a constrained administrative domain within your infrastructure).

Delegated administration is frequently implemented by means of control delegation, defined as allowing local sub-domain control within a domain. The need for centralized user administration also does not mean a need for centralized control in the security solution that provides it. In fact, we need to avoid the seemingly desirable scenario of a single point of control, which The Continuously Secure Data System recognizes as a single point of failure. Thus, to achieve central user administration and to provide control delegation, an IT security solution should use a distributed, highly non-local system, transparent to the users of the system. In short, one needs a distributed central control system, where different authority sub-domains can be activated, suspended and revoked by a central administration.

Best practice for protecting data-at-rest

In order to mitigate this increased risk, the use of encryption is increasingly being required or recommended as a best practice for protecting data-at-rest. Financial services institutions, merchants that accept credit cards, health care services enterprises, and government agencies that maintain confidential personal information are required to consider use of encryption to protect their personally identifiable information PII. System performance scalability is critical to meeting the needs of an enterprise. Introducing a variable to the infrastructure that limits scaling in a predictable manner can “bottleneck” the flow of data and prevent the organization from achieving forecasted return on its IT investment.

Encryption should be implemented to leverage the existing high-performance infrastructure and scale, not impede overall performance.

The Continuously Secure Data Protection System

Our vision is that security needs to “own” an end-to-end property; otherwise, security breaches are possible at security point-interfaces, which may allow gaps in protection. As it is clear from the previous discussion, authentication and authorization are not sufficient for this end-to-end E2E purpose.

Providing an E2E-encryption solution for IT security and user access control, the Continuously Secure Data System establishes the medium to integrate a number of core capabilities in IT security solutions including:

- tamperproof cryptographic credentials
- authentication
- authorization
- centralized user administration
- control delegation
- access control
- session control
- no single point of control
- least privilege
- data confidentiality
- data integrity
- non-repudiation
- spoof prevention
- immediate suspension as well as revocation of credentials

The Continuously Secure Data System also recognizes the need to bind a system of trust to IT security solutions, to communicate trust not only machine-to- machine, but also human–to-machine. We need to provide these capabilities in a scalable system, supporting hundreds of users, to millions or tens of millions, and which is compatible with existing infrastructure, current & evolving Internet standards, with as much backward compatibility as possible. Finally, the Continuously Secure Data System must take business drivers into account - quicker and less expensive deployment, development and maintenance cycles; less need for integration with other (changing) products; ease-of-use; and close back-end to front-end integration so that legacy systems can be reliably used.

Policy-driven data protection

Such data protection solution helps ensure that data is encrypted everywhere it may reside, with minimal intrusiveness and maximal separation of duties. Application code and database schemas are sensitive to changes in data type and data length. Our policy-driven solution allows transparent data-level encryption that retains data field type or length. Data Transformation and Protection DTP can be added to reduce the need for changes to data structures and applications. The field-level encryption approach is very useful when dealing with EDI/FTP/flat files being transferred between discrete systems. At no time is sensitive data in an unencrypted state at-rest on any system.

How to encrypt data if a binary format is not desirable

If data is to be managed in binary format, “varbinary” can be used as the data type to store encrypted information. On the other hand, if a binary format is not desirable, the encrypted data can be encoded and stored in a VARCHAR field. There are size and performance penalties when using an encoded format, but this may be necessary in environments that do not interface well with binary formats, if support for transparent data-level encryption is not used. In environments where it is unnecessary to encrypt all data within a data store, a solution with granular capabilities is ideal. Even if only a small subset of sensitive information needs to be encrypted, additional space will still be required if transparent data-level encryption is not used. Secure data-level encryption for data-at-rest can be based on block ciphers.

The proposed solution is based on transparent data level encryption with Data Type Preservation that Does Not Change ASCII Data Field Type or length. The solution provides a cost effective implementation, avoiding changes of Millions of Lines of Business Code in larger enterprise information systems. The solution also provides an effective last line of defense: selective column-level data item encryption, cryptographically enforced authorization; key management based on hardware or software, secure audit and reporting facility, and enforced separation of duties. The method is cryptographically strong, works with any DBMS and OS, works with different character sets, no application or database changes, no programming language dependence, fail safe, requires no DBA intervention. Data loader functions normally and queries function normally. Enhanced search capabilities based on partial encryption of data can easily be added with this approach.

