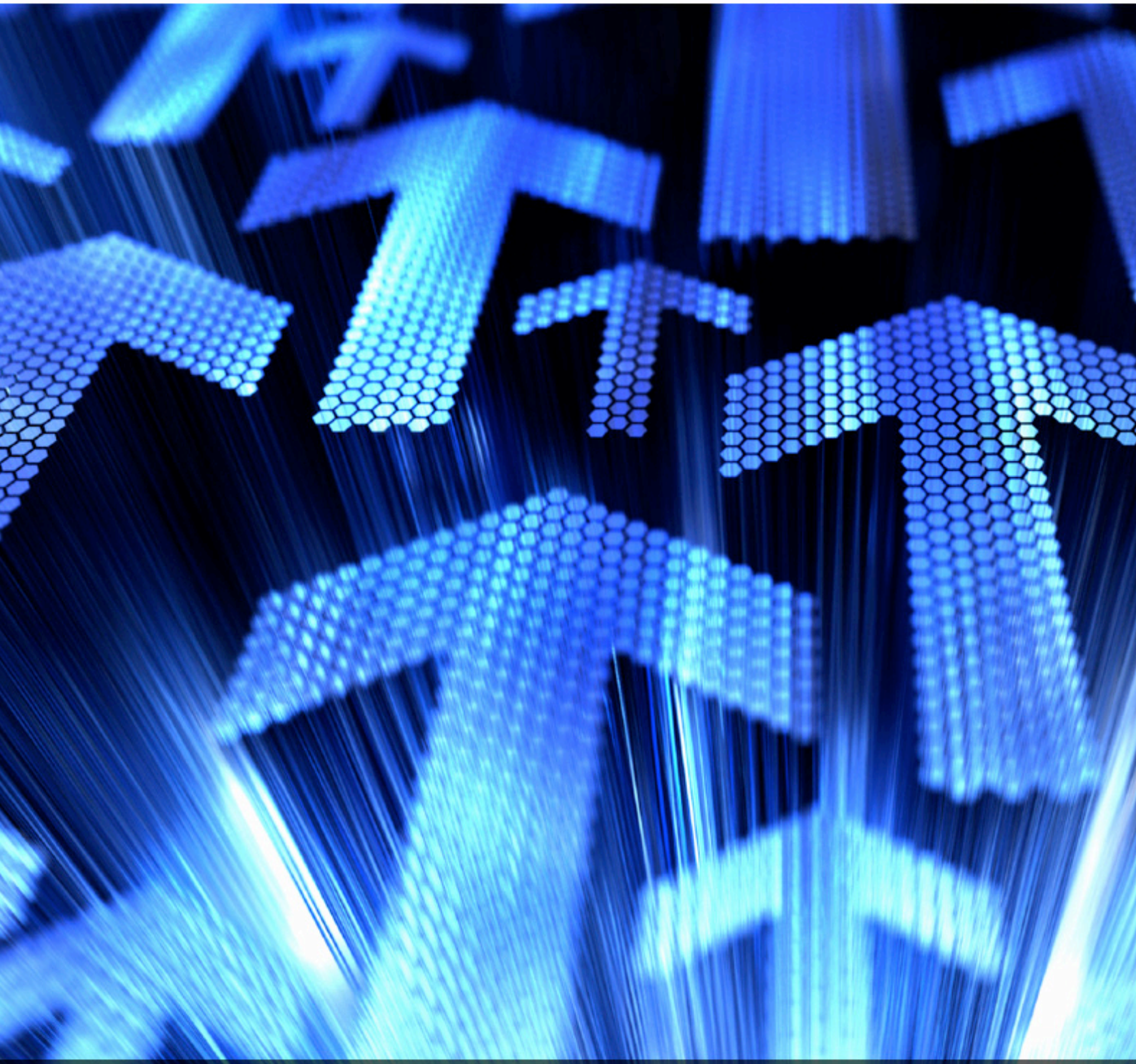
[IN]SECURE

OPEN. INFORMATIVE. TO THE POINT.

Issue 11 - May 2007



ON THE SECURITY OF E-PASSPORTS

QUANTITATIVE LOOK AT PENETRATION TESTING

SUPER NINJA PRIVACY TECHNIQUES FOR WEB APP DEVELOPERS

ENFORCING THE NETWORK SECURITY POLICY WITH DIGITAL CERTIFICATES

TABLE OF CONTENTS

It's a pleasure to see (IN)SECURE growing. We've seen a constant growth of both subscribers and downloads so this issue is packed full with more diverse material than ever, I'm sure you'll enjoy it.

If you're interested in writing for us do get in touch, we're always eager to publish fresh material from talented security professionals and enthusiasts.

Mirko Zorz
Chief Editor

Visit the magazine website at www.insecuremag.com

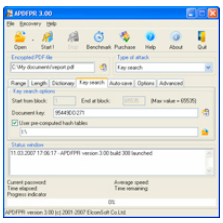
(IN)SECURE Magazine contacts

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

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

Distribution

Break 40-bit Adobe PDF encryption in minutes

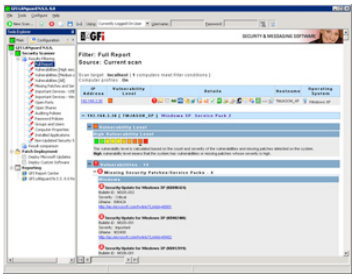


ElcomSoft released an Enterprise version of Advanced PDF Password Recovery. This program makes it easy to remove both password encryption and usage restrictions from Adobe Acrobat PDF files. APDFPR Enterprise now comes with support of all Adobe Acrobat versions up to 8.0, including those that use AES encryption, and super-fast guaranteed recovery of PDF files with 40-bit encryption using state-of-the-art “time-memory trade-off” technology. Advanced PDF Password Recovery Enterprise costs $999(US) for a single-user license and includes express delivery worldwide. (www.elcomsoft.com)

New ergonomic keyboard with built-in fingerprint reader

DigitalPersona has announced the availability of the DigitalPersona U.are.U Fingerprint Keyboard with new ergonomic design and built-in DigitalPersona placement optical reader. The new integrated keyboard has all of the accuracy, durability and convenience of a DigitalPersona U.are.U Fingerprint Reader, yet eliminates the need for desktop users to attach two USB devices such as a keyboard and fingerprint reader. DigitalPersona Pro Workstation Keyboard Package is priced at EUR 169. The DigitalPersona Pro Kiosk Keyboard Package is also priced at EUR 169. The Package includes one U.are.U Fingerprint Keyboard, one set of Pro Workstation or Kiosk for Active Directory software and one Pro Quick Start Guide. The DigitalPersona Pro Workstation software supports U.are.U Readers, U.are.U Keyboards and embedded fingerprint readers in most popular notebooks. (www.digitalpersona.com)

GFI LANguard Network Security Scanner 8 launched



GFI Software announced the release of GFI LANguard Network Security Scanner (N.S.S.) 8, the latest version of its award-winning solution that addresses the three pillars of vulnerability management: security scanning, patch management and network auditing in one integrated solution. GFI LANguard N.S.S. 8 is an essential, cost-effective solution for businesses to safeguard their systems and networks from hacker attacks and security breaches. The latest version of GFI LANguard N.S.S. has over 2,000 new vulnerability checks – using SANS top 20 and Open Vulnerabilities Assessment Language security definitions – over and above the vulnerabilities which are discovered through its inbuilt vulnerability assessment functionality. (www.gfi.com)

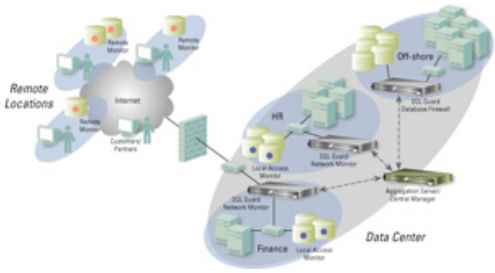
PGP upgrades its product portfolio

Currently shipping, all PGP Encryption Platform-enabled applications now support 32-bit editions of Windows Vista, in addition to existing support for Mac OS X, providing broad coverage across the most popular computer operating systems. The release also includes improved support for Lotus Notes users, increased support for additional European keyboards, and new technology to secure content on mobile devices and removable media such as USB flash drives. (www.pgp.com)

New Arbor Peakflow X 3.7 integrates threat analysis network data

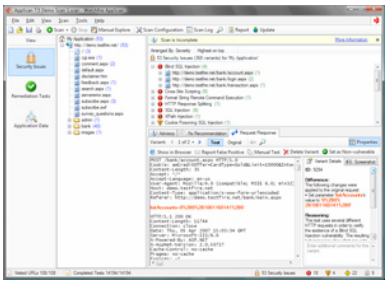
Arbor Networks announced a new version of its enterprise solution, Arbor Peakflow X 3.7, that includes new functionality designed to improve time to resolution for enterprise network, security and operations staff. The product includes integration of data gathered by Arbor's Active Threat Level Analysis System, the world's first globally scoped threat analysis network, dramatically reducing the manual collection and analysis of new vulnerabilities, exploits, botnets and malware. (www.arbor.net)

Guardium releases database leak prevention solution



Guardium announced a comprehensive solution for database leak prevention called Guardium DBLP. It automatically locates and classifies sensitive information in corporate databases, and prevents unauthorized or suspicious use based on proactive, real-time policies and continuous comparisons to normal activity. Guardium DBLP is the second in a series of solutions built upon Version 6.0 of the Guardium platform, the most widely-deployed solution for database activity monitoring, security, and auditing. Version 6.0 increases protection while leveraging automation and sophisticated data mining techniques to reduce manual efforts. (www.guardium.com)

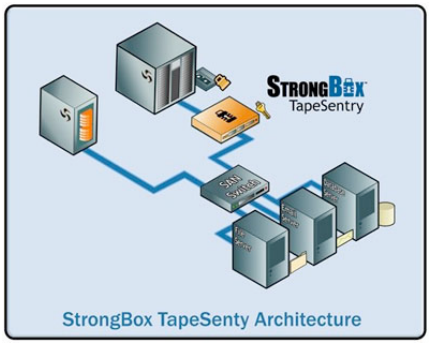
New version of AppScan web application security testing tool



Watchfire announced a new quality assurance edition of AppScan QA which introduces the latest web application security testing to the QA cycle, with new and enhanced integration with the industry's most popular software quality management solutions—HP Quality Center and IBM Rational ClearQuest. This new release complements Watchfire's web-based enterprise platform – AppScan Enterprise, a solution that enables organizations to scale application security testing into QA and development via a web-based system. (www.watchfire.com)

New StrongBox TapeSentry encryption appliance

Crossroads Systems announced its early adopter program for their' StrongBox TapeSentry solution, a new tape encryption appliance designed to protect data stored on tapes in the event of theft and loss. Crossroads' TapeSentry appliance delivers maximum security to stored data on tape media. As a high-performance, enterprise-class appliance, TapeSentry provides front-side compression and robust encryption at wire-level speed. TapeSentry provides industry-standard encryption algorithms, crypto-signed logging and robust key management to satisfy regulatory requirements and protect stored data from unauthorized data access or theft. (www.crossroads.com)



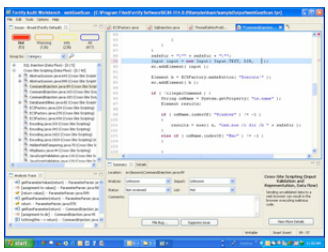
StrongBox TapeSenty Architecture

Secure Windows Vista compatible flash drive

EDGE Tech Corp announced the release of its DiskGO Secure Flash Drive Enhanced for ReadyBoost. This flash drive is the first in its market to offer secure, password-protected encryption software that is compatible with Windows Vista. Couple this compatibility with the speed and reliability of EDGE flash drives, and you have an all-in-one, drive guaranteed to see you through your Windows Vista upgrade transition and beyond. The drive features Vista-compatible Cryptarchiver software, which enables the user to choose between 448-bit Blowfish encryption and the government standard AES 256-bit encryption. (www.edgetechcorp.com)

Fortify Source Code Analysis Suite 4.5 released

Fortify Software announced the availability of Fortify SCA 4.5, which includes features that enable development, audit and information security teams to identify and fix security vulnerabilities early and with less effort. Fortify SCA 4.5 also adds more regulatory compliance reports to offer the most comprehensive details in the industry. Developers and security auditors will also reduce remediation time with a new analysis trace GUI that graphically represents security flaws discovered by the Fortify static analysis engine. (www.fortifysoftware.com)



The global introduction of electronic passports is a large coordinated attempt to increase passport security. Issuing countries can use the technology to combat passport forgery and look-alike fraud. While addressing these security problems other security aspects, e.g. privacy, should not be overlooked. This article discusses the theoretical and practical issues, which impact security for both citizens and issuing countries.

Existing legacy passports are paper based and use related security features. Despite of advanced optical security features paper based travel documents are sensitive to fraud. Two forms of fraud are most notable:

• Passport forgery: a relatively complex approach where the fraudster uses a false passport, or makes modifications to a passport.

• Look-alike fraud: a simple approach where the fraudster uses a (stolen) passport of somebody with visual resemblance.

The ICAO (International Civil Aviation Organization) has been working on what they call MRTD (Machine Readable Travel Document) technology for quite a while. This technology should help to reduce fraud and support immigration processes. The MRTD specifications became a globally coordinated attempt to standardize advanced technology to deliver strong identification methods. Rather then using common practices from the security industry the MRTD standards aimed at a revolutionary combination of advanced technology, including contactless smartcards (RFID), public key cryptography, and biometrics.

The MRTD specs support storage of a certificate proving authenticity of the document data. The signed data includes all regular passport data, including a bitmap of the holder's picture. Further data that may be stored in the e-passport include both static and dynamic information:

• Custody Information
• Travel Record Detail(s)
• Endorsements/Observations
• Tax/Exit Requirements
• Contact Details of Person(s) to Notify
• Visa

Since 2005 several countries have started issuance of e-passports. The first generation of e-passports includes some, but not all, of the planned security features. Biometric verification is generally not supported by the first generation. All 189 ICAO member states are committed to issue e-passports by 2010.

From 2007 onward immigration services will start using e-passports. Authorities promote e-passports by issuing visa-waiver programs for travelers with e-passports. A passport that conforms to the MRTD standard can be recognized by the e-passport logo on the cover.

Figure 1: The Electronic Passport logo.

Electronic Passport security mechanisms

With the aim to reduce passport fraud the MRTD specs primarily addressed methods to prove the authenticity of passport and its data, and the passport holder. The technology used for this includes PKI (Public Key Infrastructure), dynamic data signing and biometrics. The latter (biometrics) however is still under discussion and not yet fully crystallized in the specifications.

Passive Authentication

PKI (Public Key Infrastructure) technology was chosen to prove the authenticity of the passport data. This technology is successfully applied on the internet for e-commerce, and has gained high popularity. Certificate based authentication requires only reading the certificate by the inspection system, which can then use a cryptographic computation to validate the authenticity using the public key of the issuing country. This method is called passive authentication and satisfies with RFID chips without public key cryptographic facilities, since it involves only static data reading. Although the authenticity of the data can be verified, passive authentication does not guarantee the authenticity of the passport itself: it could be a clone (electronically identical copy).

Active Authentication

The cloning problem is addressed with an optional signing mechanism called active authentication. This method requires the presence of a asymmetric key-pair and public key cryptographic capabilities in the chip. The public key, signed by the issuing country and verified by passive authentication, can be given to the inspection system, which allows verification of a dynamic challenge signed with the private key. While the private key is well protected by the chip it effectively prevents cloning since the inspection system can establish the authenticity of the passport chip with the active authentication mechanism.

RFID

For the incorporation of modern electronic technology in the existing paper documents it was decided to use (contactless) RFID chips. These chips can be embedded in a page of the document and put no additional requirements on the physical appearance of the passport. A question that arises here is whether this is the only reason to apply RFIDs instead of contact based cards. Other reasons could be related to the form factor of contact smart cards which complicates embedding in a passport booklet, or the fact that contacts may be disturbance sensitive due to travel conditions. With the choice for RFID the privacy issue arises. RFIDs can be accessed from distances up to 30 cm, and the radio waves between a terminal and an RFID can be eavesdropped from a few meters distance. An adversary with dedicated radio equipment can retrieve personal data without the passport owner's consent. This risk is particularly notable in a hostile world where terrorists want to select victims based upon their nationality, or criminals commit identity theft for a variety of reasons.

Figure 2: Radio communication between inspection system and passport.

Basic Access Control

To protect passport holder privacy the optional Basic Access Control (BAC) mechanism was designed. This mechanism requires an inspection system to use symmetric encryption on the radio interface. The key for this encryption is static and derived from three primary properties of the passport data: 1) date of birth of holder; 2) expiry date of the passport; 3) the passport number. This data is printed in the Machine Readable Zone (MRZ) a bottom strip (see figure Figure 3) of one of the passport pages.

In a normal access procedure the MRZ data is read first with an OCR scanner. The inspection system derives the access key from the MRZ data and can then set up an encrypted radio communication channel with the chip to read out all confidential data. Although this procedure can be automated it sets high requirements to inspection systems and also impacts inspection performance.

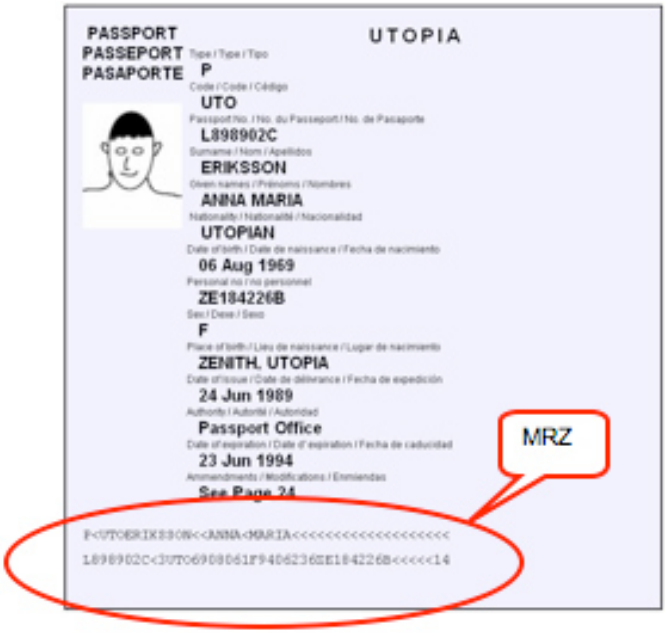


Figure 3: Passport with Machine Readable Zone (MRZ).

The BAC mechanism does provide some additional privacy protection, but there are two limitations that limit the strength of this mechanism:

• The BAC key is individual but static, and is computed and used for each access. An adversary needs to get hold of this key only once and will from then on always be able to get access to a passport's data. A passport holder may perceive this as a disadvantage considering the possibility that a passport contains dynamic data.

• The BAC key is derived from data that may lack sufficient entropy: the date of expiry is always in a window of less than ten years, the date of birth can often be estimated and the document number may be related to the expiry date.

The author of this article discovered BAC security issues in July 2005 and showed that the key entropy that could reach 66 bits may drop below 35 bits due to internal data dependencies. When passport numbers are for instance allocated sequentially they have a strong correlation with the expiry date, effectively reducing the key entropy. An eavesdropper would then be able to compute the BAC key in a few hours and decode all confidential data exchanged with an inspection system. The Netherlands, and maybe other countries, have changed their issuance procedures since this report to strengthen the BAC key.

An associated privacy problem comes with the UID (Unique Identification) number emitted by an RFID immediately after startup. This number, if static, allows an easy way of tracking a passport holder. In the context of e-passports it is important that this number is dynamically randomized and that it cannot be used to identify or track the e-passport holder.

The reader should note that these privacy issues originate from the decision to use RFID instead of contact card technology. Had this decision been otherwise the privacy debate would have been different as it would be the passport holder who implicitly decides who can read his passport by inserting it into a terminal.

Inspection system security issues

The use of electronic passports requires inspection systems to verify the passport and the passport holder. These inspection systems are primarily intended for immigration authorities at border control. Obviously the inspection systems need to support the security mechanisms implemented in an e-passport. This appears to be a major challenge due to the diversity of options that may be supported by individual passports.

In terms of security protocols and information retrieval the following basic options are allowed:

• Use of Basic Access Control (including OCR scanning of MRZ data)
• Use of Active Authentication
• Amount of personal data included
• Number of certificates (additional PKI certificates in the validation chain)
• Inclusion of dynamic data (for example visa).

Future generations of the technology will also allow the following options:

• Use of biometrics
• Choice of biometrics (e.g. finger prints, facial scan, iris patterns, etc)
• Biometric verification methods
• Extended Access Control (enhanced privacy protection mechanism).

In terms of cryptography a variety of algorithms and various key lengths are (or will be) involved:

• Triple DES
• RSA (PSS or PKCS1)
• DSA
• ECDSA
• SHA-1, 224, 256, 384, 512.

The problem with all these options is that a passport can select a set of preferred options, but an inspection system should support all of them!

An associated problem in the introduction of the passport technology is that testing inspection systems becomes very cumbersome. To be sure that false passports are rejected the full range of options should be verified for invalid (combinations of) values.

Finally, a secure implementation of the various cryptographic schemes is not trivial. Only recently a vulnerability was discovered by Daniel Bleichenbacher that appeared to impact several major PKCS-1 implementations. PKCS-1 also happens to be one of the allowed signing schemes for passive authentication in e-passports. This means that inspection systems should accept passports using this scheme. Passport forgery becomes a risk for inspection systems that have this vulnerability.

Immigration authorities can defend themselves against this attack, and other hidden weaknesses, by proper evaluation of the inspection terminals to make sure that these weaknesses cannot be exploited.

Biometrics and Extended Access Control

Biometrics

The cornerstone of e-passport security is the scheduled use of biometric passport holder verification. The chip will contain the signed biometric data that could be verified by the inspection system. It is only this feature that would prohibit the look-alike fraud. All other measures do address passport forgery, but the primary concern of look-alike fraud requires a better verification that the person carrying the passport is indeed the person authenticated by the passport. Many countries have started issuance of e-passports, but the use of biometrics is delayed. There are two main reasons:

• Biometric verification only works if the software performs a better job than the conventional verification by immigration officers. The debate on the effectiveness of biometric verification, and the suitability of various biometric features, is still ongoing. Also there are some secondary problems, like failure to enroll, that need to be resolved.
• Biometric data are considered sensitive. The threat of identity theft exists, and revocation of biometric data is obviously not an option. Countries do not necessarily want to share the biometric data of their citizens with all other countries.

The impact of first issue is decreasing in the sense that the quality of biometric systems gets better over time, although it may slow down the introduction of biometrics in e-passports. At least at this moment, there is still limited experience of representative pilot projects.

The second issue is more fundamental, issuing countries will always consider who to share sensitive data with. To alleviate these concerns the ICAO standardization body has introduced the concept of Extended Access Control.

Extended Access Control (EAC)

The earlier described Basic Access Control (BAC) mechanism restricts data access to inspection systems that know the MRZ data. EAC goes further than that: it allows an e-passport to authenticate an inspection system. Only authenticated inspection systems get access to the sensitive (e.g. biometric) data. Inspection system authentication is based upon certificate validation, (indirectly) issued by the e-passport issuing country. An e-passport issuing country therefore decides which countries, or actually: which Inspection System issuers, are granted access to the sensitive data. EAC requires a rather heavy PKI. This is for two reasons:

• Each Inspection System must be equipped with certificates for each country whose biometric details may be verified.
• Certificates should have a short lifetime; otherwise a stolen Inspection System can be used to illegally read sensitive data.