The optimal place to encrypt data will always depend on the situation

Give careful consideration to the performance impact of implementing a data encryption solution. First, enterprises must adopt an approach to encrypting sensitive fields only. Such a solution allows the enforcement module to be installed with the file system, at the database table-space level, or at column-level to meet different operations needs. It allows the encrypt/decrypt of data as the database process reads or writes to its database files. This enables it to perform cryptographic operations in file system block segments, instead of in individual cell, rows or columns.

Allow optional granularity and implementation layers for the data encryption

Compared to triggers, stored procedures, external API calls and network round-trips, there is very little overhead in some operational situations. Furthermore, this solution can decrypt data before it is read into the database's cache. Subsequent hits of this data in the cache neither incur additional overhead. Nor does this architecture diminish database index effectiveness. It depends on the situation if this exposure will meet your security requirements.

Encrypt a few very sensitive data elements

Encryption, by its nature, slows most SQL statements. With care, the amount of overhead should be minimal. Also, encrypted data will have a significant impact on your database design. In general, it is best to encrypt a few very sensitive data elements in a schema, like Social security numbers, credit card numbers, patient names, etc. Some data values are not good candidates for encryption -- i.e., Booleans (true and false), or other small sets like integers 1-10. These values, and column names, may be easy to guess, so you want to decide whether encryption is really useful. Creating indexes on encrypted data is a good idea in some cases. Exact matches and joins of encrypted data will use the indexes you create. Since encrypted data is essentially binary data, range checking of encrypted data would require table scans. Range checking will require decrypting all the row values for a column, so avoid it if it is not tuned appropriately, with an accelerated search index.

Searching for encrypted value within a column

Searching for an exact match of an encrypted value within a column is possible, provided the same initialization vector is used for the entire column. On the other hand, searching for partial matches on encrypted data within a database can be challenging and may result in full table scans if support for accelerated index-search on encrypted data is not used. One approach to performing partial searches, without prohibitive performance constraints - and without revealing too much sensitive information - is to apply an HMAC to part of the sensitive data and store it in another column in the same row.

Encrypted columns can be a primary key

Encrypted columns can be a primary key or part of a primary key, since the encryption of a piece of data is stable (i.e., it always produces the same result), and no two distinct pieces of data will produce the same cipher text, provided consistent use of the key and initialization vector. However, when encrypting entire columns of an existing database, depending on the data migration method, database administrators might have to drop existing primary keys, as well as any other associated reference keys, and re-create them after the data is encrypted. For this reason, encrypting a column that is part of a primary key constraint is not recommended if support for accelerated index search on encrypted data is not used. Since primary keys are automatically indexed, there are also performance considerations, particularly if support for accelerated index-search on encrypted data is not used.

Plan before encrypting information in indexed fields

We create indexes to facilitate the search of a particular record, or set of records, from a database table. Carefully plan before encrypting information in indexed fields. If you do not employ accelerated database indexes, lookups and searches in large databases may be seriously degraded by the computational overhead of decrypting the field contents. This can prove frustrating at first because administrators often index fields that must be encrypted - Social Security numbers or credit card numbers. New planning considerations will need to be made when determining what fields to index if accelerated database indexes are not used. Indexes are created on a specific column or a set of columns. When the database table is selected, and WHERE conditions are provided, the database will typically use the indexes to locate the records, avoiding the need to do a full table scan. In many cases, searching on an encrypted column will require the database to perform a full table scan regardless of whether an index exists. For this reason, encrypting a column that is part of an index is not recommended, if support for accelerated index-search on encrypted data is not used.

When to use initialization vectors

When using CBC mode of a block encryption algorithm, a randomly generated initialization vector is used and must be stored for future use when the data is decrypted. Since the IV does not need to be kept secret it can be stored in the database. If the application requires having an IV per column, which can be necessary to allow for searching within that column, the value can be stored in a separate table. For a more secure deployment, but with limited searching capabilities if support for accelerated index-search on encrypted data is not used, an IV can be generated per row and stored with the data. In the case where multiple columns are encrypted, but the table has space limitations, the same IV can be reused for each encrypted value in the row, even if the encryption keys for each column are different, provided the encryption algorithm and key size are the same.