The current EAC specification foresees a certificate lifetime of several days. The two conditions above will result in an intensive traffic of certificate updates.

A problem acknowledged by the EAC specification is the fact that e-passports have no concept of time. Since the RFID chips are not powered in between sessions, they do not have a reliable source of time. To solve this problem, an e-passport could remember the effective (starting) date of validated certificates, and consider this as the current date. This could potentially lead to denial-of-service problems: if an e-passport accepts an inspection system's certificate whose effective date has not yet arrived, it may reject a subsequent inspection system certificate that is still valid. To avoid this problem the specification proposes to use only certificates of trusted domestic terminals for date synchronization.

Although date synchronization based on domestic certificate effective dates would give the e-passport a rough indication of the current date this mechanism leaves a risk for some users. Infrequent users of e-passports and users being abroad for a long time will experience that their e-passport date is lagging behind significantly. For example, if an e-passport has validated a domestic EAC capable terminal 6 months ago, it will reveal sensitive data to any rogue terminal stolen over this period.

The above problem could be alleviated by using a different date synchronization method. Instead of using effective dates of inspection system certificates we would use a separate source of time. For this ICAO, or another global Certification Authority, should issue date certificates on a daily basis, and inspection systems should load and update their date certificates frequently.

A passport could then use the date certificates signed by a trusted party to get a reliable, and more accurate, source of time. This approach could be better since we can also synchronize on foreign systems and we could use the current date in stead of the inspection system certificate effective date.

With respect to EAC and biometrics several practical and standardization issues are yet to be resolved. Although EAC, in its current specification, offers strong benefits over the simpler BAC it is certainly not a panacea, and there is room for improvement. Nevertheless, migration to biometrics in e-passports is needed to effectively combat look-alike fraud.

Conclusion

The global introduction of electronic passports delivered a first generation of e-passports that support digital signatures for document authentication. The system builds on the newest technology, and a high level of expertise is needed for a secure implementation and configuration of both the e-passports and the inspection systems.

The technology got increasingly complex with the decision to use contactless RFID technology. Additional security measures were introduced as a result of privacy concerns. But these measures appear to offer limited privacy protection at the cost of procedural and technological complexity.

The next generation e-passports will include biometrics and Extended Access Control (EAC). The standardization of these features is unfinished and could still be improved. Future e-passports, using all security features, will offer strong fraud protection:

• Passport forgery is more difficult with an e-passport that supports active authentication.
• Look-alike fraud is more difficult with an e-passport that supports biometrics.

This level of security can only be reached if all passports implement these features; otherwise fraudsters can fall back to less advanced or legacy passports.

Therefore it is important for ICAO to finalize the EAC standardization, and for issuing countries to continue the migration process and enhance their passports with biometrics.

Marc Witteman has a long track record in the smart card security industry. He has been involved with security and smart card projects for over a decade and worked on applications in mobile communications, payment industry, identification, and pay television. In 2001 he founded Riscure (www.riscure.com), a security lab based in the Netherlands. Riscure offers consulting and testing services to manufacturers and issuers of advanced security technology. Today he is the Chief Technology Officer of Riscure.

In late March, security and messaging company GFI released version 8 of their flagship product GFI LANguard Network Security Scanner. In this article you can read about scanning and patching - product's main functionalities, usage details and the overall experience I had with it.

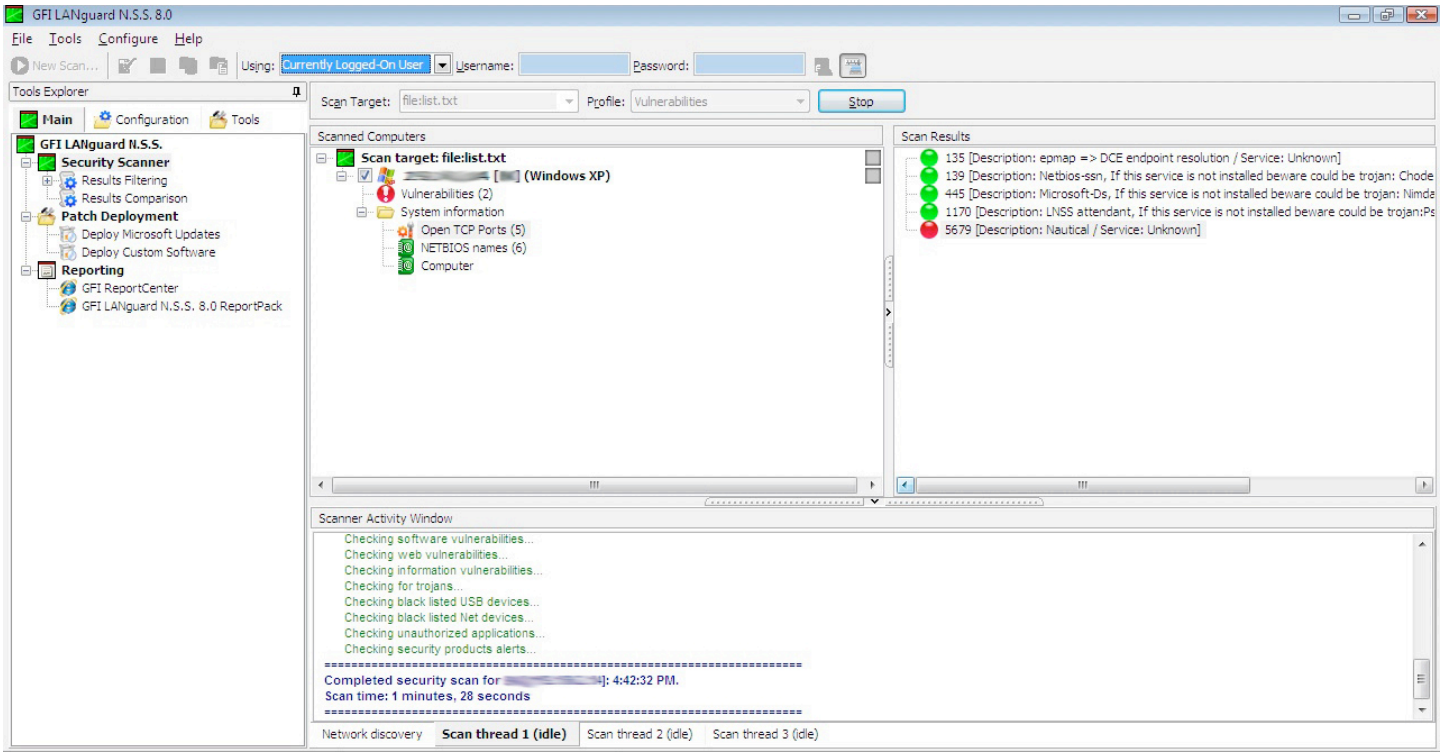
The new features in the version 8 include over 2,000 new vulnerability checks, a performance enhanced scanning engine and a highly intuitive graphical threat level indicator. Besides this, the latest version has received a variety of patch management improvements including added support to rollback Microsoft patches as well as technology to automatically download new Microsoft security patches when made available. It also supports scanning for vulnerabilities on Windows Vista-based systems.

Installation

As you will see from the screenshots, I run the software on multiple computers in my network, both Microsoft Windows XP and Windows Vista. The installation procedure took around 4-5 minutes and passed by without any problems.

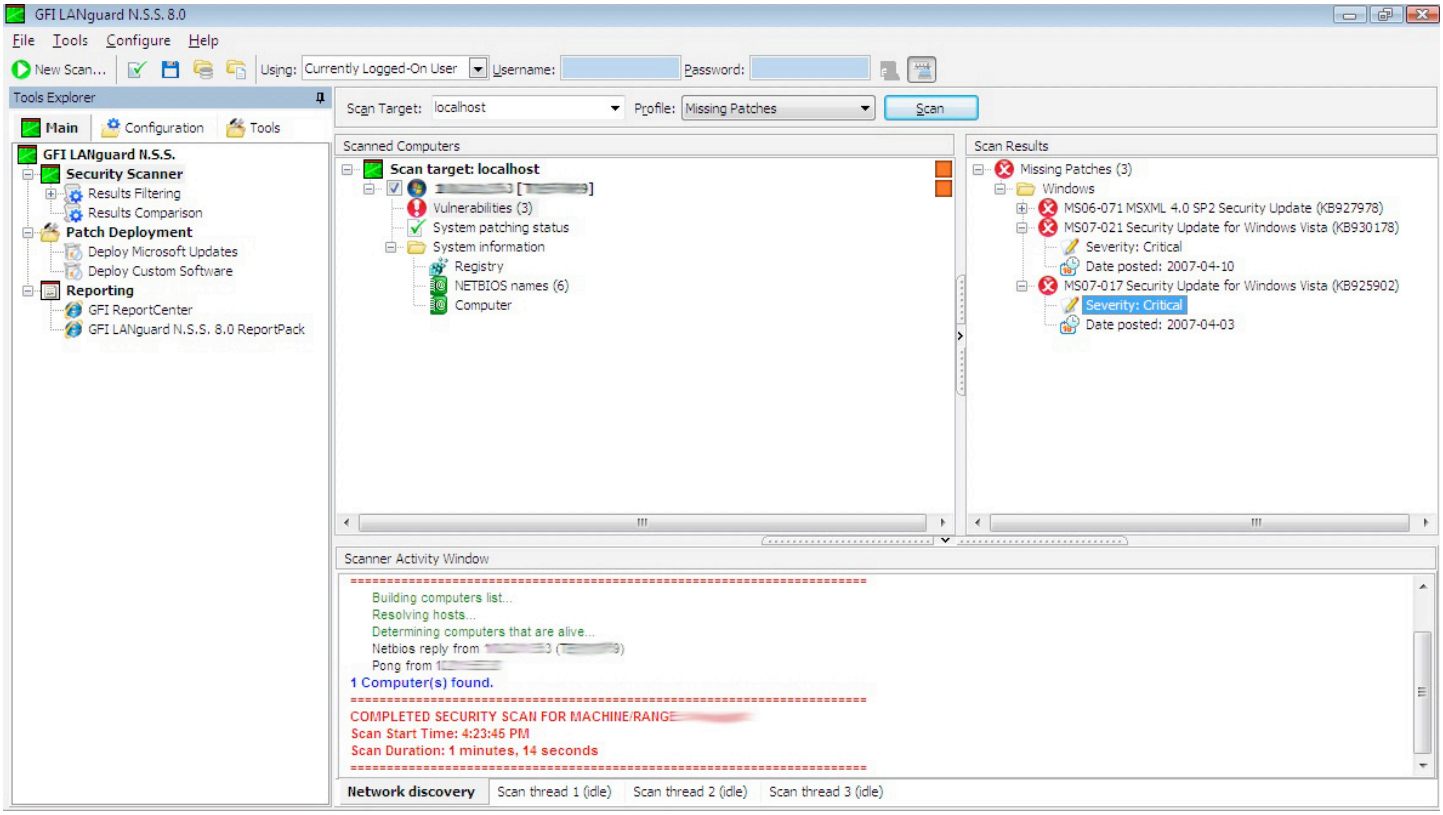
As the software is not just a typical security scanner as someone could think from its title, there are some interaction needed for completing the initial setup procedure. Although it is possible to install LANguard N.S.S with just hitting "Next" buttons, the product offers some good options that should be used.

The Attendant Service is the first option to set and it offers a way of doing automated scheduled scans. While you can enter any user name on the system, because of obvious reasons you should run the software under domain administrator account. LANguard N.S.S stores scanning information into a database, so you can chose between the default option of using Microsoft Access (never mind if you have it installed or not) or Microsoft SQL Server version 2000 or higher. For more complex networks the latter is recommended.



Windows XP computer scan results with emphasis on open ports.

One more thing you should think about are the e-mail settings alerts after successful scans. Besides the typical e-mail fields, the software supports both standard SMTP servers, as well as those that have authorization turned on. The final step of the pre-usage configuration lineup is aimed to users that don't have English version of the Microsoft Windows. As LANguard N.S.S has patching functions, users need to select the operating system languages used on the computers in the network.



Scan results showing critical vulnerabilities.

Scanning

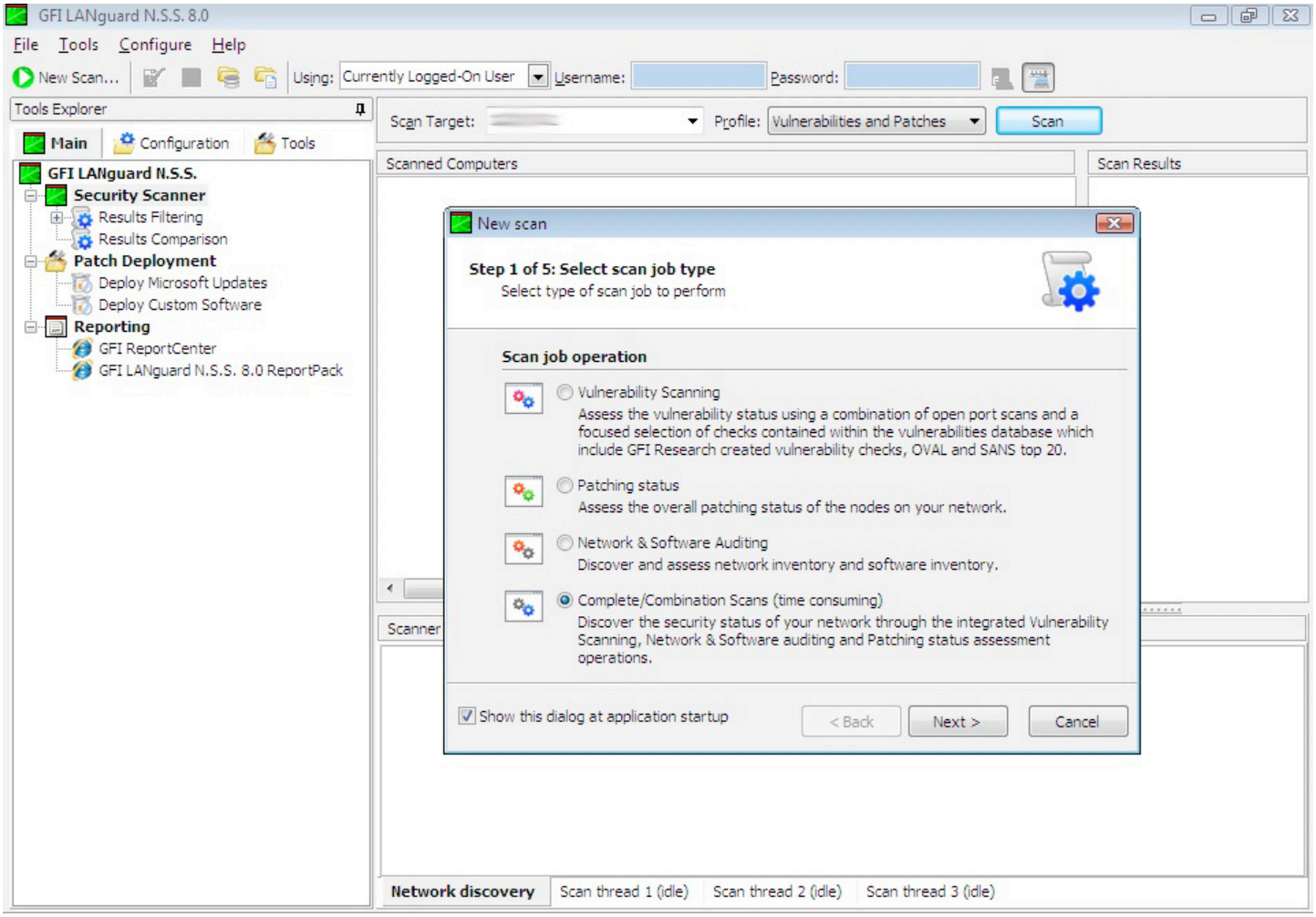
Every scan starts with a typical wizard. Because of a quite large scope of scanning options, wizard is divided into four different scan jobs:

Vulnerability Scanning - This was the option I used the most. While its function is pretty much self explanatory, there is an extra step in configuring this type of a scan which focuses on the specific scenarios you want to check out. Users that don't have a need to do a full vulnerability scan can chose from a couple of different scan profiles including Sans Top 20, SNMP, high security vulnerabilities and even trojan ports.

Patching Status - When exploring the status of Microsoft Windows patches in your network, you can chose between four profiles that will search for missing or critical patches, service packs and the modest scan of the last month's patches.

Network & Software Auditing - Through this option you will be able to scan all the network and software inventory. Scan profiles connected with it provide a line of useful checks for open ports, up time, connected USB devices and even a glimpse at disk space usage.

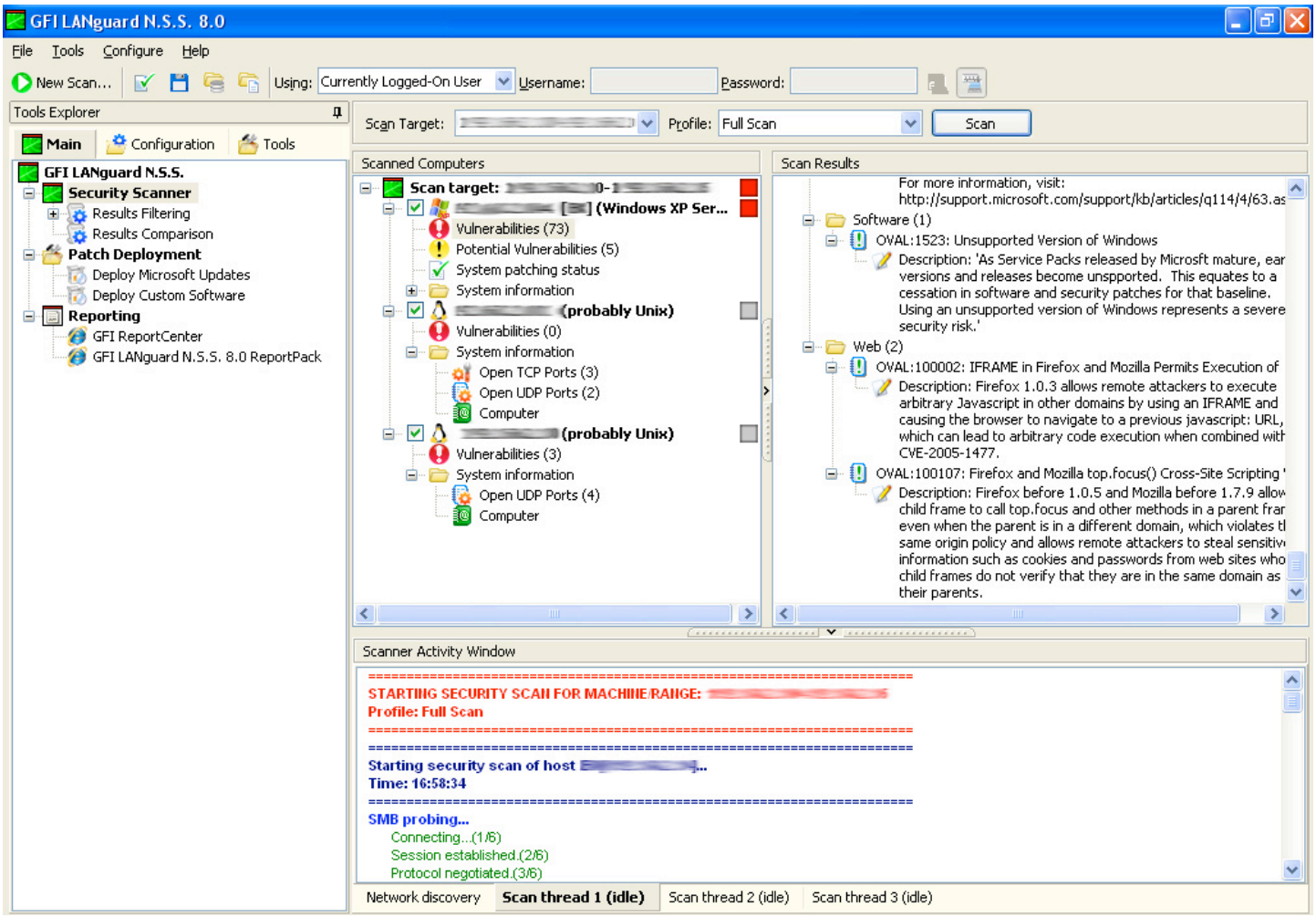
Complete/Combination Scans - Deep and thorough scans that incorporate all the previously mentioned scan jobs.



Different scan job types.

While I found all the scan jobs perfectly fitted for all the possible scenarios, it was really nice to see that the Configuration tab offers further customization opportunities. At the same time I was testing the software a new vulnerability was disclosed and majority of the machines residing on my network were affected by it.

I opened some specific attack signatures that were aimed to discovering a similar vulnerability and mangled with them a bit.



Description of security issues found on a computer in the network.

After 20 minutes of traversing through them I was able to create my own "update" which scanned the new vulnerability.

Patch deployment

From my perspective one of the main functions making GFI LANguard Network Security Scanner 8 a must have product is its powerful patch scanning and deploying mechanism.

As you all know, patch management is a tedious process, so automated scanning/patching solutions like LANguard N.S.S. could prove to be a life saver.

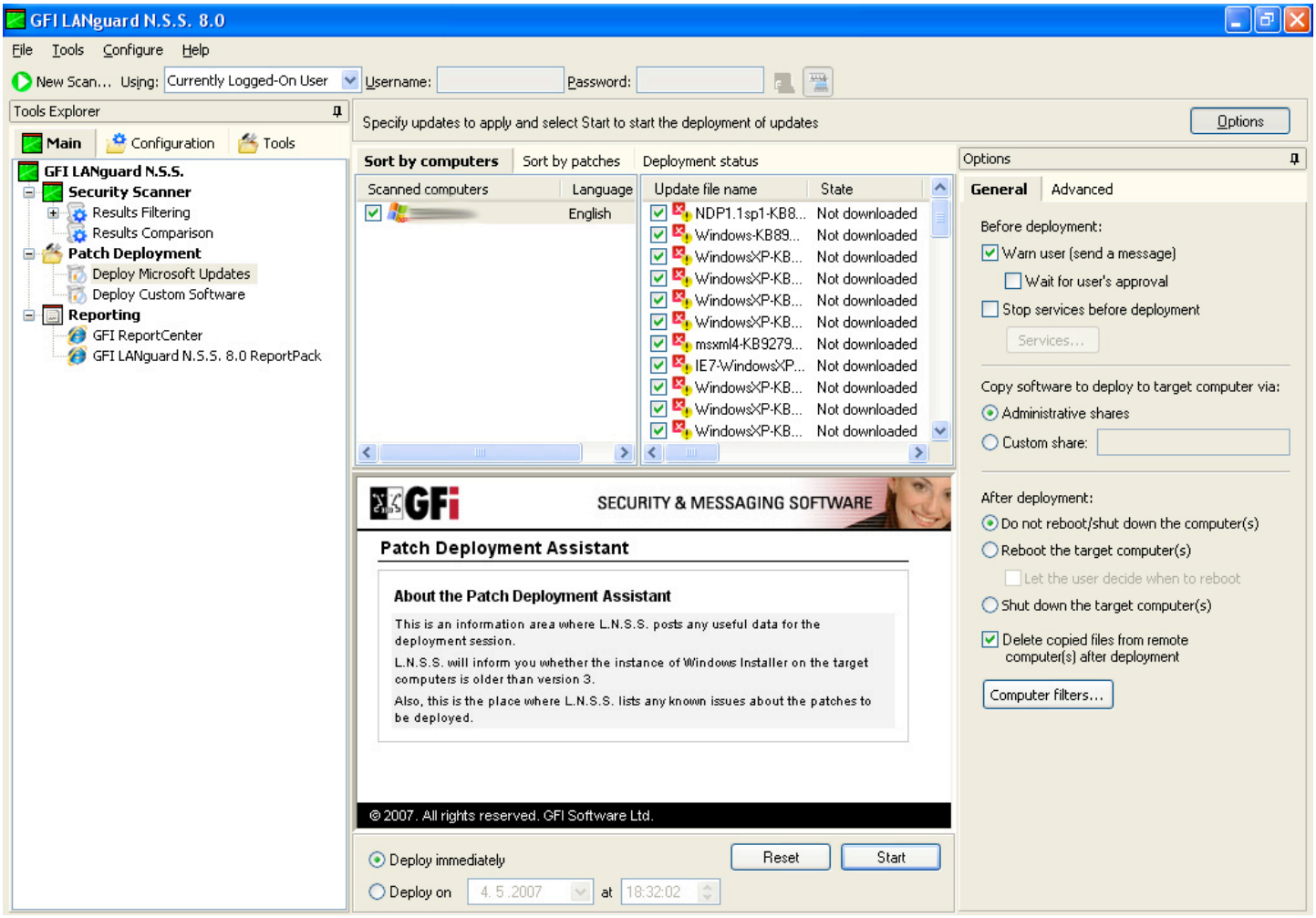
After the scan is done, the results are presented in the main console. It is easy to find out what computers are not up to date with the latest patches and with a click of a button administrator can push the new patches over the network. As a bonus to applying Microsoft updates, there is an interface that gives the opportunity of deploying custom software on remote computers.