Carefully plan before encrypting information in indexed fields.

The use of initialization vectors together with certain encryption modes

If you are using AES-CTR Advanced Encryption Standard and DTP is functionally equivalent to a stream cipher; it generates a pseudorandom cipher stream that is XORed into plaintext to form ciphertext. The cipher stream is generated by applying the AES encrypt operation on a sequence of 128-bit counter blocks. Counter blocks, in turn, are generated based on record sequence numbers (in the case of TLS), or a combination of record sequence and epoch numbers (in the case of DTLS.) AES Counter Mode is typically used as a Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS): It should be noted that although the client and server use the same sequence number space, they use different write keys and counter blocks. There is one important constraint on the use of counter mode ciphers: for a given key, a counter block value MUST never be used more than once. This constraint is required because a given key and counter block value completely specify a portion of the cipher stream. Hence, a particular counter block value when used (with a given key) to generate more than one cipher text leaks information about the corresponding plaintexts. Given this constraint, the challenge then is in the design of the counter block.

Database file encryption will leave your live database in clear

This solution's policies can selectively encrypt individual files and do not require that “the entire database” be encrypted. Database administrators can assign one or more tables to a table-space file - policies may then specify which table-spaces to encrypt. In this way, you encrypt only the database tables that have sensitive data, and leave the other tables unencrypted. This said, in some situations, some customers choose to encrypt all database files because there is little performance penalty and no additional implementation effort in doing so.

Central encryption appliances vs. distributed encryption engines

Network-attached encryption (NAED), as a network-attached encryption appliance was implemented by my teams at IBM, involving work with nCipher, Eracom and Chrysalis (SafeNet) starting in 1994. Our research and benchmarking is reported here. A NAED is a hardware device that resides on the network, houses the encryption keys and executes all crypto operations. This topology has the added security of physically separating the keys from the data. However, this added security comes at a heavy price; performance can be 10-1000 times less efficient than alternative methods. SAN /NAS proxy encryption performs close to line-speed, but it is less feasible from a scalability perspective in a terabyte configuration compared to a host based file encryption solutions using software. The heavy price paid for such network-attached encryption? Benchmarks reveal a throughput of between 440 and 1,100 row-decryptions per second. This example debunks the generally held myth that NAEDs off-load work from the database. Further, a network-attached engine does not provide high availability, unless multiple engines are configured into a high availability cluster.

An off-load of work with the network-attached appliance?

The short answer is “no,” there isn’t an off-load of work since this solution must perform one encryption operation in the database, which is the same for other topologies, in addition to the encryption functions at the NAED. When a user requests secured data, the security system manages the process of retrieving encrypted data from the database, ensuring that the request is from an authorized user, and performing the decryption process. In this topology, the encryption agent handles the request and retrieves the encrypted data from the database. It sends the encrypted data over the network to be decrypted by the NAED. Inside the NAED are the keys and algorithms to decrypt the data. Once decrypted, however, we have clear-text information that needs to be sent back over the wire to the database server. This requires that we re-secure the information for transit, typically through a secure communication process such as SSL. When the data arrives at the agent on the database server, it has to be returned to clear-text, and then it is served up to the calling application.

Exposing an encryption appliance will introduce an additional point of attack.

An integrated central and distributed solution can protect from this vulnerability. Denial-of-service attacks are another related concern with network-attached engines. Since the engine is available over TCP/IP, an attacker could flood the engine with traffic and block legitimate cryptographic requests. If required information can’t be decrypted, then a customer may not be able to place an order or access account information. If the database stores encrypted records that are critical for business operation, a successful denial-of-service attack could have severe consequences.