Reporting

Besides getting all the information in the software console, there are a couple of additional ways of getting reports through GFI ReportCenter and a GFI LANguard N.S.S. ReportPack add-on. GFI ReportCenter is a centralized reporting framework that allows you to generate various reports using data collected by different GFI products.

The GFI LANguard N.S.S. ReportPack add-on is a full-fledged reporting companion to the software. This reporting package can be scheduled to automatically generate graphical IT-level and management reports based on the data collected during your security scans.

Although I have seen sample reports generated by the ReportPack (executive, statistical and technical) I wasn't able to thoroughly test this because the add-on needs a newer version of Microsoft .NET Framework which I don't have on my computers (company policy).



Patch deployment on a sample out of the box testing computer.

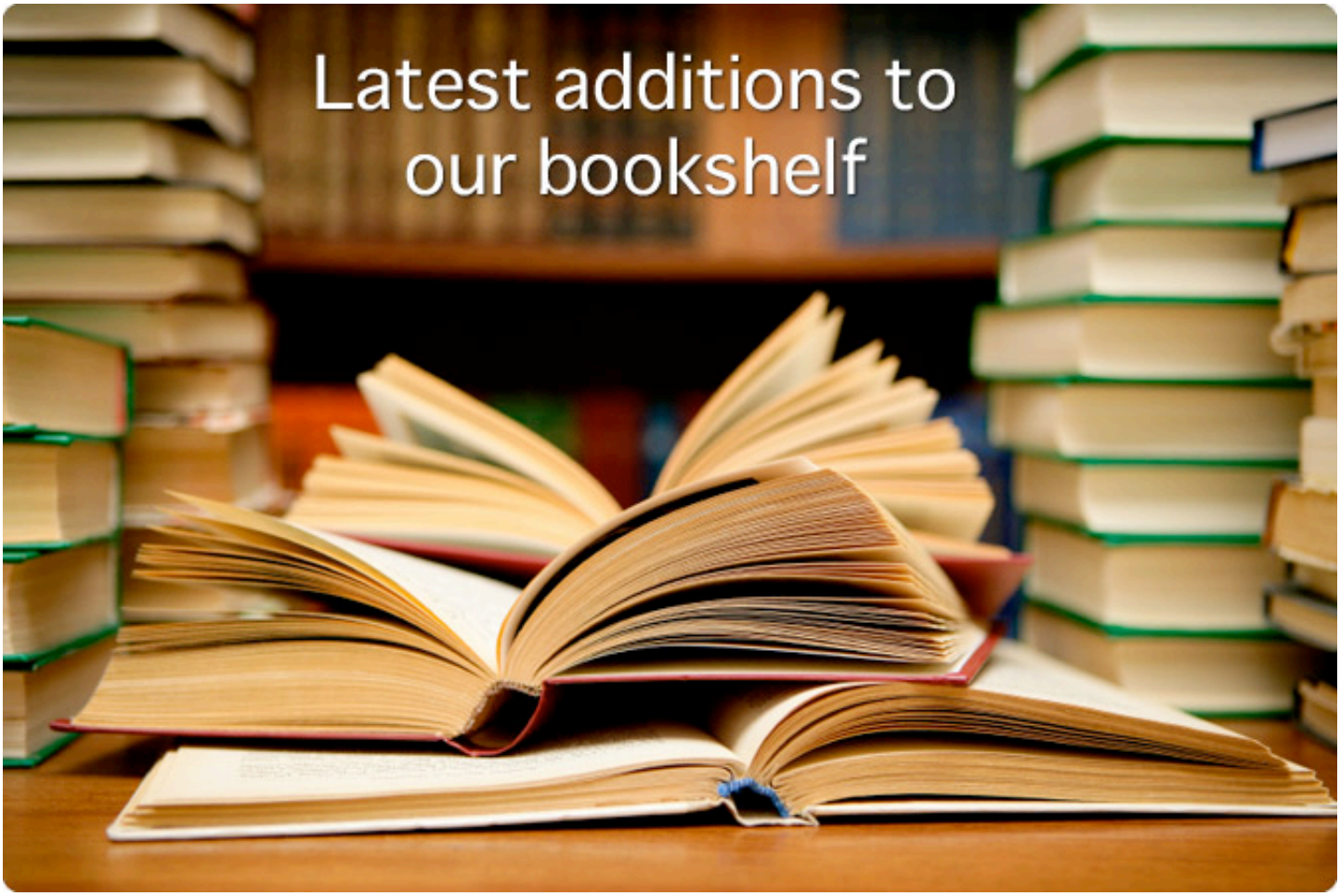
Nevertheless, reports are nicely done and the management people will surely like how the information is presented.

Final words

GFI LANguard Network Security Scanner 8 is a very fast, efficient and function filled security product that would surely be a great addition to any network and system administrators that work with Microsoft Windows computers.

To get a trial version head over to www.gfi.com/lannetscan/

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



Hacking Web Services

By Shreeraj Shah

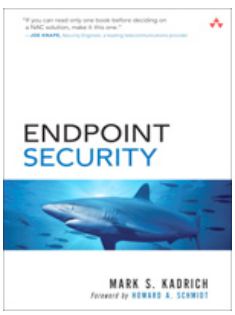
Charles River Media, ISBN: 1584504803

This is a practical guide for understanding Web services security and assessment methodologies. Written for intermediate-to-advanced security professionals and developers, it provides an in-depth look at new concepts and tools used for Web services security. Beginning with a brief introduction to Web services technologies, the book discusses Web services assessment methodology, the need for secure coding, and more. Throughout the book, detailed case studies, real-life demonstrations, and a variety of tips and techniques are used to teach developers how to write tools for Web services.

Endpoint Security

By Mark Kadrich

Addison Wesley Professional, ISBN: 0321436954

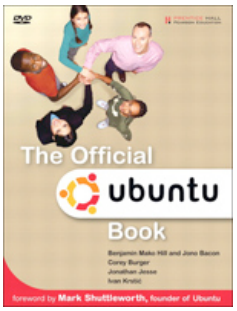


Drawing on powerful process control techniques, the author shows how to systematically prevent and eliminate network contamination and infestation, safeguard endpoints against today's newest threats, and prepare yourself for tomorrow's attacks. As part of his end-to-end strategy, he shows how to utilize technical innovations ranging from network admission control to "trusted computing." Kadrich presents specific, customized strategies for Windows PCs, notebooks, Unix/Linux workstations, Macs, PDAs, smartphones, cellphones, embedded devices, and more.

The Official Ubuntu Book

By Benjamin Mako Hill, Jono Bacon, Corey Burger, Jonathan Jesse, Ivan Krstic

Prentice Hall, ISBN: 0132435942



In recent years, the Ubuntu operating system has taken the Open Source and IT world by storm. Written by leading Ubuntu community members, the book should teach you how to seamlessly install and customize Ubuntu for your home or small businesses. It covers every standard desktop application all the way to software development, databases, and other server applications. “The Official Ubuntu Book” comes with a version of Ubuntu that can run right off the DVD, as well as the complete set of supported packages for Ubuntu, including Kubuntu.

Cisco Firewall Technologies (Digital Short Cut)

By Andrew Mason

Cisco Press, ISBN: 1587053292

Cisco Firewall Technologies provides you with a no-nonsense, easy-to-read guide to different types of firewall technologies along with information on how these technologies are represented in the Cisco firewall product family. The main Cisco products covered are the IOS Firewall, the PIX Firewall, and the ASA. The majority of focus for the Short Cut will be on the ASA and emphasis will be placed upon the latest functionality released in version 7.2. The Short Cut also provides a walkthrough for configuring the ASA using the Adaptive Security Device Manager (ASDM), the GUI management and configuration tool provided with the ASA. The Short Cut presents you with the background information and product knowledge to make qualified decisions about the type of firewall technology that best fits your working environment.

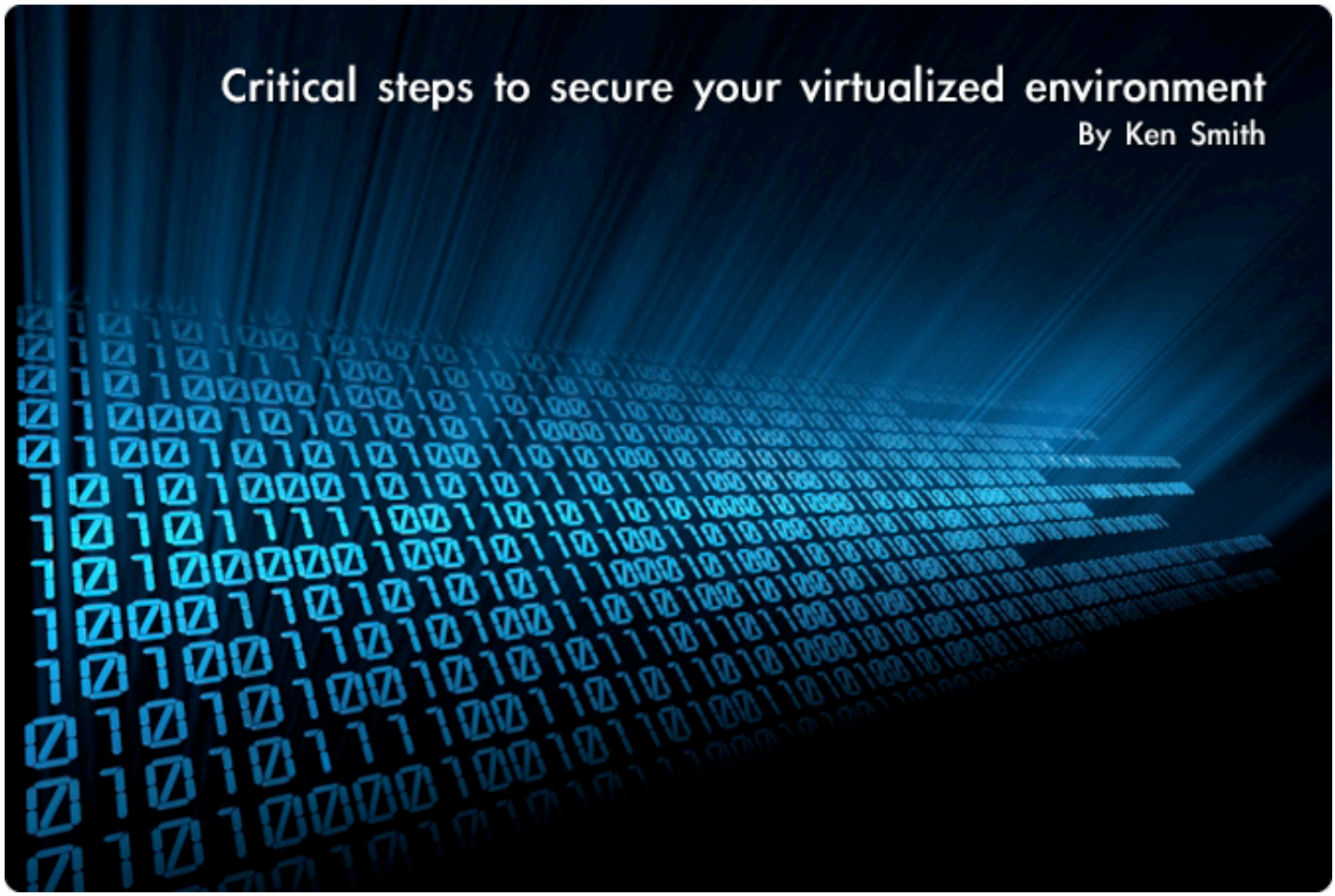
Deploying Zone-Based Firewalls (Digital Short Cut)

By Ivan Pepelnjak

Cisco Press, ISBN: 1587053101

Deploying Zone-Based Firewalls teaches you how to design and implement zone-based firewalls using new features introduced in Cisco IOS release 12.4T. This digital short cut, delivered in Adobe PDF format for quick and easy access, provides you with background information on IOS Firewall Stateful Inspection and Zone-based Policy Firewall configuration.

The Short Cut then focuses on designing zone-based firewalls and deploying zone-based policies with the new Cisco IOS command-line interface (CLI). Common deployment scenarios are included to highlight proper use of this powerful Cisco IOS feature.



Critical steps to secure your virtualized environment

By Ken Smith

Virtualization is one of the hottest technologies in the data center today, and with good reason. The benefits are clear. Virtualization can help reduce the physical space of the data center, lower hardware, software support and facilities costs, increase speed to deploy new servers and applications and enhance disaster recovery and business continuity.

As is the case when introducing any new technology it is important to have a strong understanding of how virtualization will impact your environment and all of the applications you are running. It is important to understand how virtualization may change your level or risk.

For example, if the virtual server running a web site were compromised, could the attacker continue to compromise other virtual servers on the same host undetected by network intrusion detection? There are certainly ways to leverage virtualization without increasing risk, but it's important to recognize these potential challenges and safeguard against them.

Below are a few security concerns and best practices to keep in mind as you virtualize your IT environment.

1) Ensure your software vendors provide full support for applications running within a virtualized environment - It's best to figure this out before you move an application to a virtualized environment, instead of when you need help troubleshooting an issue, especially if the application in question is mission-critical. Talk with your vendors about support options, before making the switch.

2) Update your written security policies and procedures to account for virtualization - You will now have multiple virtual systems running on the same physical server using the same physical data storage, memory and peripheral hardware such as network interface controllers.

You need to update your security requirements and policies to allow these resources to be shared in such a manner.

3) Always secure the host virtual machine - It's very important that the virtual server host operating system be locked down following the appropriate guidance for that operating system. For VMWare Infrastructure, for example, the guest Operating System is based on Linux, so it should be locked down in accordance with best practices and your corporate standards and requirements.

4) Institute appropriate access control - Since virtualization provides the opportunity to completely control a machine remotely, appropriate access control measures must be implemented to limit the risk of inadvertently shutting down, rebooting or deleting a machine. Filesystem permissions for virtual machine images also need to be stringent and consistently monitored and audited. Virtual server configuration settings such as network configuration settings should also be restricted.

5) Build Virtual DMZ's - For systems deemed to be safe for virtualization, the virtual servers that run together on the same hardware platform should share similar security requirements. Think of these systems as being together on a virtual DMZ network. The virtual machines will likely exist on the same subnet and may communicate with each other to handle transactions. It is preferable to configure hosts in this manner so that they do not need to traverse an external firewall (separate physical system) to communicate with each other.

6) Make network intrusion detection and prevention changes - If multiple virtual machines are using the same network interface cards, keep in mind the extra bandwidth that will be traversing that card. Before you may have had separate servers, each with Gig interfaces, peaking at 80 MB/sec of traffic. Now you will have a Gig interface peaking at 480 MB/sec if you run 6 virtual machines. Your network intrusion protection system may need to be re-architected slightly to keep up with the new demands of this single port.

7) Understand the impact to incident response and forensics plans - When introducing virtual systems into an environment, things like incident response need to be handled a little differently. Your incident response plan must now account for other systems running on the same virtual host. Immediately separate the suspect virtual machine from the others to ensure proper containment. Your system image acquisition process will also need to take into account the differences between nonvirtual and virtual systems.

8) Host intrusion detection and prevention - Host intrusion protection should continue to be in place as it would with a stand-alone server. Be sure to test your intrusion detection and prevention software within the virtual environment. Check with your vendor to be sure it is officially supported when running in a virtual environment.

Critical network and security infrastructure systems should remain on dedicated servers.

Does it always make sense to virtualize?

Critical network and security infrastructure systems should remain on dedicated servers.

It is important to keep critical authentication and directory services on dedicated systems. In most cases Active Directory domain controllers, RSA authentication manager servers, and RADIUS servers should not be run in a virtualized environment. However, there are exceptions to this, especially with regards to disaster recovery initiatives.

Although some firewall vendors are beginning to provide virtualization-ready solutions, it is best to hold off on virtualizing your firewall servers for now. While the idea of hosting multiple firewalls as virtual servers on a single host is appealing, you are likely running multiple firewalls that serve very different needs—with different security policies and rules. Keep these systems on their own servers for now.

Ken Smith is the Principal Security Consultant at Akibia (www.akibia.com).

Howard Schmidt has had a long distinguished career in defense, law enforcement and corporate security spanning almost 40 years. He has served as Vice President and Chief Information Security Officer and Chief Security Strategist for eBay.

He was appointed by President Bush as the Vice Chair of the President's Critical Infrastructure Protection Board and as the Special Adviser for Cyberspace Security for the White House in December 2001. He assumed the role as the Chair in January 2003 until his retirement in May 2003. Prior to the White House, Howard was CSO for Microsoft, where his duties included CISO, CSO and forming and directing the Trustworthy Computing Security Strategies Group.

At the moment you work as a consultant for governments of several countries. What do you see them most worried about in general?

While attacks on government systems is on many leaders minds, there is a high priority on the effect that cyber crime would have on their nations ability to participate in the benefits derived from increasing online e-commerce.

Their worry comes in two ways:

1) Criminals in their nations who are committing crimes online that give the country an unfair reputation of being a haven for cyber criminals.

2)The ability to investigate situations where their citizens fall victim to online crime and in turn do not trust the internet which in turn reduces their confidence in building a more robust ICT environment.

In the past you served as the CSO for giants such as Microsoft and eBay and you also worked for President Bush. What have been your biggest challenges while in such important positions?

The biggest challenges have been:

1) Convincing owners and operators of ICT/ Critical Infrastructure that they are a part of a biggest "eco-systems" and while they may be willing to accept certain risks around security, their risks may affect others as the interdependencies are not always very pronounced.
2) Getting people to realize that data is the "new currency" of the online world and protecting the data should be one of the highest priorities of any enterprise.
3) Having people understand that cyber security is NOT someone else's problem that we all have a role in securing cyber space.

Based on your experiences, is there more security in the private or government sector?

This varies from government to government as much as it does from private sector companies to each other. What I see today is both sectors are looking for ways to improve security in a cost effective way that does not reduce privacy and have negative affect on their "businesses". As far as investment goes, there seems to be a greater investment by private sector as a percentage of IT spend.

Are compliance laws taking the enterprise to a positive security level?

As much as many of us to not care for additional regulation, we are seeing a positive impact on security as compliance is linked directly to good governance and risk management which now have moved the discussion into the boardroom and the "C" suite.

What do you see as the biggest security threats today in general?

1) Insufficient application security through development shortfalls
2) Not sufficiently protecting data and data leakage through lack of content protections
3) Lack of end point security and lack of automated access controls that do not protect against "zero day" exploits.
4) Lack of widespread use of encryption which still leaves data vulnerable.
5) Attacks on mobile and wireless devices.
6) "Out of band" attacks to steal personal information.

Where do you see the current security threats 5 years from now? What kind of evolution do you expect?

While is always difficult to predict the future, I see many of today's threats being mitigated by building many of the technologies and processes into day to day IT functions both at the enterprise and the consumer level. The evolution of threats will still be directed at the end user based on the premise that the weak link in security is the human interaction.

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

Much of the data that has been accumulated over decades has been dispersed to so many different systems that locating and securing the data is the biggest challenge.

What do you expect from the future? Is it likely for a high-profile "cyber-terrorism" event to take place in the next 12 months or do you see it as media hype?

While the potential for a significant cyber security event to occur, I do not use the term "cyber-terrorism" to talk about high profile security events.

We have made cyber security a global priority which reduces the chance that an event that has a negative impact on ICT less likely. That is not to say we will not continue to deal with worms, Trojans and other malware that might be "high profile" but of limited impact overall.

I do not see discussions about this as "media-hype" as the media is not the only group that talks about the potential. It is a valid debate to have as long as people don't loose track of the hard work that has been done the past 5 years to make this less likely.

Since 2004 Matta has been running a project to test the technical competence of security consultants. With probably the largest collection of data on the methodology's and technical approach taken by some of the worlds best known security companies, some interesting conclusions can be drawn. The tests started as a result of a client asking for our assistance in running an RFP. The programme grew from there as other companies became interested in doing the same thing. In 2006, Matta provided Royal Holloway University with a version of Sentinel to make the country's first Penetration Testing vulnerable network for its students.

As there is a lot of data, the conclusions you reach will really depend on what you are looking for in the first place. I've documented in this article some of the things which I feel may be of general interest.

I would like to preface this article by saying that it is human nature to find the bad news more interesting than the good news. In our tests, we saw many impressive consultants. We tested companies which acted professionally and competently throughout, and there are consultancies who we admire and respect as a result of working either directly or indirectly with them. Many other companies could have set up the Sentinel program, and we don't place ourselves higher than our peers. It just so happened that it was Matta that was asked to do it. Typically, the clients who have run Sentinel programs, are either looking for a global Penetration Testing supplier - which Matta is not - or they are running internal accreditation schemes. Our reports have always been considered objective, and if we have something subjective to say, it goes on a separate page in the report, which is marked as a subjective observation.

Looking at some findings then, the first, and perhaps the most startling fact of all is that every consultant who has gone through the test has always found vulnerabilities with their tools, which then failed to make it on to their final report.

We sniff and log all the network traffic during the test, and are often required to demonstrate to the vendor that they did indeed find the issue, which was then absent on their report.

Clearly, there is a real problem with time limited tests, and the work required to go through reams of unqualified data to sort out the real issues from the false positives. Things just get missed. Importantly it seems, at least in our tests, something gets left out on every occasion. Our tests are intense, and time limited, so perhaps a fair conclusion to reach is that if the consultant is similarly under pressure, either internally, or from the client, then expect to get incomplete results. In some cases though, we also feel that the consultants would probably have missed the vulnerabilities regardless of the time limit. We believe that the output from some common tools is not so easy to read for those with less experience.

Second, and for me the most baffling observation, is that some consultants - a small minority - but enough to be significant, don't seem to read their briefing notes. This is really concerning. Each test we run has an engagement protocol. The vendor is given a set of briefing notes, with key information, including perhaps some login credentials to a web application, or a request to treat a database exactly as if it were a production system.

SOME CONSULTANTS DON'T SEEM TO READ THEIR BRIEFING NOTES. THIS IS REALLY CONCERNING.

So whilst most consultants had no trouble executing the tests with these instructions, one consultant repeatedly crashed the database to get debug information. Not something you would want do on a production database! On a similar note, we did hear a real life story from a client, in which a penetration tester had tried to drop a database to prove he had effected a compromise. Fortunately, due to mitigating factors, he was unable to drop it, but the client was less than happy, and I don't believe they required his services again.

Another consultant on our test, ran the password cracking tool, John the Ripper, on a system he was required to treat as production. He used 100% of the CPU for 24 hours on our 'production' server trying to crack the password. The sad thing was that the password was blank, and he never cracked it. His report stated that our password policy was very robust.

A further example with passwords was someone who spent hours trying to crack a password on an application, when the objective was privilege escalation, and the username and password were given to him in the briefing document. If only he had read it!

Most consultants of course, actually do read the briefing notes, and follow the instructions as you would expect, but if you're engaging with a new vendor, it certainly pays to make no assumptions.

Third, every vendor has a methodology statement, and clearly some follow it, but actually we find many do not. This is one area, I believe we as an industry can do much better. The old UK government CHECK approach is a good one, and anyone can follow it regardless of whether you have CHECK accreditation or not. I believe that many vendors are not active enough in ensuring their adopted methodology is followed. Typically, some of the issues we have seen include:

• missing issues, because the consultant has not stepped through it in a logical and progressive manner
• going in too 'deep' because the consultant gets excited about some vulnerability they've found, but then forgets, or runs out of time to do some of the basics
• running exploits, changing passwords, etc, and failing to clean up afterwards. In the real world we have been on incident response calls where the 'hacked host' was just the result of a previous security consultant failing to clean up after an assessment.

As I mentioned before, there are companies out there who we admire and respect. We have worked with companies who were pinging our network, waiting for us to open the firewall to them and start the test. They worked round the clock, were courteous, communicated with us when necessary, and didn't stop until we closed the connection at the end of the test. Then there were those that started late, and finished at 5 p.m. on the dot, even though they still had much more to do. There were those that read the briefing notes, and those that didn't. Those which scanned all 65k+ ports, and those which did a quick scan only.

All consultants and vendors are not equal. Some of the less competent vendors are nevertheless good at selling their services to clients who may not be aware how to judge the difference. More often nowadays we see companies choosing their Penetration Testing vendors based on incorrect metrics, such as accreditations of varying value, and of course on price. My hope is that an independent body of technically competent people with experience in Penetration Testing, but who are not vendors, set up a program which works in a way similar to how we have run Sentinel, and to award technical accreditations to individual consultants, not companies, in a range of technical security assessment areas. Until then, as a vendor, we'll continue to be put under pressure to 'buy' every new PCI, CISSP,CREST, CEH, et all accreditation to be competitive in the market, and most companies will continue to operate in the dark without a set of good, industry standard, technical metrics to guide them.

Nick Baskett is Managing Director of Matta (www.trustmatta.com), a security consultancy and software company based in Richmond on Thames, London.

WINDOWS - LockNote
http://www.net-security.org/software.php?id=649

LockNote will change the way you work with confidential notes. Application and document in one: the mechanism to encrypt and decrypt a note is part of it. Secure, simple, independent. No installation required.

LINUX - MailScanner
http://www.net-security.org/software.php?id=144

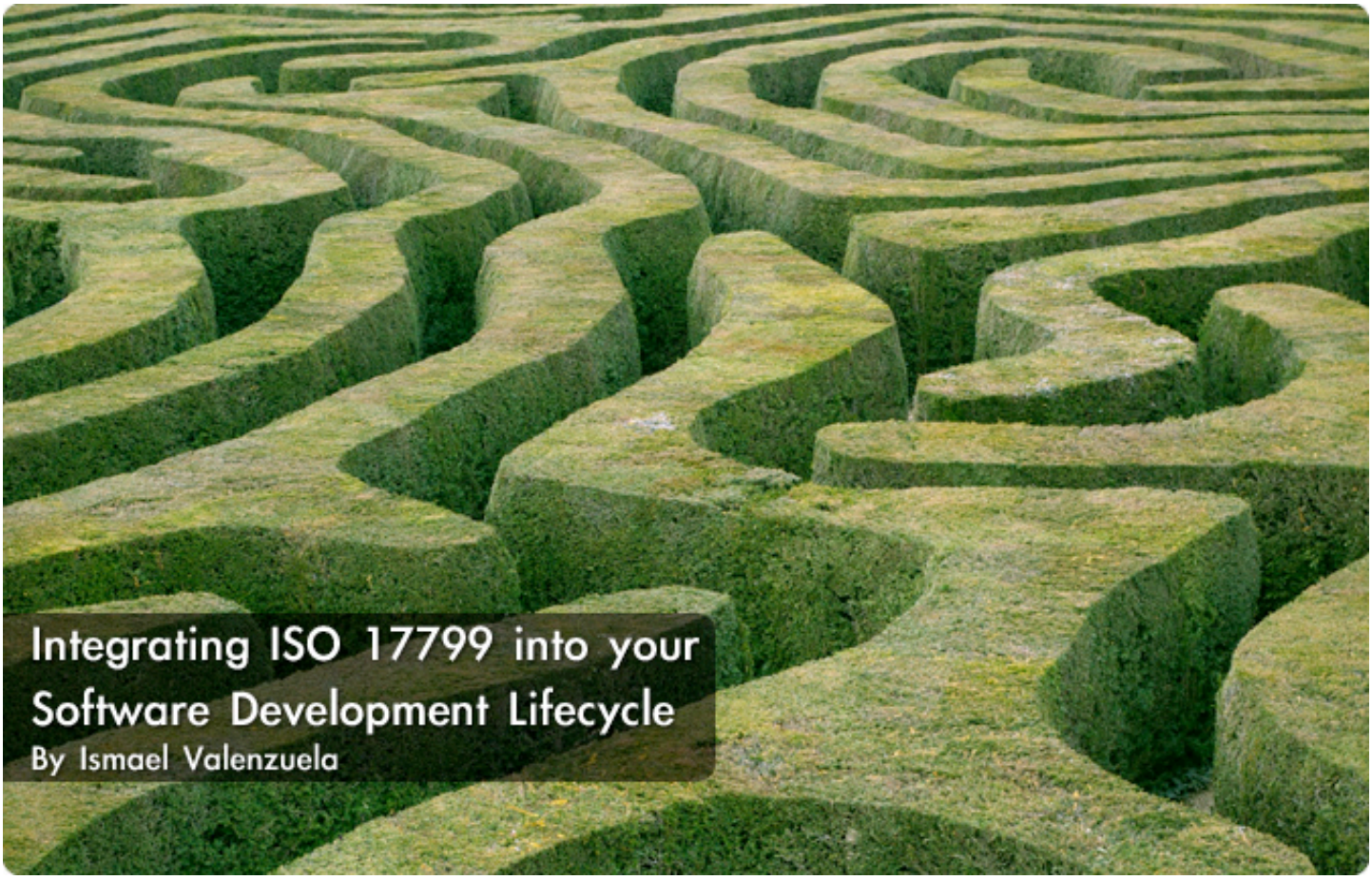
MailScanner is a virus and spam scanner for e-mail designed for use on e-mail gateways. Not only can it scan for known viruses, but it can also protect against unknown viruses hidden inside e-mail attachments by refusing entry to attachments whose filenames match any given pattern.

MAC OS X - Radmind Assistant
http://www.net-security.org/software.php?id=630

A suite of Unix command-line tools and a server designed to remotely administer the file systems of multiple Unix machines. For Mac OS X, there's also a graphical interface.

POCKET PC - SecuBox for Pocket PC
http://www.net-security.org/software.php?id=543

Reliable and user-friendly encryption software for Pocket PCs. It encrypts all sensitive information keeping it secure and protected, even in such catastrophic cases when the Pocket PC is lost or stolen. Protects information with NIST-approved AES 256-bit encryption.



Integrating ISO 17799 into your Software Development Lifecycle

By Ismael Valenzuela

It is a well-known fact in computer security that security problems are very often a direct result of software bugs. That leads security researches to pay lots of attention to software engineering. The hope is to avoid the ever present penetrate-and-patch approach to security by developing more secure code in the first place. - McGraw and Felton, 1999.

It's no wonder that including security early in the development process will usually result in less expensive, less complex and more effective security than adding it during the lifecycle.

Given that ISO 17799 is the international code of reference for information security, we will focus on how to integrate key controls selected from such standard into all phases of the SDLC process, from initiation to disposal.

SDLC is a framework for developing software successfully that has evolved with methodologies over time. Discussions over different models are out of the scope of this article but regardless of which software development model is used, there are typical phases that need to be included. The basic phases are:

• Project initiation and functional requirements definition
• System design specifications
• Build (develop) and document
• Acceptance
• Transition to production (installation)
• Operations and maintenance support (post-installation)
• System replacement (disposal).

Therefore, to successfully include security into the SDLC process, the following requirements must be met:

• It must be based on security principles adhering to a recognized standard and information privacy.
• It must be focused on risk and compliance
• It must include activities designed to ensure compliance to ISO 17799:2005
• It must require security-related steps in SDLC procedures
• It must be supported by management as well by information and business process owners.

Before going further, we can think in ISO 17799 like 'the security control supermarket'; hence, you go there and pick what you fancy! However, this is a peculiar supermarket in the way that you need to justify all the decisions you make on what controls you choose and what controls you don't. This justification will be based in periodic risk assessments. This is what we call a risk based approach.

So based on these typical phases, the next section provides a correlation of where security tasks and ISO 17799 based controls should be included during the activities completed at each of these SDLC basic phases.

Security Activities within the SDLC

Project initiation and functional requirements definition

At the beginning phase, business needs are identified along with the proposed technical solution. The identified solution must be aligned to business strategy as well as to IT strategy and security strategy.

At this stage, ISO 17799:2005 section 6 (Organization of Information Security) highlights the importance of a well established security management framework where security related decisions are supported by the business, responsibilities are clearly allocated and activities coordinated across the organization. During this early phase of development, the organization will determine its information security requirements, often developed by successive refinement, starting from a high level of abstraction that may include the information security policy and the enterprise architecture, and then adding additional specifications during consecutive phases.

However, the definition of the security requirements must always include security categorization and a preliminary risk assessment.

According to section 7 (Asset management and information classification), to ensure that the information handled by your application receives the appropriate level of protection, you will have to identify information assets and categorize each according to regulatory impact, business criticality and sensitivity.

Most of information classification schemes define three levels (low, moderate or high) of potential impact for organizations or individuals should there be a breach of security (a loss of confidentiality, integrity or availability). This standard will assist you in making the appropriate selection of security controls for your application.

On the other hand, a preliminary risk assessment will result in a brief initial description of the basic security needs of the system, expressed again in terms of the need for integrity, availability and confidentiality. This assessment will establish the threat environment in which the application will operate, followed by an initial identification of required security controls that must be met to protect it in the intended operational environment. The technical, operational and economical feasibility of these controls and any other security alternatives must be analyzed at this point. A cost / benefit analysis should be undertaken for each control, resulting in a preliminary risk treatment plan. To assess the effectiveness of those controls, a security test and evaluation plan will be developed in order to provide important feedback to the application developers and integrators at later stages.

This risk-based approach, as stated on section 4 from the standard, is the basis for any successful security initiative; hence risk assessments must be repeated periodically during the application lifecycle to address any changes that might influence the risk assessment results, until consistency is achieved.

Although you can choose among many different risk analysis methods, the risk assessment will not necessarily be a large and complex document. It is extremely easy to get lost in a complex risk analysis, so bear in mind that the risk assessment is a mean to achieve your goal but not the goal itself, so keep it simple.

In addition, the application context should be considered, as it might affect other applications or systems to which it will be directly or indirectly connected. If the context is not considered, there is a possibility that the application being developed could compromise other organization systems.

Additionally, the security functional requirements analysis should include not only a security policy and enterprise architecture analysis, but also an analysis of applicable laws and regulations, such as the Privacy Act, HIPAA, SOX, ISO 27001, and others, which define baseline security requirements. As section 15.1 (Compliance with legal requirements) states, all relevant legal and contractual requirements as long as functional and other IT security requirements should be explicitly defined, documented, and kept up to date for each information system in the organization.

A preliminary business continuity plan focused on the required business objectives is also produced at this point, e.g. restoring of specific communication services to customers in an acceptable amount of time, etc. Producing this plan requires full involvement from application and business processes owners, and again, is based on a business continuity risk assessment. A list of items that must be considered within the business continuity planning process is included in section 14.1.3 (Developing and implementing continuity plans including information security) of the standard.

Typically, a service level agreement (SLA) is also required to define the technical support or business parameters that an application service provider will provide to its clients, as well as the measures for performance and any consequences for failure. These kinds of agreements together with a typical list of terms are covered on section 6.2.3 (Addressing security in third party agreements) of the standard.

This section finalizes with the security framework documentation, resulting in a high-level description of the security issues, risks and controls in the proposed application and the assurance requirements. This material will be used to support the derivation of a cost estimate that addresses the entire life-cycle. It is usually the case that there is a balance such that increased expenditures during early development stages may result in savings during application operation.

PRIOR THE APPROVAL OF DESIGN SPECIFICATIONS, A COMPREHENSIVE SECURITY RISK ASSESSMENT SHOULD HAVE BEEN CONDUCTED

System design specifications

This phase includes all activities related to actually designing the application. In this phase, the application architecture, system outputs, and system interfaces are designed while data input, data flow and output requirements are established. Detailed security specifications are included into the formal baseline documentation and the security test plan will be updated, including specific procedures on how to validate system components through development and deployment stages.

Prior the approval of design specifications, a comprehensive security risk assessment should have been conducted, including those risks related to third parties that may require access to the organization's information and information processing facilities. This assessment will result in the identification of appropriate security controls that will be agreed and included into a contract or into a SLA. A list of issues that should be taken into account before granting access to any external party are listed in section 6.2.1 (Identification of risks related to external parties) of the standard.

At this point, access control rules must be defined to ensure that access to information and information processing facilities are controlled on the basis of business and security requirements previously defined. In addition, a policy should be in place to maintain the security of information that may be exchanged through the application with any external entity. Section 10.8.1 (Information exchange policies and procedures) contains a comprehensive list of security issues that should be considered when using electronic communication facilities for information exchange, i.e. using cryptographic techniques to protect the confidentiality, integrity and authenticity of information.

Capacity management is also a key area that must be formally considered when it comes to application development. At this stage, section 10.3.1 (Capacity management) states that any projections of future capacity requirements should take account of new business and system requirements and current and projected trends in the organization's information processing capabilities. This is particularly important in case your application requires any resources with long procurement lead times or high costs.

At the end of this phase, all appropriate security controls must be defined and included into the application design specifications.

Build (develop) and document

During this phase, the source code is generated, test scenarios and test cases are developed, unit and integration testing is conducted, and the program and system are documented for maintenance and for turnover to acceptance testing and production.

At this stage, the parallel security activities must ensure that any security-related code is actually written (or procured) and evaluated, security tests are performed and that all approved security components in formal baseline are included.

Most of security controls that will be implemented during this phase are found on section 12 (Information systems acquisition, development and maintenance) of the standard, i.e.:

• Input and Output data validation to ensure that data is correct and appropriate and to prevent standard attacks including buffer overflow and code injection.
• Validation checks to detect any corruption of information through processing errors or deliberate acts.
• Cryptographic techniques to ensure authenticity and protecting message confidentiality and integrity in applications.

Additionally, section 12.4 (Security of system files) gives some guidelines on securing access to system files and program source code. Test environments are usually complicated and difficult to manage environments, so special care should be taken to avoid exposure of sensitive data within them. It is highly recommended to avoid the use of operational databases containing personal data or any other sensitive information for testing purposes, as this could result in a breach of data protection laws, and access to program source code and associated items (such as designs, specifications, verification plans and validation plans) should be strictly controlled in order to prevent the introduction of unauthorized functionality and to avoid unintentional changes. Section 12.4.3 gives particular recommendations to control access to program source libraries in order to reduce the potential for corruption of computer programs.

Acceptance

In the acceptance phase, an independent group develops test data and tests the code to ensure that it will function within the organization's environment and that it meets all the functional and security requirements. Prior to this stage, managers should ensure that the requirements and criteria for acceptance of new applications are clearly defined, agreed, documented and tested. It is essential that an independent group test the code during all applicable stages of development to prevent a separation of duties issue, as recommended by section 10.1.3 (Segregation of duties) of the standard.

As recommended in the previous section, any test must be carried out with previously sanitized data to ensure that sensitive production data is not exposed through the test process. A list of items that should be considered prior to formal application acceptance being provided is found on section 10.3.2 (System acceptance).

Good practice, as stated in section 10.1.4 (Separation of development, test and operational facilities), includes the testing of software in an environment segregated from both the production and development environments, as this provides a means of having control over new software and allowing additional protection of operational information that is used for testing purposes. This should include patches, service packs, and other updates.

The security testing should uncover all design and implementation flaws that would allow a user to violate the software security policy and requirements, and to ensure test validity, it should be tested in an environment that simulates the intended production environment. As a result of such tests, security code may be installed and necessary modifications undertaken.

Section 12.6.1 (Control of technical vulnerabilities) provides guidance on how to perform integrated application component tests and identifies several steps that should be followed to establish an effective management process for technical vulnerabilities, including vulnerability monitoring, vulnerability risk assessment, patching, asset tracking, etc.

This will be the last chance to detect security weaknesses or vulnerabilities as, once the application security has been verified and the system has been accepted, it will moved into production.

SPECIAL CARE SHOULD BE TAKEN WHEN TRANSFERRING A SYSTEM FROM DEVELOPMENT TO OPERATIONAL STAGE, AS SUCH CHANGES CAN IMPACT ON THE RELIABILITY OF APPLICATIONS

Transition to production (installation)

During this phase the new system is transitioned from the acceptance phase into the live production environment. Typical activities during this phase include training the new users according to the implementation and training schedules; implementing the system, including installation, data conversions, and, if necessary, conducting any other parallel operations. Security control settings and switches are enabled in accordance with the defined security baseline and available security implementation guidance.

Parallel security activities verify that the data conversion and data entry are controlled and only those who need to have access during this process are allowed on the system.

Also, an acceptable level of risk is determined and accepted by business managers and appropriate controls are in place to reconcile and validate the accuracy of information after it is entered into the system. It should also be tested the ability to substantiate processing.

Special care should be taken when transferring a system from development to operational stage, as such changes can impact on the reliability of applications. Therefore, section 10.1.4 (Separation of development, test and operational facilities) gives additional recommendations that should be considered, i.e. removing any development tools or system utilities from operational systems when not required, removing development and test personnel access rights to the operational system and its information, etc.

However, even though small organizations may find enforcing segregation of duties and environments difficult to achieve, the principle should be applied as far as possible and practicable. Whenever it is difficult to segregate, as recommended by section 10.1.3 (Segregation of duties), other controls such as monitoring of activities, audit trails and management supervision should be considered.

Finally, transition to production must be controlled by the use of formal change control procedures to minimize the corruption of information systems. You will find a comprehensive list of items that the change procedures should include on section 12.5.1 (Change control procedures).

Operations and maintenance support (post-installation)

During this phase, the application will be in general use throughout the organization. The activities involve monitoring the performance of the system and ensuring continuity of operations. This includes detecting defects or weaknesses, managing and preventing system problems, recovering from system problems, and implementing system changes.

It's no wonder that inadequate control of changes is exactly the most common cause of system and security failures.

Therefore, to ensure the correct and secure operation of information processing facilities, any changes to systems and application software should be subject to strict change management control, as recommended by section 10.1.2 (Change management).

In general, changes to operational systems should only be made when there is a valid business reason to do so, and must be always preceded by an assessment of the potential impacts, including security impacts, of such changes. Hence, periodic risk analysis are required whenever significant changes occur, including a change in data sensitivity or criticality, relocation or major change to the physical environment, new equipment, new external interfaces, new operating system software (as considered on section 12.5.3 – Technical review of applications after operating system changes -), or new application software. It is recommended that a specific group or individual is given responsibility for monitoring vulnerabilities and vendors' releases of patches and fixes. Also, someone should be assigned the task of verifying compliance with applicable service level agreements according to the initial operational and security baselines.

Other parallel security activities considered during this stage include:

• System monitoring to detect any unauthorized information processing activities, to check the effectiveness of controls adopted, and to verify conformity to an access policy model, as stated on section 10.10 (Monitoring). This section also addresses audit logging activities, the protection of log information and logging facilities and supporting activities like clock synchronization.
• Network security management to ensure the protection of the application information and the protection of the supporting infrastructure as stated on section 10.6 (Network security management).
• Technical compliance checking to ensure that hardware and software controls have been correctly implemented and usually involving penetration tests or vulnerability assessments as considered on section 15.2.2 (Technical compliance checking). Special care should be taken when auditing to minimize the risk of disruption to business processes and access to audit tools should be protected to prevent any possible misuse or compromise. Further information on this topic can be found on section 15.3 (Information systems audit considerations).
• Documenting operating procedures as considered on section 10.1.1 (Documented operating procedures), to ensure the correct and secure operation of information processing facilities. This control also helps to ensure that system activities associated with the application (backups, maintenance, media handling, etc…) are always made available and updated to all users who need them.
• Control of operational software to minimize the risk of corruption to operational systems by implementing a rollback strategy, activating auditing logs, archiving old versions of software and other guidelines found on section 12.4.1 (Control of operational software).
• Protection against malicious and mobile code to protect the integrity of software and applications. Section 10.4 (Protection against malicious and mobile code) provides guidance on the detection, prevention and recovery controls that should be implemented across the organization.

Nevertheless, when it comes to access control, the standard allocates a whole section to this pillar of security. Controlling the allocation of access rights to information systems, privilege management, password management and the review user access rights are a day-to-day challenge. You'll find particularly useful to follow the guidelines found on section 11 (Access control) and to implement those specific controls that will be selected as a result of the previous risk assessments.

System replacement - disposal

Disposition, the final phase in the SDLC, provides for disposal of the application in place. Information security issues associated with disposal should be addressed explicitly. In general, when information systems are transferred, obsolete, or no longer usable, it is important to ensure that organization resources and assets are protected. Generally, an application owner should archive critical information, sanitize the media that stored the information and then dispose of the hardware/software.

ISO 17799:2005 gives particular emphasis to secure disposal or re-use of equipment (section 9.2.6) when it recommends that all devices containing sensitive data should be physically destroyed or the information should be destroyed, deleted or overwritten using techniques to make the original information non-retrievable rather than using the standard delete or format function.

Finally, as stated on section 9.2.7 (Removal of property) you must remember that any equipment, storage media, information or software should not be taken off-site without prior authorization and, where necessary and appropriate, it should be recorded as being removed off-site.