Scalable, centralized life-cycle cycle management for encryption keys

Well-worn though it may be, the saying that “the chain is only as strong as its weakest link” clearly applies to efforts of organizations to secure sensitive data and ensure data privacy. Keys are the foundation of all encryption-based security solutions. If a hacker, internal or external, gains access to your private keys, the security of all data formerly protected by encryption is gone. Not reduced - gone. That is a risk currently assumed by companies that store private keys used for data encryption in insecure locations whether Web, application, or database servers. These servers are typically not secure because there are many people with access to them, the servers are often misconfigured, and they often aren't kept up to date with the latest security patches. Additionally, keys are usually stored in an easily readable plaintext format. Even organizations that make efforts to protect private keys with passwords find that these passwords aren't protected properly, are chosen poorly, and usually must be shared between multiple administrators. These keys are vulnerable to discovery. An intruder who compromises your keys can launch "eavesdropping" attacks using the stolen key to hack into vital data repositories. This could result in data theft, loss of privacy for your employees and customers, and damages to brand credibility and customer confidence. Stringent security defenses protect each sensitive element of the system - each protected by its own unique, randomly generated key. Private keys are stored encrypted with several Triple-DES encryption keys that are nested.

AN INTRUDER WHO COMPROMISES YOUR KEYS CAN LAUNCH "EAVESDROPPING" ATTACKS USING THE STOLEN KEY TO HACK INTO VITAL DATA REPOSITORIES.

Effectively and efficiently manage encryption keys

Our encryption key management solution enables organizations to effectively and efficiently manage encryption keys generated by disparate enterprise applications, helping to guarantee the seamless flow of protected information, with minimal intrusiveness. One of the primary elements of modern cryptography most often recommended by regulations and industry standards is the concept of a data encryption key. Encryption requires that a key be used to initially encrypt a piece of sensitive information and is subsequently required to decrypt that information when needed by applications. Not only is it important to effectively protect this key against misuse, it is also important to ensure that the key is quickly accessible by applications when needed. Traditionally, applications that use encryption technology have had to handle the management of encryption keys on their own - creating a host of incompatible solutions.

The Key Manager is designed to help companies alleviate these problems by centralizing the life-cycle management of encryption keys across their information infrastructure. Key Manager works across a wide variety of operating platforms and development environments to ease integration and ongoing administration of applications that use encryption. It is also easily integrated into retail point-of-sale terminals, reservation systems, payment systems and other applications to protect sensitive information such as credit card magnetic stripe data and consumer data at point of entry.

Protect at the point of entry and throughout the information life-cycle

The capability to protect at the point of entry helps ensure that the information will be both properly secured and fully accessible when needed at any point in its enterprise information lifecycle. Regulatory compliance and industry security standards such as the PCI Data Security Standards DSS continue to motivate large corporations to develop and adopt an encryption strategy for their high-risk data stores and applications. Recent high-profile security breaches exposing personal identity information have made the need for better information protection obvious to the public. However, effectively implementing an encryption strategy has traditionally required application developers and data architects that possess a high level of security knowledge. Ongoing administration and management of encryption technology is also a major concern as more applications and data stores require it in order to protect data.

The Key Manager solution provides a secure storage of encryption keys. All keys in the key vault database are encrypted using a protected master encryption key. This multi-layer hierarchy of keys ensures the highest level of protection against attack with a hierarchy in which each key is protected by a parent key. Authentication and authorization for system administrators is performed using the included Access Manager.

Access Manager is designed to provide the necessary separation of duties and administrator roles required for strong security over the Key Manager system as well as to meet specific PCI standard requirements.

How to reduce the risk of memory attacks

Memory attacks may be theoretical, but cryptographic keys, unlike most other data in a computer memory, are random. Looking through memory structures for random data is very likely to reveal key material. Well made libraries for use as Local Encryption Services go to great efforts to protect keys even in memory.

Key-encryption keys are used to encrypt the key while it is in memory and then the encrypted key is split into several parts and spread throughout the memory space. Decoy structures might be created that look like valid key material. Memory holding the key is quickly zeroed as soon as the cryptographic operation is finished. These techniques reduce the risk of memory attacks. Separate encryption can also be used for different data. These encryption keys can be automatically rotated based on the sensitivity of the protected data. Dedicated Encryption Services are also vulnerable to memory attacks. However, a well made Dedicated Encryption Service runs only the minimal number of services.

Secure key backup

A weak link in the security of many networks is the backup process. Often, private keys and certificates are archived along with configuration data from the backend servers. The backup key file may be stored in clear text or protected only by an administrative password. This password is often chosen poorly and/or shared between operators. To take advantage of this weak protection mechanism, hackers can simply launch a dictionary attack (a series of educated guesses based on dictionary words) to obtain private keys and associated certificates. Private keys should never be exported from the product in clear text. The backup file should be password protected and then encrypted using an internal key.