SDLC Phases	Project Activities	Parallel Security Activities	ISO 17799:2005 mapping
Project Initiation and Functional Requirements Definition	• Identify business needs • Identify areas affected and responsibilities • Develop functional requirements • Propose technical solution • Evaluate alternatives • Document project's objectives, scope, strategies, costs and schedule. • Select / approve approach • Prepare project plan • Prepare preliminary test plan • Select acquisition strategy • Establish formal functional baseline	• Determine security requirements • Classification and criticality of information/applications • Identify legal, statutory and contractual requirements • Initial Risk Analysis Cost / benefit analysis • Preliminary contingency planning • Prepare a security evaluation plan • Include security requirements in the security baseline as well as in request for proposal and contracts • Determine SLAs • Document security framework	5.1.1 – Security Policy 7.x – Asset management and information classification 6.1.1, 6.1.2, 6.1.3 – Organization of Information Security 12.1 – Security requirements of information systems 6.2.3 – Addressing security in third party agreements 15.1 – Compliance with legal requirements 14.1.3 – Business Continuity Management
System Design Specifications	• Develop detailed design (system architecture, system outputs and system interfaces). • Detail the solution's interactions with external systems. • Update testing goals and plans. Establish data input, data flow and output requirements. • Establish formal baseline/ quality controls and requirements.	• Identification of Risks related to external parties. • Define access control strategy • Define security specifications (program, database, hardware, firmware and network) • Develop security test procedure • Include security area in formal baseline documentation and quality assurances	11.1 – Business requirement for access Control 6.2.1 – Identification of risks related to external parties 10.8.1 – Information exchange policies and procedures 10.3.1 – Capacity management
Build/Development and Documentation	• Construct source code from detailed design specifications. • Perform and evaluate unit tests. • Implement detailed design into final system.	• Write or procure and install security-related code. • Control access to code. • Evaluate security-related code. • Ensure approved security components in formal baseline are included.	12.2.x –Correct processing in Applications 12.3.x – Cryptographic controls 12.4.x – Security of System Files

SDLC Phases	Project Activities	Parallel Security Activities	ISO 17799:2005 mapping
Acceptance	• Test system components. • Validate system performance. • Install system. • Prepare project manuals. • Perform acceptance test. • Accept system.	• Sanitize test data. • Independent security tests. • Install security code with necessary modifications. • Document security controls.	10.3.2 – System acceptance 12.6.1 – Technical vulnerability management 10.1.4 – Separation of development, test and operational facilities
Transition to Production (implementation)	• Train new users according to implementation. • Implement the system (installation, data conversions...).	• Control data conversion and data entry. • Reconcile and validate data integrity. • Enforce segregation of duties and segregation of environments.	12.5.1 – Change control procedures 10.1.3 – Segregation of duties 10.1.4 – Separation of development, test and operational facilities
Operations and Maintenance Support (post-installation)	• Monitoring performance. • Ensuring continuity of operations. • Detect weaknesses or defects. • Manage and prevent system problems. • Recover from system problems. • Implement system changes.	• Periodic risk analysis. • Change management. • Verify compliance with applicable SLAs and security baselines. • Maintain release integrity with secure and controlled environments.	10.10. x – Monitoring 12.5.2 – Technical review of applications after operating system changes 10.6.x – Network security management 11.x – Access control 15.2.2 – Technical compliance checking 15.3.x – Information systems audit considerations 10.1.1 – Documented operating procedures 12.4.1 – Control of operational software 10.4.x - Protection against malicious and mobile code
System Replacement - Disposal	• Hardware and Software disposal.	• Information preservation. • Media sanitization.	9.2.6 – Secure disposal or re-use of equipment 9.2.7 – Removal of property

Conclusion

Introducing a risk management program along all your project phases is the key to success in introducing security into SDLC. However, we must admit that it can be challenging on an uncompleted cycle and identification of mitigation points is sometimes tricky. Additionally, adding an IT process-centered practice approach, like ITIL and COBIT, aids in being able to determine how best to embed security controls into your operational processes and how to measure their effectiveness. Security awareness is another driving factor and collaboration between all parties, the business and ICT department, is critical. Management must be clearly committed to information security and managers must be made responsible and accountable for the security of their application systems. They should ensure that all proposed system changes are reviewed to check that they do not compromise the security of either the system or the operating environment.

Ismael is working as an Information Security Specialist at iSOFT plc. He is involved in security governance and compliance, implementing ISO 27001, providing risk assessment and security consulting and strategy. He has also participated as a senior consultant for many big security projects in Spain, as well as an instructor, writing articles and promoting security business. Ismael holds a Bachelor in Computer Science, is certified in Business Administration, ITIL, CISM and CISSP and was recently accredited as IRCA ISO 27001 Lead Auditor by Bureau Veritas UK. Ismael can be reached at ismael.valenzuela@gmail.com and www.linkedin.com/in/ivalenzuela.

A public key infrastructure (PKI) can provide a set of security building blocks that other infrastructure components can use to provide stronger security services. For quite some time there is discussion around PKI. After more than a decade there is still a feeling of doubt among organizations whether they should implement a PKI and how certificates and related cryptosystems can play a role within their businesses. PKI is definitely not new and it is a fact that it never really became a huge success. Is this changing? Let's discuss this in more detail and then draw your own conclusions.

A Public Key Infrastructure (PKI) provides a set of security building blocks that other infrastructure components can use to provide strong security services to their users. In this perception these services are highly important in todays IT infrastructures and the questions around it are really hot topics. It's beyond the scope of this article to explain PKI entirely. This article discusses and focuses on the important considerations concerning PKI and what it can do for your business.

The pros and cons of PKI

If you start searching for information about PKI and implementations within larger organizations you generally see a huge discussion about it. After more than a decade there is still a struggle with the question whether it is needed to adopt PKI and how certificates in the organization must be introduced.

Possible questions with which we are confronted are:

- do we have to set up an internal PKI service on our own or can we buy certificates externally?
- how is the integration with other parties, software, compatibility?
- and what about the basis of faith and the factor trust?
- what is the position of externally bought certificates?
- what is the third party liability and what are the possible consequences of this?

- do we have some legal regulations that makes PKI necessary?
- are there no other technical solutions to accomplish the same goals?

Furthermore are the high implementation costs, complexity and time consuming projects that we can hear as critics. Although there are many examples in which the implementation of PKI failed, we must be aware of the projects that ended up successfully and had a large added value to business in those cases.

Governmental organizations, such as army, justice and police force, by nature have a larger interest with PKI because security and confidentiality do have high priority in daily processes.

Commercial organizations like a internet bookseller generally start from a different point. To be competitive they have to present more customer friendly services. No hard barriers because the goal is to do simply business with each other (preferably in a secure way). However, in past years a few things changed. There are some regulations and laws (Sarbanes-Oxley, COBIT and so on) that forces companies to have a different look at security related topics.

The CIA triad

Among the security building blocks that a PKI can offer are identification, authentication, confidentiality, integrity, and nonrepudiation. Identification gives an entity a way to check another entity's identity. In order to be sure that John is indeed John. Second, authentication ensures that, for example, the sender of a message is the one from whom it originates. Next, confidentiality is a service that protects against unauthorized disclosure of information. Then integrity protects against undetected modification of a message. Nonrepudiation gives protection against denial, by the entities involved in a communication process.

The previous issues are all important for most of us IT professionals and certainly those of us familiar with security. We know that these topics are most of the times part of the basic ingredients of the "CIA triad": Confidentiality, Integrity and Availability. We would say: PKI is the answer to all of the commonly known security challenges. Sorry but it isn't that simple as it seems to be.

PKI as infrastructural basis

It's really important to stress the last character of the PKI acronym: PKI is an infrastructural component, which means that by itself it has no direct value. Added value comes at the moment other services and infrastructure components can build on it to provide strong(er) security.

PKI is an electronic system (definitely with solid processes around it) that works with public and secret (private) digital keys. In short - asymmetric cryptographic ciphers deal with public keys and private keys. The two keys mathematically are stipulated and derived from each other.

The true power of public key cryptography lies in the possession of a private key, uniquely, by each party. The "demonstration of knowledge" of the private key by using this key, provides a powerful pillar in the PKI framework and in asymmetric cryptography.

A third party in this process can be trusted by all services / persons. This third party is known as the Certification Authority. Therefore, the heart of a PKI is pure cryptography.

A PKI provides services and processes to manage these keys and the entire lifecycle of it. Among these services are certification, user registration, key generation, key update, key archival, certificate publishing, certificate renewal, and certificate revocation.

Use of a PKI

A way PKI can be used is that a certificate can be linked to a person or identity and the Certificate Authority (CA) supplies on request the certificate of that specific person. You can then log on to a workstation using a certificate that is stored on a smart card. At that time do have the so called "two factor authentication". Something you own or what is in your possession (the smart card with certificate stored on it) and something you know which is in most cases a pin-code that is handed out in combination with the smart card.

A PKI can also be used as a framework for secure WLAN. The certificates can be used in the WLAN components and to certify your Windows clients. The 802.11i standard does not deal with the full protocol stack but addresses only what is taking place at the data link layer of the OSI model. The use of EAP, however, allows for different protocols to be used to fill in the gap and deal with authentication. EAP and Transport Layer Security (EAP-TLS), carry out this authentication through digital certificates.

If EAP-TLS is being used, the authentication server and wireless device exchange digital certificates for authentication purposes. When using EAP-TLS, the steps the server takes to authenticate to the wireless device are basically the same as when an SSL connection is being set up between a web server and web browser. Once the wireless device receives and validates the server's digital certificate, it creates a master key, encrypts it with the server's public key, and sends it to the authentication server. Now the wireless device and authentication server have both a master key, which they can use to generate individual symmetric session keys. These session keys are being used for encryption and decryption purposes, a secure channel between the two devices. As you can see a complex process where PKI can really play a part in. However, you can implement secure WLAN without PKI - the use of PEAP in combination with MSChap v2 for example.

There are several applications of PKI. It can be used to certify hardware components, to uniquely bind a certificate to a person, for digitally signing documents or encrypting data.

Trust is very important within a PKI.

The factor trust

Trust is very important within a PKI. To ensure the "trust" factor for all the relationships within a PKI you have to implement very strict processes / procedures to ensure that certificates are handed out to the right services, applications and persons. That is why most of the times a PKI is complex, time consuming and cost a lot of money to set it up in the appropriate way.

Different implementations

In the discussions around PKI frequently several terms are mixed up. In this respect it is useful to distinguish several implementation appearances of Public Key Cryptography (PKC's) or systems. We can make thereby the distinction between stand alone PKC's, Internal or a Closed PKI and External or Open PKI.

PKC's are most of the times embedded in specific solutions or a specific product. It can be very efficient and valuable to implement such a solution in case of, for example, secure WLAN and a VPN solution. However, there is limited operational integration between different components and more management needed over different platforms.

A closed PKI is most of the times used only (and limited for use) within an organization perimeter. You can't use this type of PKI to digitally sign your mail that is going to be send to another company over the internet because you and the receiving company do not trust a common party called a certification authority like Verisign or Thawte. Cross certification is most of the times too complex and not applied frequently.

You can use this type of PKI for internal authentication purposes (smart cards) and for example internal client hardware certification. You maybe want to use a Microsoft CA to fill in this need and setup an internal PKI.

And then there is Open PKI. The broader use of PKI and certificates intended for authentication, for use concerning digitally signing of mail (externally), the use of encryption and on behalf of applications and services that are external orientated can make Open PKI the way to go.

PKI and e-commerce

In the digital outside world it is clear that there is a bigger challenge to retrieve and be sure about an identity as within an organization. For some time it really seemed that PKI would play an important role on the internet and within e-commerce. However, in an e-commerce application it is most of the times only necessary for an end-user to ask the question if a website can be trusted such as www.amazon.com.

To get this type of trust we mostly see implementations with SSL. The tiny litte lock presented in your browser. This does not go with user certificates, although it is possible within SSL to also authenticate a client party (or in real: the web browser) to a server, it is not a common practice to do so. This because so-called mutual authentication is more complex.

The offered service on the web portals will be to present a server certificate to an end-user. SSL makes use of this and establishes two things: present the identity of that server to the user and second to get a secure communication channel before you hand over your personal matter such as delivery address and credit card data. Such certificates can be bought for SSL externally by contacting Thawte or Verisign.

Most commercial parties are not confident that PKI can play an more important role in this whole process. How much more secure will this be, and against what costs? They accept the risks that comes with this and the loss of profits. The most important point is that it creates more complex processes and a barrier for potential buyers or customers. The conclusion can be drawn that freedom, simplicity and doing business more easily have a higher priority compared with rock solid and maximum security. This is a fact and reality.

Digital signatures

There was for some time no clarity concerning the legality of a digital signature and the minimum requirements for use. To solve these problems, and to stimulate e-commerce, in the end of the year 1999 an European directive appeared with no. 99/93/EG concerning electronic signatures. In the US the same thing happened. This directive states that the Member States of the European Union must adopt laws to make digital signatures valid.

Law articles say that an electronic signature is considered reliable enough when the signature is linked to a person that signed a message in a unique way and that the signatory always can be identified.

Besides that, each modification afterwards can be traced. With all this precautions a "sophisticated" electronic signature becomes valid. Conclusion is that a reliable signature is possible by using digital certificates.

Introducing PKI needs good agreements concerning liability.

Liability

Introducing PKI needs good agreements concerning liability. By the so called CPS or the Certification Practice Statement we create a set of rules concerning the use and the liability of certificates. This CPS is certainly of huge importance in case you decide to buy in external expertise and have a managed PKI.

PKI and the identity question

Often it has been written that without a PKI the identity from a person on the internet or in the virtual digital world never can be determined with some certainty. But in daily practice it happens to be that PKI also doesn't provide all the answers on this topic.

Yes, PKI gives the possibility to bind unique names or persons to a certificates or keys but the most important step - to really link that one identity with only one certificate or key still isn't accomplished automatically, is not secured and in any way guaranteed.

I'll give you an example of this. With PKI you'll know that a specific electronic document is digitally signed with a private key. A key that is used by one identity or person. However, there are still some questions left:

- Did indeed that person sign the document?
- What is the underlying process of digitally signing?
- Did that person really read the document or is it a computer system or application that carried out the actual signing without approval?
- How did this person came into possession of the private key?
- Is the identity really true and correct that is linked to the private key?

All these highly important processes are not filled in automatically at the mathematical side of PKI. Cryptography is really strong within PKI but the weakest link is still the human factor and the implementation of strict procedures. As you can see, within the whole security chain of PKI there are the same weak spots like in other security solutions. Nothing more and nothing less. Within a closed PKI (or internal PKI) of an organization it is better possible to implement strict procedures to ensure that a person really represents the correct identity. After that it is possible to link that person to a specific certificate or private key by handing it out personally.

In other words, the physical determination of the identity can be accomplished. After handing out a certificate on, for example, a smart card, there is no guarantee anymore that the person is who he or she claims to be. We assume it is but are we sure about that? If we talk about the digital outside world, then this determination is nearly impossible. We have in no way sufficient control about processes at all.

With PKI you'll know that a specific electronic document is digitally signed with a private key.

Justification for PKI

A couple of years ago we could see that there was no solid case we could found in most organizations having PKI implemented all the way. A first warning sign of operational and financial inefficiency as Gartner laid down in a 2006 report. And nothing has changed in respect to PKI solutions in my respect. The method of: "implement it and the services which makes use of PKI will come within time" is not a sufficient argument and a justifiable point of view for the introduction of PKI.

There are enough technical solutions possible to have valuable alternatives to implement VPN, protected Wi-Fi, mail signing and so on. Is a PKI then worth looking at? Yes it certainly is but it is really important to overlook the field of possible solutions on a strategic term. Delimit the scope clearly and at an early stage in such projects. This will mean that there is a big need to have a clear answer on how to implement it and for what kind of services. In other words - implementation strategy.

Therefore not only have a look at the position of PKI for the short term and quick wins but also for problems (or challenges) over a longer period in time. Do not bring PKI forward as the ultimate solution for all problems within the company: the three character magic word. Once PKI has been introduced it is really difficult to say it farewell.

Considerations for implementing PKI

It isn't that easy to have it all clear from the beginning. There are a lot of arguments you have to consider before the decision can be made implementing a PKI or not. Although hard to give some advise in general, I'll try to give you some ammunition.

First you must consider if there is any clear (business) case that justifies the implementation of PKI and second if there is only one challenge where PKI did came into the picture. Think about it again if the case is not clear and ask yourself the question if you can find another solution without using PKI.

However, if there is are two or more cases from business perspective where PKI is in the picture, you might want to know if there are other scenarios is the future where there is the possibility to position PKI as an infrastructural component and solution within your environment. If so there can be a point in time that it is more wise to implement PKI instead of half a dozen of point solutions. This stand alone solution at that time can be more of a challenge in management and costs.

Generally speaking you have to take into account that a full implementation of PKI in a larger organization without experience will take between 9-12 months. It's not the technical side of it all that will take time and effort but the biggest challenge is to get all the necessary procedures in place in a secure and controlled way. I think this is 80 percent of the time versus 20 percent for technical issues.

After all it is most of the times not a "must have" to implement PKI. Some measures like a more solid process around identities (Identity Management or IDM) and the use of strict Role Based Access (RBAC) gain more success.

In an organization like I'm working for this certainly is a consideration. Designate the Human Resource department for issuing identities and make them full responsible for the Pre-employment Screening and the issuing of accounts. These accounts can be provisioned to certain important platform like the Active Directory and give access to the Windows infrastructure and workstation.

If an employee leaves the company the system will take care of withdrawing all possible accounts and rights. The return on investment (ROI) in such circumstances can be much better.

The trend with PKI today is seamless integration: you don't want the user to know they are using a certificate or encryption key and bother them with difficult processes or techniques.

Conclusion

The trend with PKI today is seamless integration: you don't want the user to know they are using a certificate or encryption key and bother them with difficult processes or techniques. More and more the interoperability improvements finally starting to pay off. Standards are more and more used in this market and so there is a broad spectrum of applications and solutions that can be used in combination with a Public Key Infrastructure.

Another key point is the integration in for example Microsoft and Cisco products. Integration with Microsoft's CryptoAPI interface, which is used by all Microsoft OS's and other products for encryption functionality (even other third party solutions), is available today and makes it far more easy to start using a PKI than a couple of years ago. Moreover, certificates and keys can be controlled through centralized (policy) settings, all automatically and seamlessly from the Active Directory in a Windows environment.

After more or less critical sounds in this article I think PKI can play an important role for business today and prove its usefulness. However, you have to be really careful and think twice about the investments to make, the complexity of technology and procedures you have to implement and adopt with your organization. If you do so you can then decide for yourself whether or not implementing a PKI.

Rob P. Faber, CISSP, MCSE, is an infrastructure architect and senior engineer. He is currently working for an insurance company in The Netherlands with 22.000 clients. His main working area is (Windows Platform) Security, Active Directory and Identity Management. You can reach him at rob.faber@icranium.com.

INFORMATION IS EVERYTHING

Register Today at
www.infosecurityevent.com/Helpnet

JUNE 13 – 14, 2007 • METRO TORONTO CONVENTION CENTRE • TORONTO, ONTARIO

LEARN HOW TO BEST PROTECT YOURS.

When it comes to your critical information – it's not a question of if it's at risk, it's a question of when. Stay in front of the fast, ever changing information security curve at the only IT security event in Canada, Infosecurity Canada 2007. It's where the Canadian IT industry gathers to get up-to-date on how to best deal with today's threats to vital information, and how to be prepared for tomorrow's information hazards.

infosecurity CANADA

Leading solutions critical to developing a secure and compliant information infrastructure within any size business including:

- Access Control • Anti-Spam
- Email Security • Firewalls
- Intrusion Detection
- Intrusion Protection
- LAN/WAN Security
- Network Security • Virus Protection
- Client Server Security

It's all comprehensively covered at Infosecurity Canada 2007.

Take advantage of our unrivaled education program providing the most critical and relevant strategic and technical knowledge you need.

Because your information is everything – register today it's easy and **FREE** at: **www.infosecuritycanada.com**

Diamond Sponsor: Microsoft

Platinum Sponsors: CA, Qualys

Global Sponsor: Symantec

Gold Sponsors: allstream, Cisco, Rittal, TELUS

Silver Sponsors: Novell, WinMagic Data Security

Bronze Sponsors: ADT, ESET, ForeScout, nCi, Stonewood FlagStone

Official Media Sponsors: CDN, Computing Canada

Priority Code: WL6

Strategic Information Security Singapore
23 May-25 May 2007 – Singapore
http://www.uninetintelligence.com/events.htm

Strategic Information Security Dubai
27 May-29 May 2007 – Dubai
http://www.uninetintelligence.com/events.htm

9th Annual Techno Security Conference
3 June-6 June 2007 – Marriott Resort at Grande Dunes, Myrtle Beach, SC, USA
http://www.Techno2007.com

Infosecurity Canada 2007
12 June-14 June 2007 – Metro Toronto Convention Centre, Toronto, Canada
http://www.infosecuritycanada.com/

IT Underground Dublin 2007
20 June-22 June 2007 – Dublin, Ireland
http://www.itunderground.org

Information Security Asia 2007: SecureAsia@Bangkok Exhibition
10 July-11 July 2007 – Queen Sirikit National Convention Centre, Bangkok, Thailand
http://www.informationsecurityasia.com/

3rd Annual Techno Forensics Conference
29 October-31 October 2007 – NIST Headquarters, Gaithersburg Maryland
http://www.Techno2007.com

Interview with Christen Krogh, Opera Software's Vice President of Engineering

By Mirko Zorz

Christen Krogh is responsible for all software development at Opera. Krogh received his bachelor's degree in computer science from Glasgow University and his Ph.D from the University of Oslo. In this interview he provides insight into Opera security.

What is Opera's market share? How many users do you have?

Market share is a difficult number to measure and different companies use different methods and track different websites, so a true and accurate representation is almost impossible. Our numbers though are more interesting: we have between 10 and 15 million users of the desktop browser, more than 10 million cumulative Opera Mini users, come pre-installed on more than 40 million mobile phones and are available to anyone using Nintendo Wii or Nintendo DS.

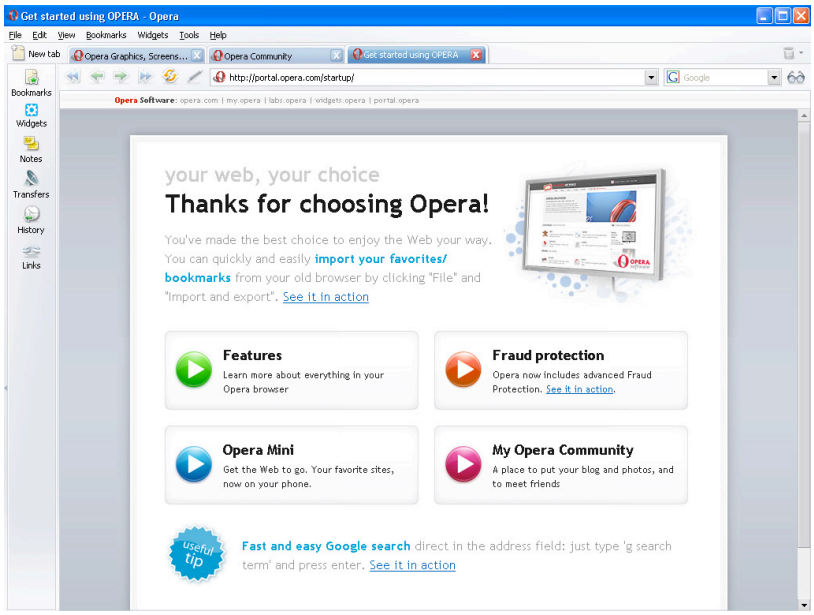
In your opinion, what are Opera's strengths when it comes to security?

Our strenght is that we take it really really serious. We have an excellent Q&A team that tests the browser versions priort to release, both manually, and automatically. We even have a group of skilled experts who call themselves "Evil Knights" working at finding holes and issues prior to launch.

Second, we try to develop our product in such a way that it helps the end users to browse safely. Our advanced Fraud Protection is one example of such a feature. Thirdly, whenever something comes up as a security issue after we have launched a product it takes first priority. We aim to never let a security issue stay unpatched.

Does Opera use technology that makes it stand out from other browsers?

For us, security is largely about architecture, process, and user interface. Architecturally, we might be less prone to certain issues, due to the fact that we have a self-contained browser application with few necessary dependencies to the underlying platform. Process-wise, we might test more diversly than the competition, due to the fact that we



release our products on the largest amount of different platforms. Regarding user interfaces, it has always been a design goal never to mislead the user that they are in a safe environment when they aren't.

Do you believe that you are more secure than other available browsers?

Security can be classified in several ways. Principled security is a function of architecture, process (including Q&A), and design (including user interface). For the lay person, however, security is measured largely by statistics:
1) how many issues
2) how long (on average) did it take to release a Q&A'ed version with a patch (as opposed to how long did it take to have a suggested code change which is not Q&A'ed)
3) how many issues are unpatched (at any one time)
4) the severity of an issue.

The only way of evaluating this is to consult with an independent advisory organization such as secunia.org. According to their independent analysis, we have a superior track record, of which we are very proud and work hard to maintain.

How many security issues have you patched in 2006?

According to secunia.org, Opera 9 had two known security vulnerabilities in 2006, both were patched. In 2006, Opera 8 had two reported vulnerabilities, both were patched.

What has been your average response time to a reported critical vulnerability?

If reported correctly with sufficient details in the report, it is usually less than 24 hours.

Do you believe that your level of security would drop if you managed to get a quite larger portion of the market?

No. I don't think so. Recall the distinction between principled security and the lay persons perception. Our principled security will be at least as good with higher market share. The amount of attacks directed at Opera only might increase, but it is important to remember that almost all attacks are tried out on all the main browsers. Thus the net result of even more attacks will most likely not be significant. What *will* be significant, however, is that the overall security level of end users browsing will be better if Opera gets a larger market share - due to the facts discussed above.

What's your take on the full disclosure of vulnerabilities?

We prefer that reporters contact vendors prior to disclosing a vulnerability in order to ensure that the impact on innocent bystanders (i.e. end users) is as minimal as possible. When there is a patch available from a vendor, we understand and respect that some reporters want to disclose their findings to the community. Out public security policy can be found at www.opera.com/security/policy/

If I keep my documents on Google Docs, my mail on Yahoo Mail, my bookmarks on del.icio.us, and my address book on .Mac, is there any point in talking about the privacy of my data any more? Should I just accept that using web-hosted applications means that privacy doesn't exist?

Many new applications do a great job of making it easy and free for you to post your information online. In a lot of cases, your data is combined with other people's data, to pull helpful or interesting relationships out of aggregate data ("People who bought this book also bought...."). Your photos on your hard drive are not as useful as your photos on Flickr, where others can comment on them, find them via tags, share them, and make them into photo-related products.

Obviously, though, this shift has many implications for privacy, and it is worth wondering what the future of privacy is for web application users. A security breach on one of the most popular hosted web applications could easily reveal private information about thousands or even millions of the site's users. An employee of one of the largest providers could access information about the site's users without anyone knowing. How should a user of these applications think about these risks?

Right now, most application providers either don't talk about these risks or simply ask users to trust that they have their best interests in mind; and as far as we know, the companies providing these applications do in fact make great efforts to respect the privacy of their users. As users, though, the "trust us" proposition does not offer much in the way of reliability of certainty. We essentially must rely on the harm that a large-scale privacy breach would cause the provider as counter-incentive against allowing one to occur.

As developers of Wesabe, and online personal finance community, we think about these questions a great deal. We believe that there is a significant benefit to consumers in anonymously combining their financial data online, since this allows us to produce an aggregate view of where consumers find the

best values (sort of like a reverse FICO score -- a value rating for businesses). However, this project asks our users for a lot of trust. We decided from the outset that, as a startup without the name recognition of a Google or Yahoo, and simply as people interested in providing privacy and security to our users, that we should come up with as many approaches as possible that would help us protect Wesabe users' privacy.

Many of these techniques are generally applicable. While there is a fair amount of information online for individuals who want to protect their own privacy, we found little for web application developers interested in protecting their users' privacy; so, we want to document what we've learned in hope of making these techniques more common, and developing better critiques and improvements of the approaches we've taken so far.

Below, we outline four techniques we use which we think any web application developer should consider using themselves, and describe the benefits and drawbacks to each.

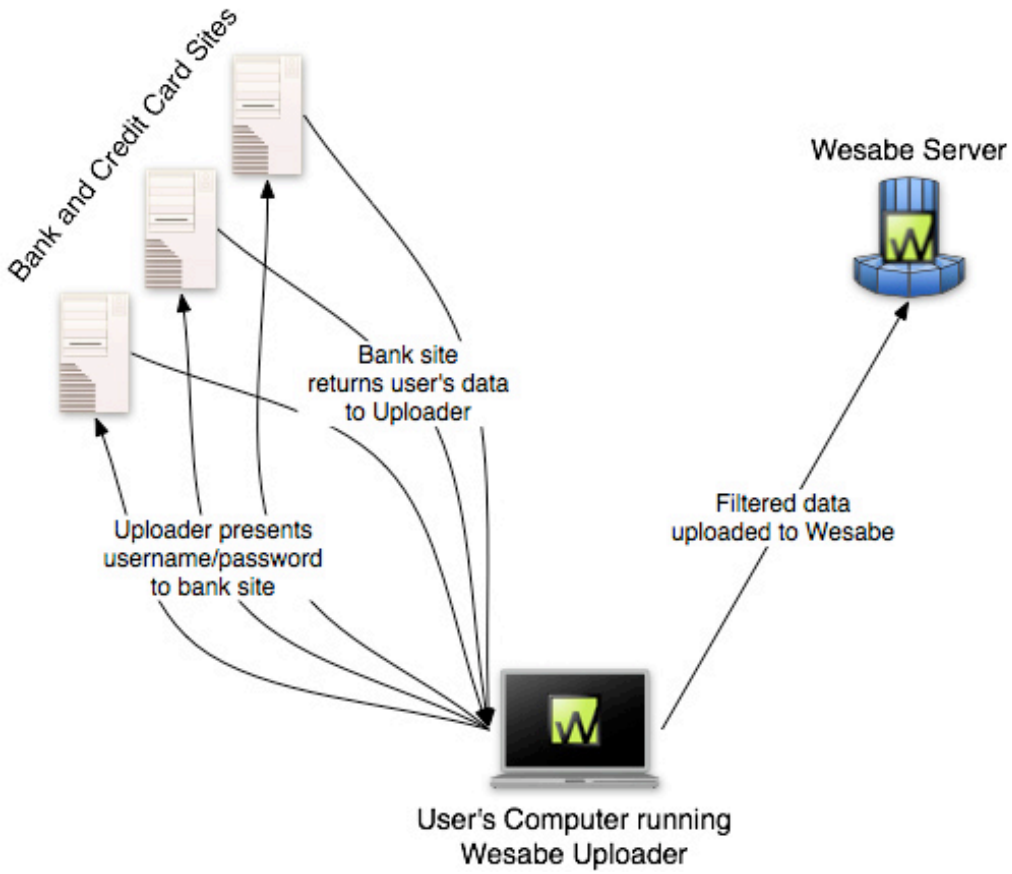
1. Keep critical data local

As a web application developer, the best way to ensure that you protect the privacy of a user's data is not to have that data at all. Of course, it's hard to develop a useful application without any data, but it is worth asking, is there any information you don't absolutely need, which you could make sure not to have at all?

In designing Wesabe, we decided that the most sensitive information in our system would be the bank and credit card website usernames and passwords for our users.

These credentials uniquely identify a person to the site, allow them to make security-critical actions such as bill payments and bank transfers, and enable access to other information, such as account numbers, that can be used for identity theft. In interviewing people about the Wesabe idea, we heard loud and clear that consumers were, quite rightly, extremely sensitive about their bank passwords, having been inundated by news reports and bank warnings about phishing.

Our solution was to make sure our users did not have to give us their bank and credit card credentials. Instead, we provide an optional, downloadable application, the Wesabe Uploader, which keeps their credentials on their own computer.



The Uploader contacts the bank and credit card sites directly, and uses the user's credentials to log in and download their data. It then strips sensitive information out of the data file (such as the user's account number), and uploads just the transaction data to Wesabe. The Uploader acts as a privacy agent for the user. We also provide a way for the user to manually upload a data file they've downloaded from their bank or credit card web site, though this requires more effort on their part.

The advantages of the client model are that the user need not invest as much trust in the web application as they would otherwise, and that we do not have a central database of thousands of users' bank credentials (a very tempting target for an attacker).

As a small startup, not having to ask our users for as much trust is great - we can grow without needing people to be willing to give us their bank credentials from the start. Likewise, as a user of the site, you can try it out without having to surrender these credentials just to experiment.

The Uploader approach has been extremely successful for us - our users have (as of early April 2007) uploaded nearly half a billion dollars in transaction data, with over 80% of that information coming through the Uploader.

The most significant disadvantage of the Uploader model is that it places a significant security burden on the user. If the user's machine is vulnerable, storing bank passwords on their machine does not protect them. (Note, however, that if the user's machine is vulnerable, an attacker can go after those same credentials via the web browser, so in some sense the burden on the user is the same.)

Asking a user to download a client application is also a usability burden, since it requires greater commitment and trust that the client application does what it says it does and does not contain spyware or trojans. Finally, if we were to become very successful, the Uploader application could itself become a specific target for trojans, degrading its benefit.

Overall, we believe that a local client is a good privacy tool for new companies, and for applications where some data should absolutely never be placed on a server. Wesabe will continue to provide a local client for all users, but we will also move to providing other data syncing tools that do not require a client download, since we believe that over time people will be more comfortable with those approaches and will want the convenience of not running the Uploader.

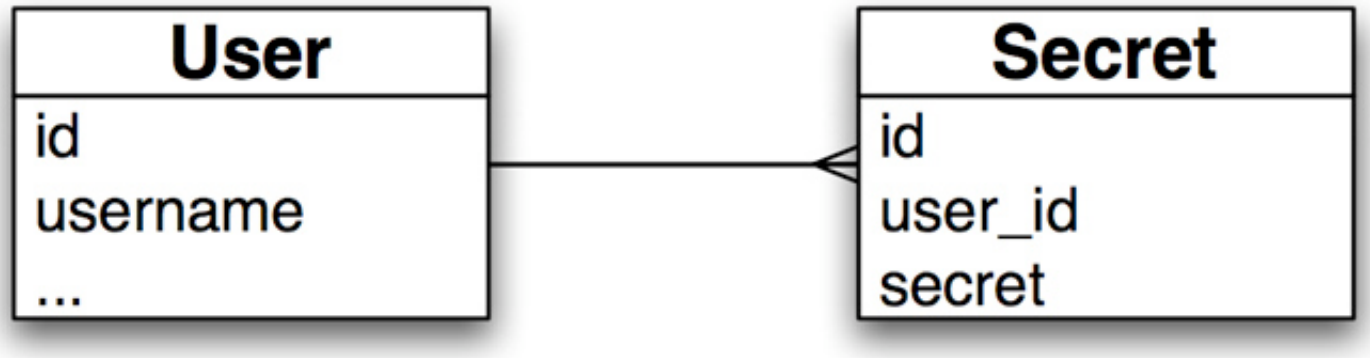
For now, though, a local client has been a great approach for us, and should be considered whenever an application involves data the user legitimately would hesitate to ever upload.

2. Use a privacy wall to separate public and private data

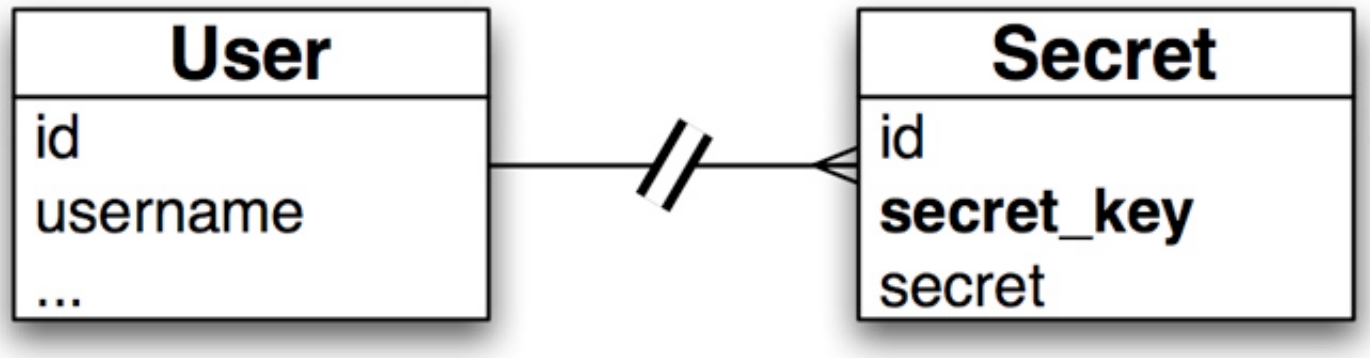
The first people we asked to upload data to Wesabe were some of our closest friends. Many of them replied, "Um, will you be able to see all my bank data, then?" Even people who trusted us were, understandably, very reluctant to participate. We devised a method, the "privacy wall," for protecting their information even from us as developers of the site. We believe this model is a good approach to ensuring that employees of a company have the least possible access to users' data, and to minimizing the harm that would come from a security breach on the site.

The idea of a privacy wall is simple: don't have any direct links in your database between your users' "public" data and their private data. Instead of linking tables directly via a foreign key, use a cryptographic hash that is based on at least one piece of data that only the user knows-such as their password. The user's private data can be looked up when the user logs in, but otherwise it is completely anonymous. Let's go through a simple example.

Let's say we're designing an application that lets members keep a list of their deepest, darkest secrets. We need a database with at least two tables: 'users' and 'secrets'. The first pass database model is show on the following page.



The problem with this schema is that anyone with access to the database can easily find out all the secrets of a given user. With one small change, however, we can make this extremely difficult, if not impossible:



The special sauce is the 'secret_key', which is nothing more than a cryptographic hash of the user's username and their password (plus a salt). When the user logs in, we can generate the hash and store it in the session. Whenever we need to query the user's secrets, we use that key to look them up instead of the user id. Now, if some attacker gets ahold of the database, they will still be able to read everyone's secrets, but they won't know which secret belongs to which user, and there's no way to look up the secrets of a given user.

So what you do if the user forgets their password? The recovery method we came up with was to store a copy of their secret key, encrypted with the answers to their security questions (which aren't stored anywhere in our database, of course). Assuming that the user hasn't forgotten those as well, you can easily find their account data and "move it over" when they reset their password (don't forget to update the encrypted secret key); if they do forget them, well, there's a problem.

The privacy wall technique has a number of possible weaknesses. As mentioned earlier, we store the secret key in the user's session. If you're storing your session data in the database and your database is hacked, any users that are logged in (or whose sessions haven't yet be deleted) can be compromised. The same is true if sessions are stored on the filesystem. Keeping session data in memory is better, although it is still hackable (the swapfile is one obvious target). However you're storing your session data, keeping your sessions reasonably short and deleting them when they expire is wise. You could also store the secret key separately in a cookie on the user's computer, although then you'd better make damn sure you don't have any cross-site scripting (XSS) vulnerabilities that would allow a hacker to harvest your user's cookies. Other holes can be found if your system is sufficiently complex and an attacker can find a path from User to Secret through other tables in the database, so it's important to trace out those paths and make sure that the secret key is used somewhere in each chain.

A harder problem to solve is when the secrets themselves may contain enough information to identify the user, and with the above scheme, if one secret is traced back to a user, all of that user's secrets are compromised. It might not be possible or practical to scrub or encrypt the data, but you can limit the damage of a secret being compromised.

We later came up with the following as an extra layer of security: add a counter to the data being hashed to generate the secret key:

secret key 1 = Hash(salt + password + '1')
secret key 2 = Hash(salt + password + '2') ...
secret key n = Hash(salt + password + '<n>')

Getting a list of all the secrets for a given user when they log in is going to be a lot less efficient, of course; you have to keep generating hashes and doing queries until no secret with that hash is found, and deleting secrets may require special handling. But it may be a small price to pay for the extra privacy.

3. Data fuzzing & log scrubbing

While this is the most basic and best-known of the techniques we describe, it's also probably the most important. Application developers naturally want to keep as much information about the operation of the application as possible, in order to properly debug problems.

They also want to have that information be as accurate as possible, so that disparate events can be correlated easily. Unfortunately, both of those desires often fly right in the face of protecting your users' privacy.

Techniques such as the Privacy Wall are pretty much useless if your log files allow someone to pinpoint exact information about a user's actions. To prevent logs and other records from violating users' privacy, those records should purposefully omit or obscure information that would uniquely identify a user or a user's data.

Early in the development of Wesabe, we hit this problem when one of the developers found an exception on our login page. Since exceptions are reported into our bug system and also emailed to all of the developers, the exception sent around a full record of the action, *including* the developer's login password (since that was one of the POST parameters to the request that failed). After that developer changed his password, we went about making sure that any sensitive information would not be logged in exception reports. Good thing, too -- the next day, one of our early testers hit another login bug, and her action caused an exception report, fortunately containing "'password'=>'[FILTERED]'" rather than her real password. Setting up exception reports to omit a list of named parameters in exception reports is necessary precaution to prevent errors from causing privacy leaks. (In Ruby on Rails, which we use at Wesabe, there is a filter_parameter_logging class method in ActionController::Base that exists for just this purpose.)

Another good datum to filter is IP address. Tracking IP addresses is useful for security auditing and reporting on usage for an application. However, there is usually no need for every log in the application to record the full IP address at every point. We recommend zeroing-out that last two quads of the IP -- changing 10.37.129.2 to 10.37.0.0 -- whenever possible. Most of the time, this information is completely sufficient for application-level debugging, and prevents identifying a specific user on a network by correlating with other network logs.

Google recently announced their intention to mask the last quad of IP address information after 18-24 months, in order to better protect their users' privacy and comply with EU privacy laws.

Likewise, dropping precision on dates -- or dropping dates altogether -- can significantly protect a user. One of our advisors suggested this practice to us after an experience with an anonymous source inside a company, sending him email with information. He noticed that date information, which is often logged with date and hour/minute/second precision, could uniquely identify a sender even if no other information is present.

Obviously some logs will need date information to be useful for debugging, but if possible, dropping whatever precision you can from a date log is good protection.

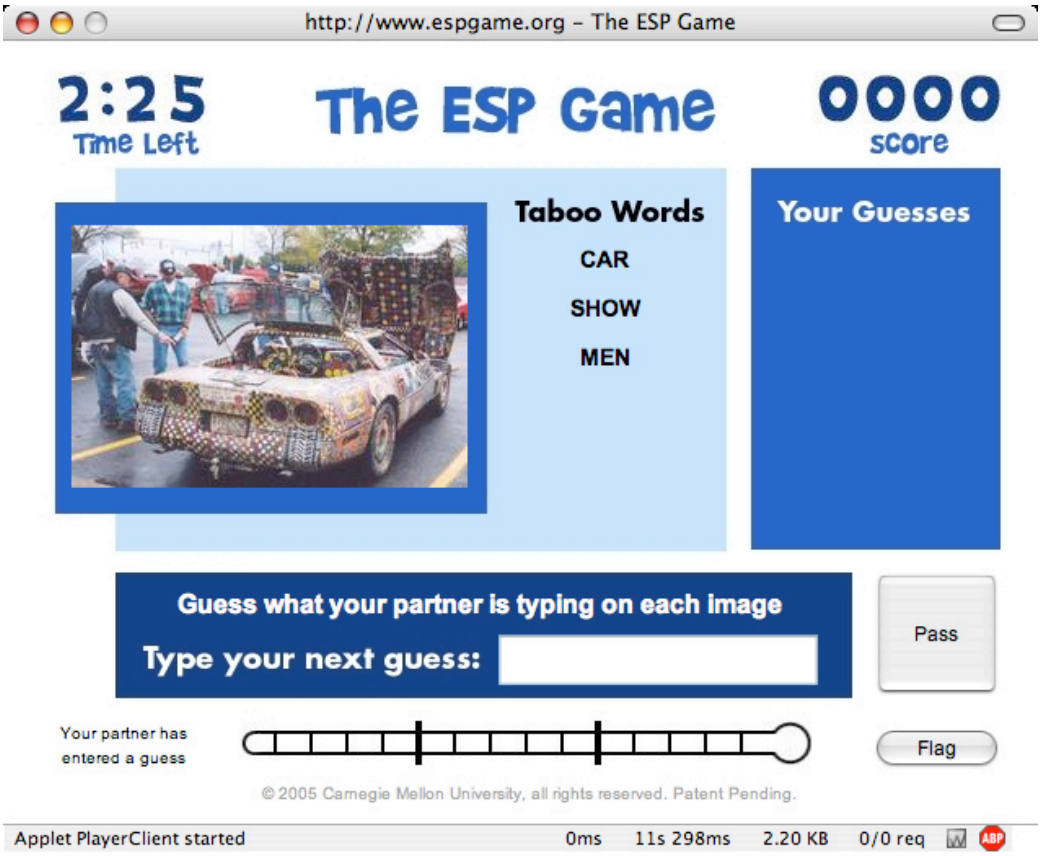
For our application, tracking personal finances, a similar approach could be taken with transaction amounts. A record of all financial transactions, with payee, date, and amount, could be used to identify a particular person even without any additional information. By rounding dollar amounts to the nearest dollar, or randomly selecting a cents amount for each transaction, the application would allow a user to have a good-enough estimate of their spending without penny-level precision. (The privacy threat here would be a request for "all transactions at Amazon on May 13th for $23.45" -- a fairly limited result set, especially since not all Amazon buyers are Wesabe users.)

With all of these filters, you lose a certain amount of precision in your ability to debug a problem when one does occur. One workaround for this is to retain precision and sensitive data where needed, but to write that data to a separate, well-secured file store, and to send a reference to the captured data to the developers. In this way, needed information is centralized and protected under stricter policies, while the email broadcast or bug report announcing the problem is sanitized.

All of these techniques are beneficial when faced with accidental privacy leaks or a desire to avoid having data that would make your service a target of forced data recovery (either criminal, such as a coordinated attack, or governmental, such as a subpoena). However, covering all of the types of data mentioned above in all parts of your application is difficult, and requires care from all developers on the project. Likewise, none of these techniques would prevent a trace and tap (wiretap) order from mandating a change to the application specifically to target a user. Nonetheless, we believe all of the filters mentioned above are both good practice and substantial privacy protections.