When private keys are backed up from the solution platform, they should be encrypted twice, once using an administrative backup key and a second time with the internal Repository key. This type of key management makes it impossible for attackers to launch dictionary attacks and other password-guessing techniques aimed at exposing an administrative password and unlocking the backup file. Your private keys can never be exported in clear text and cannot be released without cracking several layers of triple-DES encryption, ensuring secure preservation of key data in all backup and storage activities.

A WEAK LINK IN THE SECURITY OF MANY NETWORKS IS THE BACKUP PROCESS.

An optional hardware security module when FIPS 140-2 Level 3 is required

Best practice - taking response time, added overhead and path length into account, that always occur invoicing a remote hardware routine invocations - network-attached encryption is to use the HSM for optional key management operations. This is the only general solution that proves to be scalable in an enterprise environment. The solution includes an optional, tamper-resistant hardware security module (HSM), including HSM's certified to FIPS 140-2 Level 3, the widely accepted standard of government-specified best practices for network security. Private keys are generated and stored in encrypted form within an HSM. Keys stored in the HSM are protected from physical attacks and cannot be compromised even by stealing the HSM itself. Any attempt to tamper with or probe the card will result in the immediate destruction of all private key data, making it virtually impossible for either external or internal hackers to access this vital information. If we compare the response time for a query on unencrypted data with the response time for the same query over the same data (some or all of it encrypted), response time over encrypted data will increase due to the cost of decryption as well as additional overhead and path length that always occur with a remote hardware routine invocations (Network-attached encryption). On z/OS there are ways to avoid this by using native z/OS silicon implementation of encryption algorithms.

Centralized control of all key management operations

The Key Manager solution provides a centralized administration of all key management operations across applications and data stores that employ encryption, to help simplify the deployment and ongoing administration of the overall encryption solution. Key life-cycle management includes policy-based key generation, retrieval, automated expiration, distributed and local caching, central archival and restoration, as well as audit logging.

It also includes robust fail-over and availability features to help ensure maximum uptime for critical applications that require access to keys. The solution the use of standard database technologies combined with strong security protections. And it eases implementation by presenting simple programming interfaces for developers, eliminating the need to understand keys or their management. This reduces development time as well as implementation risks.

A secure mechanism for key rotation

Data privacy solutions should also include an automated and secure mechanism for key rotation, replication, and backup. One easy solution is to store the keys in a restricted database table or file. But, all administrators with privileged access could also access these keys, decrypt any data within your system and then mask their intrusion/attack.

Database security in such a situation is based not on industry best practice, but on an employee honor code. If your human resources department locks employee records in file cabinets where one person is ultimately responsible for the keys, shouldn't similar precautions be taken to protect this same information in its electronic format? All fields in a database and different encryption keys do not need the same level of security.

With tamper-proof hardware and software implemented, the encryption being provided by different encryption processes utilizing at least one process key in each of the categories master keys, key encryption keys, and data encryption keys, the process keys of different categories being held in the encryption devices; wherein the encryption processes are of at least two different security levels, where a process of a higher security level utilizes the tamper-proof hardware device to a higher degree than a process of a lower security level; wherein each data element which is to be protected is assigned an attribute indicating the level of encryption needed, the encryption level corresponding to an encryption process of a certain security level.

With such a system it becomes possible to combine the benefits from hardware and software based encryption. The software-implemented device could be any data processing and storage device, such as a personal computer.

The tamper-proof hardware device provides strong encryption without exposing any of the keys outside the device, but lacks the performance needed in some applications.

On the other hand the software-implemented device provides higher performance in executing the encryption for short blocks, in most implementations, but exposes the keys resulting in a lower level of security.

Support for PCI Credit card key management requirements

The solution supports PCI key management requirements and helps companies meet these guidelines. A robust, open architecture leverages proven cryptographic toolkits and is built using industry-standard security practices and protocols. The product also integrates with other security technologies including authentication. Many companies facing the PCI compliance issue are wondering how they can enforce the PCI regulations without significantly increasing staff and IT costs.