4. Use voting algorithms to determine public information

One of the purposes of Wesabe is to aggregate our users' transaction histories around merchants. This allows us to provide pricing information (what is the average price for this plumber's services?) and other useful data (if all the Wesabe members who try this restaurant never go back, it's probably not very good). We faced a problem, though, in developing this feature -- how should we determine which payees are really "merchants" for which we should aggregate and publish data, versus private transactions (such as a check from a wife to her husband), which we definitely should not publish? We decided to use a voting algorithm to help sort this out.



The idea for using a voting algorithm came from an interesting online application called the "ESP Game" (see www.espgame.org). The purpose of the ESP Game was to improve image search engines by getting two people to collaborate on labeling a random image from the web. People who register with the site may start a labeling game at any time, and they are randomly matched based on when the request a game. Presumably, the two participants do not know each other and have no way of communicating except through the game. They are both shown an image at the same time, and asked to enter words that describe the image. If they both enter the same word, they get points in the game and are shown another image (and so on, until a timer runs out). This approach helps improve image searching since two people are agreeing on one term that describes the image, and that image can then be returned for searches on that term. The image is described by people who understand it, rather than having to be analyzed by a computational process that can extract very limited information from it.

Wesabe uses the same approach to determine when we should start publishing aggregate information about a merchant. We wait until a "quorum" of users has identified a transaction as being at a particular merchant name before publishing any information about that merchant. As an example, say that User A downloads their transactions from their bank and uploads them to Wesabe. Each transaction has a description of the payee provided by the bank. These descriptions are often quite obscure, such as:

DEB/14673 SAFEWA 37 19 OAKLS G

User A can then edit the payee to a form they'll more easily recognize, such as:

Safeway

This benefits User A, since their subsequent transactions at Safeway will be automatically converted for them. User B then uploads their own data, and edits one of their transactions to the payee name "Safeway," too. This repeats for Users C, D, E, and so on. When a certain threshold of users have all used the same merchant name to describe one of their transactions, we aggregate the transactions with that payee name and release a page on "Safeway" that contains the data we've collected.

This approach offers several benefits. First, this method works on completely opaque information -- ESP Game does not need image analysis algorithms, and we do not need a battery of regular expressions to comprehend the bank's payee representation. Second, we are essentially defining a merchant based on the amount of transaction activity in which that merchant participates. This allows us to capture a far broader range of merchant information -- for instance, eBay and Craig's List sellers -- than would be available if we simply bought a database of merchant names. Third, users do not need to manually identify each transaction as public or private -- we simply draw the line based on a consensus among our users that a merchant should be public. Finally, no developer or Wesabe employee needs to make the public/private distinction, either (that is, the system is fully automated). When people agree on a merchant name, that name is common knowledge; if enough people agree, it is probably public knowledge.

There are a few drawbacks, of course. We understate the full extent of our database in our public pages, simply because some real merchants have not yet reached a quorum and thus are not published in our index. Likewise, a private individual who collects checks from many Wesabean friends for a group activity may find themselves listed in our index when they should not be. That said, we believe the automation and scope benefits outweigh these drawbacks.

More Information

While we've written above about software techniques for protecting users' privacy, there are also policy techniques for the same ends. We have published a "Data Bill of Rights" to specify the promises we make to our users about the treatment of their data, which any organization is free to copy - www.tinyurl.com/2tujnl.

Marc Hedlund and Brad Greenlee are developers at Wesabe (www.wesabe.com), an online personal finance community for consumers.

A regional event not to be missed!

Info Security • RFID • Card Technology

Now In Bangkok!

Take A Stand At

InformationSecurityAsia 2007

SecureAsia@Bangkok

The Official Trade Exhibition of the (ISC)² Security Leadership Conference

Concurrent events

CardExAsia 2007
The 7th Card Technology Conference & Exhibition

RFID expo ASIA

10 & 11 July 2007
Queen Sirikit National Convention Center
Bangkok • Thailand

www.informationsecurityasia.com
www.cardexasia.com

For more information,
please call 03-6140 6666 | Ms. Gloria Voon or email: gloria@protemp.com.my

Exhibition Organised by: protemp, Protemp Exhibitions Sdn Bhd

Conference Organised by: (ISC)², ACIS

Supporting Organisation: SiPA

Supporting Publication: ConnectWorld, [IN]SECURE, virus bulletin, Infotoday

Information security has finally become mainstream. It is almost a recognized profession, with its own areas of specialization: network security, audit, incident response, forensics, and security management.

Salaries for IS practitioners have been rising constantly, the market for security products and services is much bigger than it was five or ten years ago, and more firms are entering it.

The "security frontier" has moved from firewalls and anti-virus to IM and VoIP security.

However, convincing people and organizations to implement effective security measures has not become easier, so we must ask ourselves:

Is security worth it?

First, let's look at how vendors attempt to sell security. There is usually some FUD (Fear, Uncertainty and Doubt) factor involved. Years ago it was pretty blunt, concentrating on web defacements and Denial of Service (DoS) takedowns "the malicious hackers are coming". Now, sleek statistics from reputable firms or institutions are used, so the language has also become more grown up: "organizations should secure,", "we must ensure that every piece of critical information in a company is appropriately secured", etc.

The problem with these approaches is that the need for security is not personalized enough to trigger a buying decision.

Security as insurance does not work really well because either people can see through FUD and dismiss it as a cheap sales ploy, or because the potential consequences of a lapse in security are not immediately clear.

The issue is quantification. You or your firm may not care much that "virus attacks have increased by X% in the last 12 months", but you may pay more heed if the warning was specific to your industry: "virus attacks against XYZ systems running ABC applications have increased against ACME-industry institutions".

It is of course, easier to sell any type of insurance or advisory services in regulated industries: housing or car insurance, financial services, health care, government. One only has to look at laws like Data Protection Act, HIPAA (US) and Sarbanes-Oxley to see how these created new business opportunities for consulting firms in may countries.

However, for the security practitioner catering for a diverse clientele, another class of arguments must be found, in order to successfully convince clients to buy security services and products.

Fear vs. economics

The problem with using fear to sell security is that it is subject to the stroboscopic light effect: you get used to it, you may not realize when it really is bad and you could collapse under it not knowing why. Fear also works if you are naturally risk averse. But, it doesn't work if you've never experienced the touted bad consequences or, if you are not risk averse.

Basic economics tells us that a free market for one specific product or "good" (let's leave it "good", please, as this is the basic economics terminology) will converge to an equilibrium position, where supply equals demand, at a certain price P per unit. However, security is a complex issue, where many remedies are required for different aspects, so such a simplistic view may not be enough to look at when selling our security wares.

Besides, in some cases it is difficult to determine what "one unit" of that product or good may be and company purchasing decisions are not as simple as the theoretical academic models may suggest.

Some industry participants complain about increased competition as a factor in depressing their security sales. However, let's take a quick look at a typical large European country as a "market" for example Germany or the UK. This reveals that there will be, on average, ten firms providing Managed Security Services (MSS), with the biggest firm holding about a 20% market share. There will also be around 30 firms providing various security consulting services and we'll perhaps find one with the biggest market share of 10%. This would mean HHI indexes of competitive intensity of 526 and 135 respectively.

Glancing back at our economics textbooks, we find that this is not an overly competitive market to be selling security services in, even if we accept that defining the actual 'market' may be the trickiest part of this type of analysis.

Security ROI

Then there is another way: proving security ROI. Of course, ROI is a valid financial tool. In the security industry, however, every vendor seems to have one, which is slightly different from other vendors' and which 'proves' that buying that vendor's product or service makes the best economic sense.

For example, I'm sure we've all seen the statistics stating that having someone else to manage your company's firewalls is a 400% ROI over one year, when compared to managing them in house.

Whenever we are confronted with such figures, there are several things we need to ask: How many firewalls do these figures refer to? How many different technologies? Were these devices located in one company office, or distributed on a country or continental level? What service levels do the costs refer to? How many clients participated in the survey, how many vendors?

Many ROI calculations adopt a simplistic and/or simplified view of the underlying costs. They also tend to disregard 'communications' costs, human and skills costs, dealing with process or operational exceptions, with network upgrades.

One must always seek to understand the assumptions of any ROI model.

As a final note, an IDC study in 2003 found that 83% of companies do not track ROI for their security investments. Things are likely to have changed, but caution and scrutiny should still be applied to ROI models.

Buy or Build and the Individual Perspective

From a client perspective, a lot of energy is usually spent debating whether security is best kept 'in house' and delivered by client's own personnel (or built by internal efforts), or is it better to outsource or buy 'off the shelf'.

Because security is essentially a trust issue, the natural inclination is to keep it in house, shrouded in secrecy. We know that, from a technical perspective, 'security through obscurity' is not good practice. The encryption algorithms that become standards are subjected to scrutiny for years before being widely adopted.

From an economic perspective, there will be security tasks which are more efficiently carried out by an outsourcer (e.g. managing firewalls or IDS), and some which are more suited for in house delivery (e.g. fraud and incident investigations), if skills exist in-house. A good provider will remind the client that they always retain the full responsibility for their organization's security posture, even if some security tasks have been 'delegated' to hands and brains outside the firm.

Economics also plays a part in everyday decisions taken by individuals (employees) when it comes to doing the "right security thing." We must ask whether security is facilitating or hindering their jobs. Is it 'cheaper' to comply with or to flaunt security rules and procedures? What is the employee's time-horizon when it comes to making security decisions?

The answer is making security a business enabler and with a relatively low compliance cost. Otherwise, individual cost-benefit analysis decisions (e.g. about how often to change their system password) may trump the best laid out corporate security strategies.

Fear, Risk and Economics

So, where does this discussion leave us? Are we any wiser about how to make security more widely adopted -- and encouraging clients to spend more on their security budgets?

The main idea we need to tell our clients is that security can be a business enabler and not just an "IT cost," Let's stop viewing information security through the prism of fear and start to quantify it and, more generally, technology risks and threats in Economic terms. At the end of the day, buying decisions are made by business people and not necessarily by technologists, so security investment decisions must make business sense in order to be adopted.

We need to articulate the economics angle whenever we buy or sell security. This should enable us to make rational (economics-based, rather than fear-based) decisions when it comes to security.

Let's not allow fear or the latest technological fad to cloud our judgement. We can and should place economic value on security measures, be they technology, people or processes.

If we adopt an economic approach, we can demystify Information Security and make it a friend of the organization. This should benefit both the 'buy' and the 'sell' side of the market.

Finally

Next time you turn on your system at work and it asks you to change your password, you know you're facing an economic decision. It is always cheaper to comply than to clean up after a security incident.

The economic benefit of complying with the security policy will accrue to both you and your organization. Then, you can concentrate on doing what you do best, knowing you've done "your bit" to keep your information safe. You know it makes (economic) sense.

Ionut Ionescu is the Director of Security Services for EMEA at Nortel. He has over 14 years of ICT industry experience and specializes in systems and network security. His work involves designing, implementing and auditing enterprise, carrier and e-business infrastructures.

Hacking the Cisco NAC - NACATTACK
http://www.net-security.org/article.php?id=1001

At Black Hat Europe we met Dror-John Roecher and Michael Thumann who were able to hack the Cisco NAC solution by exploiting a fundamental design flaw. In this video they illustrate how they worked towards this discovery and give us some exploit details. It is not their intention to simply release a tool, they want the audience to understand how Cisco NAC works and why it is not as secure as Cisco wants us to believe.

Web Application Security with Jeremiah Grossman
http://www.net-security.org/article.php?id=993

Jeremiah Grossman is the CTO of WhiteHat Security. In this video he talks about the differences between web application security and network security, the assessment process in general, logical vunerabilties as well as Web 2.0 security developments.

New Security Features in Internet Explorer 7
http://www.net-security.org/article.php?id=1003

Markellos Diorinos from the IE team at Microsoft introduces the new security features in IE 7 and speaks about extended validation SSL certificates. He also covers the Certification Authority Browser Forum whose members apart from Microsoft include also the Mozilla Foundation, Opera Software and KDE.

Practical Tips for Safer Computing
http://www.net-security.org/article.php?id=989

Reliable and user-friendly encryption software for Pocket PCs. It encrypts all sensitive information keeping it secure and protected, even in such catastrophic cases when the Pocket PC is lost or stolen. Protects information with NIST-approved AES 256-bit encryption.

A firewall is a software which is used to control the movement of network traffic according to a set of rules. Linux ships with an excellent GPLed firewall called iptables.

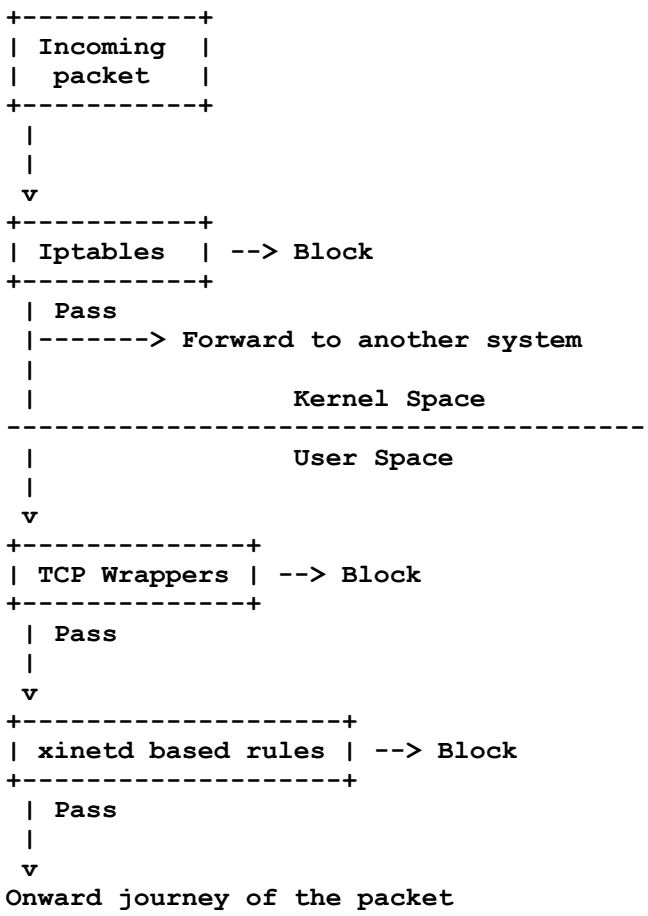
Here I will explain the rudimentary concepts in using iptables. Iptables is a packet filter which supersedes ipchains. It forms the first point of contact for packets that flow into or out of your network. In fact the packets are checked in the following order when it reaches your computer.

As you can see in the diagram on the following page, iptables works in the kernel space. Here I will give a simple introduction to this very useful and powerful but cryptic form of securing a network. If you are using kernel 2.4 and above, you will be using iptables. Its functionality is directly compiled into the Linux kernel as a module (netfilter). The policies are checked at the layers 2, 3 and 4 of the OSI Reference Model. That is 'Datalink', 'Network' and 'Transport' layer. It is very fast because only the packet headers are inspected. There is a wonderful tutorial on configuring firewalls using iptables at Netfilter.org. But if you are lazy (like me) to plod through over 130 pages of the tutorial, then read on.

Netfilter is divided into tables which in turn are divided into chains and each can have different targets.

Netfilter tables

There are three inbuilt tables. They are as follows:
1. Filter - This is the default table if no table name is specified in the rule. The main packet filtering is performed in this table.



2. NAT - This is where Network Address Translation is performed. For example, if you are using your machine as a router or sharing your internet connection with other machines on your network, you might use the NAT table in your rule.
3. Mangle - This is where a limited number of 'special effects' can happen. This table is rarely used.

Netfilter chains

Each table has a number of inbuilt chains and these are as follows:

For filter table
1. INPUT - Handles packets destined for the local system, after the routing decision.
2. OUTPUT - This chain handles packets after they have left their sending process and before being processed by POSTROUTING (applicable to nat and mangle) chain.
3. FORWARD - This chain handles packets routed through the system but which are actually destined for another system on your LAN.

For the NAT table
1. OUTPUT - see explanation above.
2. PREROUTING - This is the entry point of packets on their arrival. All packets first pass through this chain before even passing through the routing decision.
3. POSTROUTING - If PREROUTING is the first chain that a packet encounters, POSTROUTING is the final point of contact for any packet before it leaves the system.

For the mangle table
The mangle table contains a union of all the chains in the filter and NAT tables. Over and above the built-in chains, you can also have custom user defined chains too. Usually you use a custom chain to group a series of actions together before passing it to one of the built-in chains.

Rule targets

Each chain can have different targets. They are broadly classified into builtin and extension targets. The target names must be preceded by the option -j (as in jump).

The targets are outlined on the following page.

Built-in targets
• DROP - As the name indicates, discards the packet. No message is relayed back to the sender of the packet.
• ACCEPT - Allows the packet to pass through the firewall.
• RETURN - This is a built in target which is created for convenience. Because most targets do not return. That is if a packet matches a rule, the checking of that packet ceases and the chain is exited.

Extension targets
• LOG - This is used to log messages to your system of offending or blocked packets. Usually, control is passed to the syslog facility which logs the message to the file **/var/log/messages** and then returns the control back to the iptables.
• REJECT - If this target is used, a notice is sent back to the sender. Like for example "you are denied access to this service" message.
• DNAT - Used for destination NAT ie rewriting the destination IP address of the packet.
• SNAT - Used for rewriting the source IP address of the packet.
• MASQUERADE - This is used to do either SNAT or DNAT. Basically this target is used to set up internet connection sharing in your network.

All extension targets are usually implemented in special-purpose kernel modules.

To know which all modules are loaded on your system, execute the command:

```
# lsmod |grep ipt


ipt_limit               1792  8
iptable_mangle          2048  0
ipt_LOG                 4992  8
ipt_MASQUERADE          2560  0
iptable_nat            17452  1 ipt_MASQUERADE
ipt_TOS                 1920  0
ipt_REJECT              4736  1
ipt_state               1536  6
ip_conntrack           24968  5
ipt_MASQUERADE,iptable_nat,ip_conntrack_irc,ip_conntrack_ftp,ipt_state
iptable_filter          2048  1
ip_tables              13440  9
ipt_limit,iptable_mangle,ipt_LOG,ipt_MASQUERADE,iptable_nat,ipt_TOS,ipt
_REJECT,ipt_state,iptable_filter
```

These are the modules that are loaded on my system. As you can see, all modules that start with the name 'ipt_' are extension modules. So in the above listing, iptable_nat module uses a extension module called ipt_MASQUERADE. And to use the LOG extension target, you should have loaded the ipt_LOG extension module.

What follows is a few examples.

```
# iptables -t filter -A INPUT -p tcp -s
192.168.0.5 -j DROP
```

This rule can be read as follows. In the filter table (-t), append (-A) to the INPUT chain the rule that, all packets using the protocol (-p) tcp and originating (-s) from the remote machine with IP address 192.168.0.5 should be dropped (-j DROP).

```
# iptables -A FORWARD -s 0/0 -p TCP -i
eth0 -d 192.168.5.5 -o eth1 -- sport
1024:65535 --dport 80 -j ACCEPT
```

This rule reads as follows: Append (-A) to the FORWARD chain, the rule that all packets coming from anywhere (-s 0/0) using the protocol (-p) TCP and using unreserved ports (--sport 1024:65535), incoming (-i) through the interface eth0 , and destined (--dport) for port 80 on address (-d) 192.168.5.5 and outgoing (-o) through the interface eth1 should be accepted.

```
# iptables -L
```

List (-L) all the rules in the iptables.

```
# iptables -F
```

Flush (-F) all the rules from iptables. Now you can start afresh.

```
# iptables -A OUTPUT -j LOG
# iptables -A INPUT -j LOG
```

Log all incoming and outgoing rules in the filter table to the file `/var/log/messages`.

Iptables is a very powerful and flexible tool and can be used to block anything or everything that comes into or goes out of your computer.

Usually the commands that you executed above will reside in memory but will not persist across rebooting. Which means, once you reboot, all your rules are lost and you have to start all over. In order to avoid this, you save your rules into a file which is read by the OS when you reboot your machine. In RedHat/Fedora, the iptables rules are saved in the file `/etc/sysconfig/iptables`. You save it using the programs iptables-save as follows:

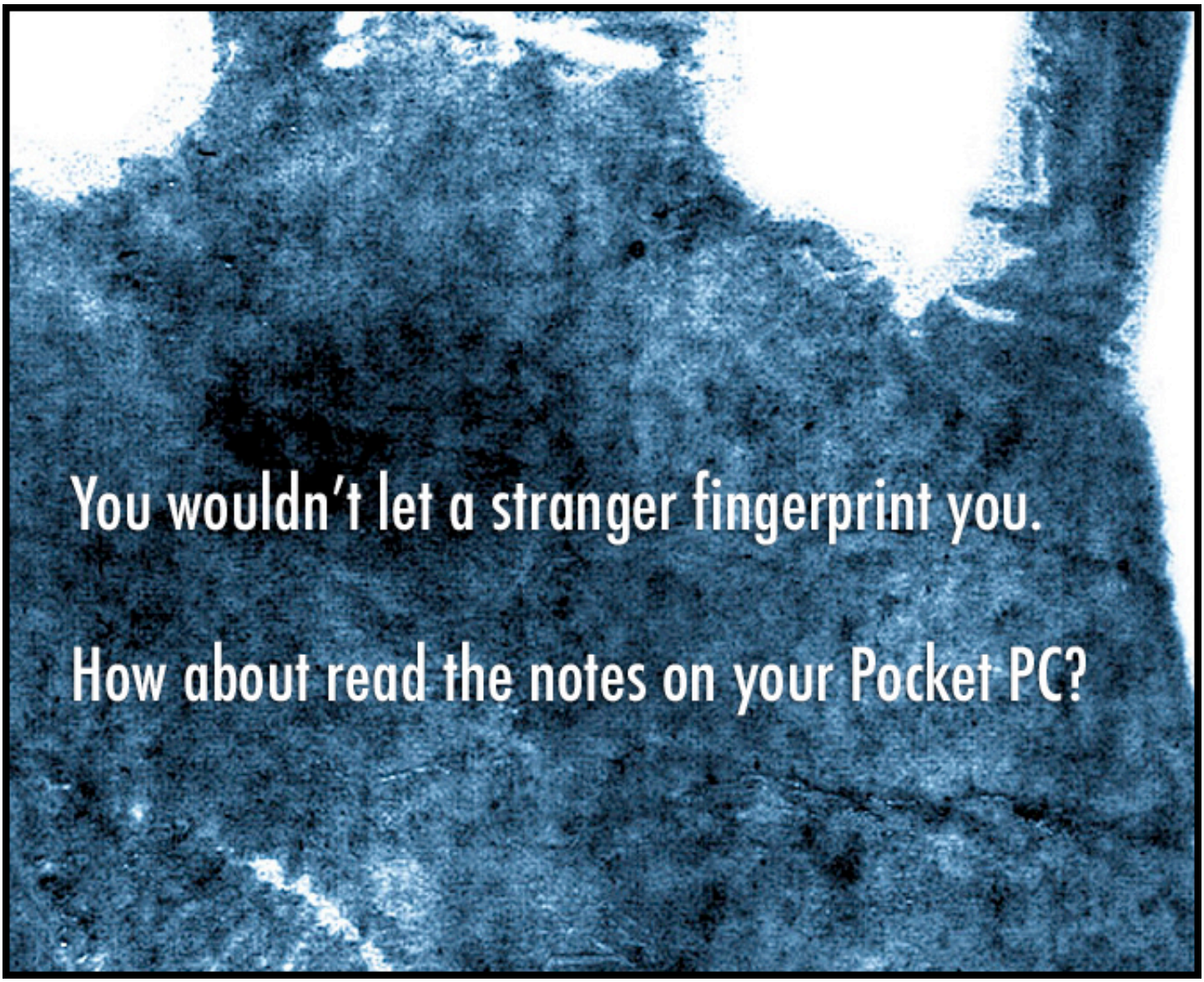
```
# iptables-save > /etc/sysconfig/iptables
```

or do the following:

```
# service iptables save
```

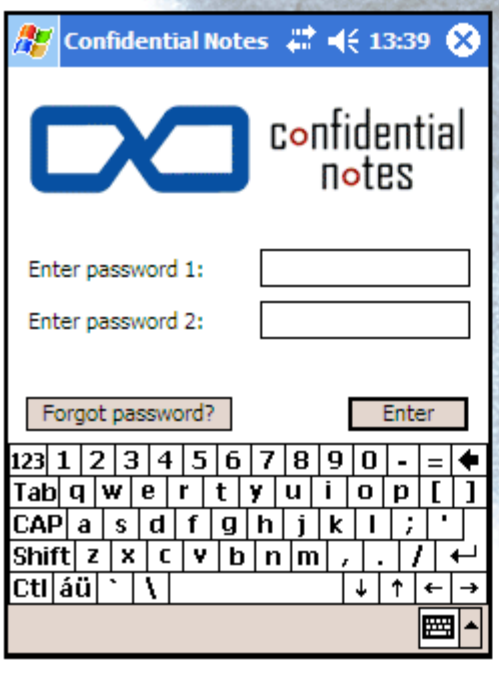
There is another script called iptables-restore which can be used to load the rules from a file into memory.