With the potential result of non-compliance being severe damage to the financial health and the brand reputation of an enterprise, organizations want to protect themselves to the fullest while minimizing necessary costs.

After an initial PCI compliance audit is completed, there are a host of initiatives organizations should consider in order to stay in front of emerging security threats and evolving compliance mandates.

This session offers an overview of the PCI mandate, including which organizations are affected, which specific rules pertain to encryption, and an overview of encryption solutions that help address these mandates. Also included is a case study outlining a sample deployment, a set of best practices that ensure not only a successful PCI audit, but a sustained improvement in the security of sensitive data that can help mitigate the threats of data theft and its costly aftermath.

Conclusion

This paper presents experience from many years of research and practical use of cryptography for safeguarding information from the point of acquisition to the point of deletion. We use the key concepts of security dictionary, type-transparent cryptography, and propose solutions on how to transparently store and search encrypted database fields. We showed that the hybrid database encryption solution is the most successful offering for most application environments.

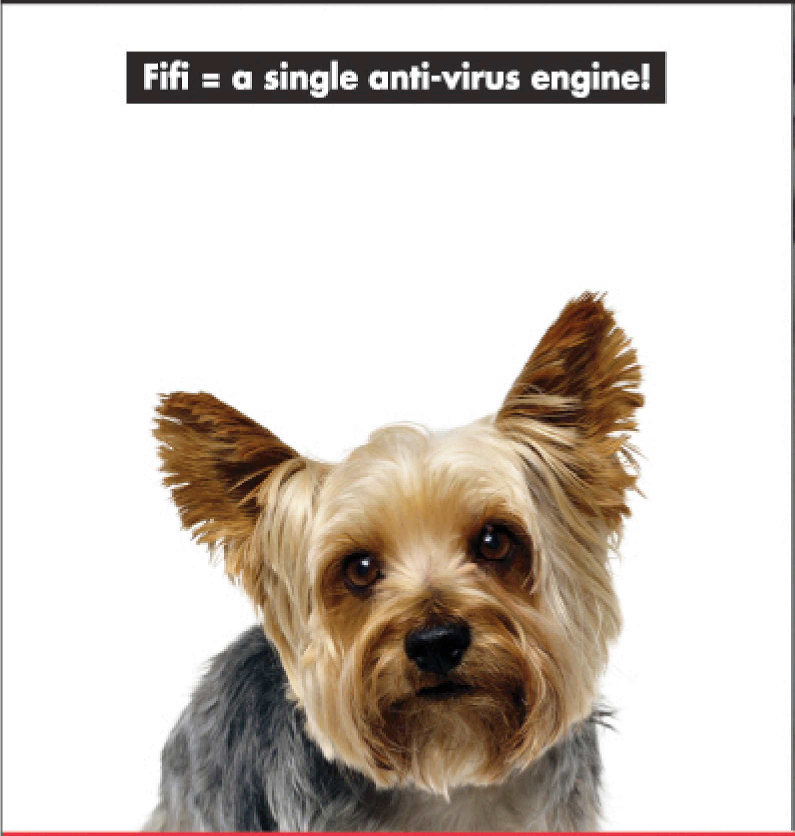
This paper presented a design principle that helps guide placement of functions for encryption and security enforcement among the modules of a distributed computer system. The principle suggests an enterprise approach to data protection. Whether you decide to implement encryption inside or outside the data store, we recommend that encrypted information should be stored separately from encryption keys, strong authentication should be used to identify users before they decrypt sensitive information, access to keys should be monitored, audited and logged, sensitive data should be encrypted end-to-end, while in transit in the application, and while in storage in enterprise data stores.

We present this solution as an example of a system that complies with these requirements, and provides a cost-effective implementation. Sensitive data is never in an unencrypted state at-rest on any of the systems, including temporary files and tables.

Ulf T. Mattsson is the CTO of Protegrity. Ulf created the initial architecture of Protegrity’s database security technology, for which the company owns several key patents.

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. Ulf holds a degree in electrical engineering from Polhem University, a degree in Finance from University of Stockholm and a master's degree in physics from Chalmers University of Technology

Who's guarding your Exchange Server?



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

GFi MailSecurity

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

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

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

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

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

GFi NETWORK SECURITY
CONTENT SECURITY
MESSAGING

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