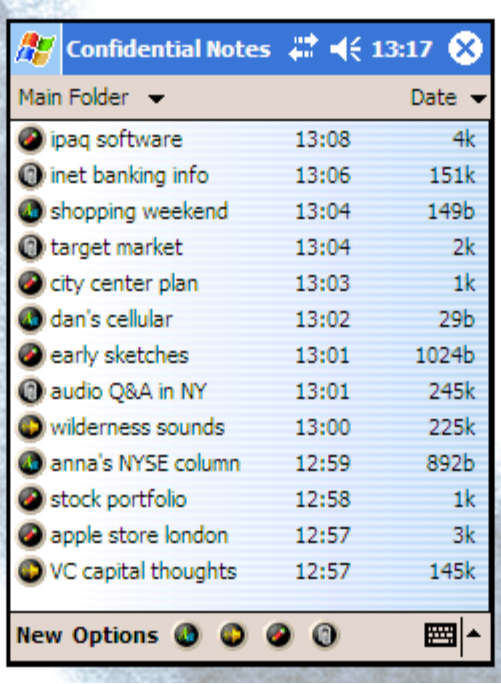
Ravi Kumar is a Linux enthusiast who maintains a blog related to Linux, open source and free software at linuxhelp.blogspot.com.



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





An impressive crowd of security professionals, high profile speakers, hackers as well as incognito individuals going only by their first name, gathered at the Moevenpick Hotel Amsterdam City Centre in the Netherlands to attend one of the most important security events in the world - Black Hat Briefings & Training Europe.

The most intensive part of Black Hat is certainly the training and new for this year were Metasploit 3.0 Internals (by Matt Miller, aka skape), Web Application (In)security (by NGS Software) and Live Digital Investigation -Investigating the Enterprise (by WetStone Technologies).

The Briefings were filled with fascinating presentations covering a variety of topics, here are some of them:

• RFIDIOts!!! - Practical RFID hacking (without soldering irons) by Adam Laurie.
• SCTPscan - Finding Entry Points to SS7 Networks & Telecommunication Backbones by Philippe Langlois.
• Data Seepage: How to Give Attackers a Roadmap to Your Network by David Maynor & Robert Graham.
• Software Virtualization Based Rootkits by Sun Bing.
• GS and ASLR in Windows Vista by Ollie Whitehouse.
• Attacking the Giants: Exploiting SAP
•Internals by Mariano Nuñez Di Croce.
• Making Windows Exploits More Reliable by Kostya Kortchinsky.

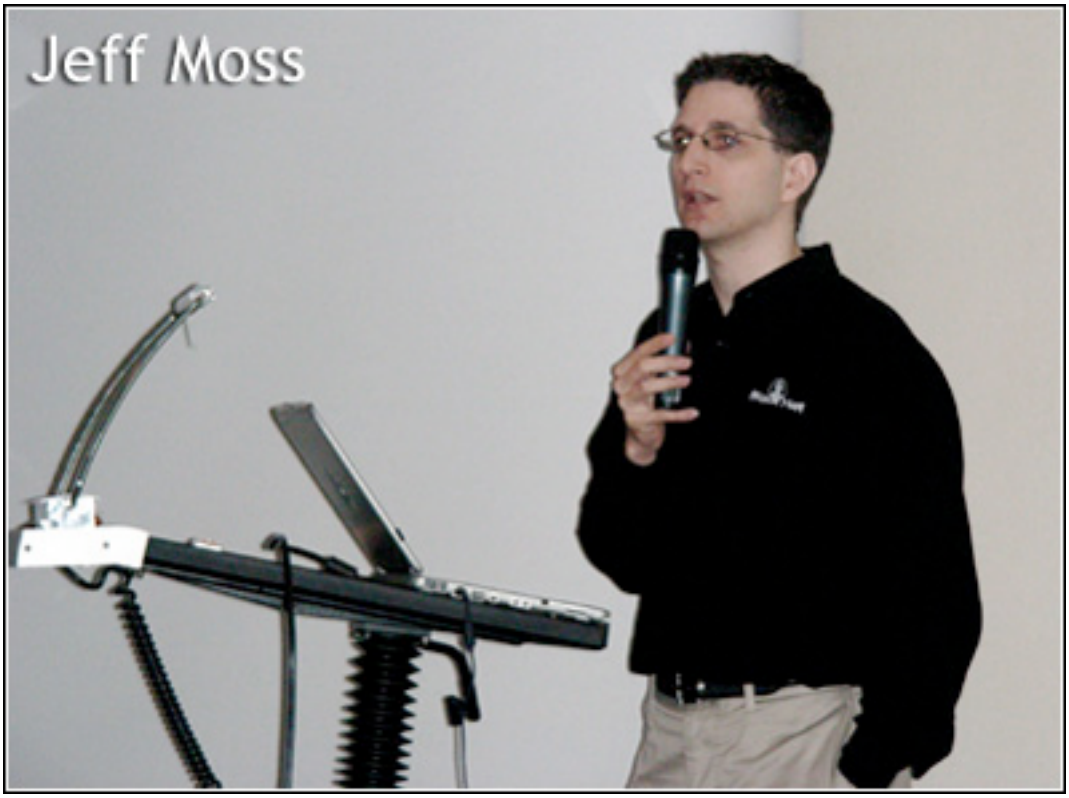
A variety of IT companies watch closely the materials presented at Black Hat as they are always very cutting-edge and sometimes present holes in very popular software and operating systems.

This year, a plethora of attention was focued towards Nitin Kumar and Vipin Kumar that presented "Vboot Kit: Compromising Windows Vista Security". They got an invitation to dinner from Microsoft and we could see they were very excited about it. After all, they came from India to get a job in the industry.

Under the microscope were Dror-John Roecher and Michael Thumann since they spoke about Cisco in their "NACATTACK" presentation. Cisco wasn't tearing up conference material and we learned that they just had a pleasant conversation with the authors. Some change from the 2005 incident with Michael Lynn from ISS where Cisco acted like a bully. Lessons learned!

If you need credits towards a certification, you'd be glad to know that ISC2 credits are available to everyone that attends. The large growth in the number attendees (from 300 to around 450 this year) and the high quality of the presented material, Black Hat Europe is proving to be the best event of its kind in this part of the world. If that's not enough, the Google folks with the "Hiring Squad" T-shirts should be enough for anyone having the skills and looking for a high-profile job offer.

Photos are a courtesy of Gohsuke Takama.



This is a friendly guide to computer certificates and their practical usage for VPN and secure Web access, using open source software.

As a security professional, it is my responsibility to make information security more accessible and understandable for others. Far too often, security is compromised because administrators or even security professionals do not know how to use certain technologies. This unfortunately increases the risk and devaluates the information security profession in people's eyes.

I am going to suggest a solution to two of many security problems that organisations face today:
• Secure VPN access to an office network from the Internet.
• Secure access to Extranet applications for employees or 3rd parties.

1. A little theory around digital certificates

It would be unprofessional to jump straight to real life examples without setting the scene by explaining the theory behind certificates.

1.1 Terminology

Digital certificate - there is are a lot of definitions of digital certificates available on the Internet. And to add to them, here is mine. In the simplest form a digital certificate is a passport proving an identity of the holder of the private key. Certificates are issued (usually) by certificate authorities in the process that consist of a) verifying identity of the subject, b) checking for the correctness of details in the certificate request and c) signing the request with the certificate authority private key.

Private key - a private part of the key pair generated. This part is a secret and must be kept protected. One way of protecting is using encryption and pass-phrase. private key is used to sign message and decrypt data. Public key - the other half of the pair. The unique mathematical relationship means the data encrypted with a public key can only be decrypted with the corresponding private key, and vice versa. At least until such time when

computers will be smart enough to process operations with long numbers fast enough. See RSA topic on Wikipedia for greater level of detail.

Digital signature - a cryptographic function where a private key of the signing subject is used to encrypt cryptographic hash of the object (usually message, certificate request, file or packet).

Certificate chain - concatenated certificates starting from the issuing certificate authority up to the root certificate authority. Certificate chain is rather necessity as the validity of a certificate depends on complete path from the certificate to the root certificate authority. usually, only root certificate authority certificate is trusted by a computer and it would be impractical to import all sub certificate authorities leading to the root one. Certificate chain is used when a client tries to connect to a server, the client trusts root CA but the server has got a certificate issued by a sub CA of the root CA. The server then sends it own certificate plus the chain file for the client to establish the certificate path and trust the server's certificate.

Certificate Revocation List (CRL) - List of revoked certificates signed by private key of issuing CA. This is used to check whether a certificate, while still within its validity period, still holds its trust given by CA.

1.2 Theory

A digital certificate is a certificate that attests that the public key belongs to the specific subject, like a person, computer or web site. The certificate contains a signature issued by an issuer, which can be either Certificate authority, another subject, or self signature.

The certificate should include:
• subject name
• issuer subject name
• validity (start and end)
• purpose (like client, server, encryption only, signature only, CA, S/MIME)
• public key to be signed
• digital signature

Optionally it can include:
• revocation list locations
• certificate authority statement

Today, the most common certificates are so called X509 certificates but watch XML based methods, like XKMS.

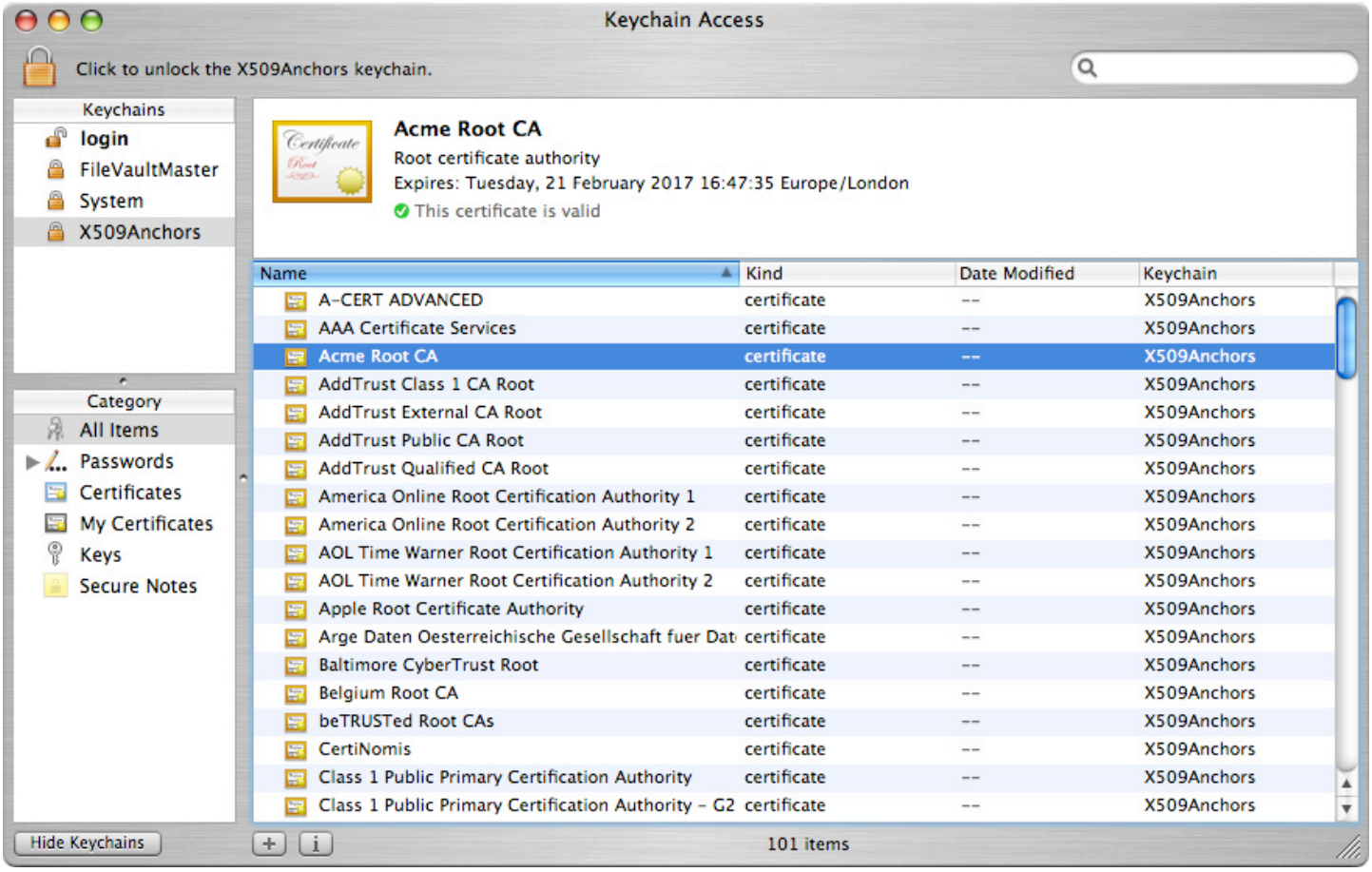
Certificates are the tool to implement trusts. At To most, certificates are used to prove that a web site you are purchasing goods from actually belongs to the company that owns the domain name. This trust is facilitated by the so called "Certificate Authority" that your web browser or computer trusts. The list of such certificate authorities has been pre-populated by operating system or web browser producers.

Such certificate authorities make actually make a very good business out of these certificates and that is not going to change for some time. On the following page is such list from my Mac.

Similarly, this list can be viewed in other operating systems and browsers. In Internet Explorer, go to Tools, Internet Options, Privacy, Certificates and select Trusted Root Certificate Authorities tab.

So how does your web browser know when to trust a certificate presented by a web site? It simply looks up whether an issuing certificate authority is listed in the trusted root certificate authorities list, whether the current time falls within the certificate validity boundaries and whether the website fully qualified domain name (FQDN) is the same as stored within the server's certificate. Finally it looks at whether the certificate has been issued by a certificate authority that is on the list of trusted ones. Commercial certificate authorities, those which certificates have been pre-populated in operating systems, take great care when issuing certificates to companies. As you can imagine verifying the identity of a subject is the most important think to retain the trust that users have in these CAs

X509 certificates are widely used and there are various forms these can be stored. The most used formats are PEM and DER. You can also see PKCS standards, which is RSA developed suite of formats for various cryptographic functions. The most used are PKCS1,7,10,11 and 12.



Let's have a look at a typical X509 certificate for a WEB server.

RAW format, PEM encoded (Base64) certificate:

```
-----BEGIN CERTIFICATE-----
MIIGfTCCBGWgAwIBAgIBATANBgkqhkiG9w0BAQUFADBiMQswCQYDVQQGEwJVSzEPMA0GA1UEBxMGTG9uZG9uMR
EwDwYDVQQKEwhBY211IEx0ZDEUMBIGA1UECxMLSVQgU2VjdXJpdHkxGTAXBgNVBAMTEEFjbWUgRXh0cmFuZXQg
Q0EwHhcNMDcwMzA4MjAyNDEwWhcNMTAwMzA3MjAyNDEwWjBlMQswCQYDVQQGEwJVSzEPMA0GA1UEBxMGTG9uZG
9uMREwDwYDVQQKEwhBY211IEx0ZDEUMBIGA1UECxMLSVQgU2VjdXJpdHkxHDAaBgNVBAMTE2V4dHJhbmV0LmFj
bWUuY28udWswggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQCbXC0SCIUj5o+zIyR/aZyBxX550wF6k2
Rf1byRQ/wSoqGdwVNKbnFI/9nn0jXwXSUAOQ+jQiLzC1OJd8VzgPlRt/Jr8Ac/Mxs0lNancv9DatQMMjxpfykt
FimYEbEbAIT+XyIv6c9qO8uesbHzvfmfNsxVslN8gs2qymsv98jtJAahx3jHlDYnK8ZLEre+Xo01jUi+8ibHNj
ZGVWZrglZSmPTQRpp/4p4AerwyzMZZkCAdyxF08TLGg9NTEDAuV5tASBLwZbAqKIQMEeTdu2CVuiYnqrAWnfnF
A1RjOMiOkMiV5PQL6iJCw81MGpuqtOD+d0sOYnaKHtk6hfcaEaqE4CXRKFfvMTNNLz7Bkyp6pD/7SDB2BD2UrG
hFP8onORlTs8lbWLMbfY+K6BEmWdmxRnWuls6Qva8kicujCd5azbJA6XMtHr15CvzgW5PEZ9lziuPM/dBrpjKi
YDpAEZYOLkOHVTxKFZPVvuHM05us0pAcXRMoMz4HTJhXVpFqHPHQ7dHfx6I37NXPlGcybhg8iWfiirW39OksSV
NPblo8b+31cDfaguBDkLycLn2nqKfG3Ty1FKLWCbolNbXB6ZoySKvwTNX+UHLa9il7YxFEyG1zLgZ2SDqO5u5f
C5PLmaJUGikjtAhKQLnZhRDzjHF+RTE8HgzJz4O1s9FvogvyqQIDAQABo4IBOTCCATUwCQYDVR0TBAIwADARBg
lghkgBhvhCAQEEBAMCBkAwKwYJYIZIAYb4QgENBB4WHFRpbnlDQSBHZW5lcmF0ZWQgQ2VydGlmaWNhdGUwHQYD
VR0OBBYEFBgLKxchYfg2UimLMoJaF3WUvdGZMIGyBgNVHSMEgaowgaeAFKLDdUD2kD8jjC84WIgF9OfyARwSoY
GLpIGIMIGFMQswCQYDVQQGEwJVSzEPMA0GA1UEBxMGTG9uZG9uMREwDwYDVQQKEwhBY211IEx0ZDEUMBIGA1UE
CxMLSVQgU2VjdXJpdHkxFTATBgNVBAMTDEFjbWUgUm9vdCBDQTElMCMGCSqGSIb3DQEJARYWaXQuc2VjdXJpdH
lAYWNtZS5jby51a4IBAjAJBgNVHRIEAjAAMAkGA1UdEQQCMAAwDQYJKoZIhvcNAQEFBQADggIBAI20uQyEFfQP
p7u2I+Hbz2IRcZWvuH4rpeLLJ+MA3ig3CCk/27dDUy39JecS+sB+oD5dXH2HeNP/giwvxST2lk75Acy7KOFeyn
YaMvpYFNpuW0mZ+KqmTmfmU1MDkB/18WXe07Ce2Q7auHpAB10b8EXx4va1odWnWi3/rDnxU4zTelDUXsEe+RZB
CjGR5OQjZ0aKN71G2g0QMDVnFZ0jmE6BZpG6paa07n2T9YBzrIaCQ52oUjxegqvNTZX4zTHm488zfbQvZCRO3k
Ay7zfORBxUKe5ru0Cnl0oLaK5lB8sLuZdrSHP1J+m5iMfDdw119gpN7HOk51JcRaNIpotQNHfsYB/I0RYg5yAh
TBM6Zhqj4n8XNiLOc3JXCxrUM8kvbkcmCdKWjixVn/sY5A5j7Jqu9P0nlHzkHXznItL7k8lgBUDRlPh7VJAWXx
VhMhHVUBWoFw/STSMDhYreafZbE4p1jyRsKVisFjTh4kBuJGdUwoHqg0vhtnXr4BtZ046Am04Z4B/F6H1M4aY0
4+NJXR5iFbJcHu08hHV/NRXYzfO/YAgr6Tf0Nat5PqcCeRJ4gUsgXb+OkueqrdBSB2WAi5uB2xzlKU5/V8MPp3
mRf93gtjVJaFEkVm8B2TyszxKoslBInuHcZbZIfV86Agwy+p2sQQw0gHhdcqmfWMFyGpAc
-----END CERTIFICATE-----
```

Let's see the same certificate in more readable form.

```
:/etc/apache2/ssl$ openssl x509 -noout -text -in extranet.acme.co.uk-
cert.pem
Certificate:
    Data:
          #refers to V3 extension used
        Version: 3 (0x2)
          #serial number used by CA, it does not have to be incrementing but unique in
CA's database
        Serial Number: 1 (0x1)
        Signature Algorithm: sha1WithRSAEncryption  #algorithm used to sign public key
of a server by CA's private key
        Issuer: C=UK, L=London, O=Acme Ltd, OU=IT Security, CN=Acme Extranet CA #CA's
distinguished name
        Validity
            Not Before: Mar  8 20:24:10 2007 GMT
            Not After : Mar  7 20:24:10 2010 GMT
        Subject: C=UK, L=London, O=Acme Ltd, OU=IT Security, CN=extranet.acme.co.uk
#CN is important attribute. it is checked against DNS name by web browsers
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (4096 bit)
                Modulus (4096 bit):   #Public key belonging to the server
                    00:9b:5c:2d:12:08:85:23:e6:8f:b3:23:24:7f:69:
                    9c:81:c5:7e:79:d3:01:7a:93:64:5f:d5:bc:91:43:
                    fc:12:a2:a1:9d:c1:53:4a:6e:71:48:ff:d9:e7:d2:
                    35:f0:5d:25:00:39:0f:a3:42:22:f3:0b:53:89:77:
                    c5:73:80:f9:51:b7:f2:6b:f0:07:3f:33:1b:34:94:
                    d6:a7:72:ff:43:6a:d4:0c:32:3c:69:7f:29:2d:16:
                    29:98:11:b1:1b:00:84:fe:5f:22:2f:e9:cf:6a:3b:
                    cb:9e:b1:b1:f3:bd:f9:9f:36:cc:55:b2:53:7c:82:
                    cd:aa:ca:6b:2f:f7:c8:ed:24:06:a1:c7:78:c7:94:
                    36:27:2b:c6:4b:12:b7:be:5e:8d:35:8d:48:be:f2:
                    26:c7:36:36:46:55:66:6b:82:56:52:98:f4:d0:46:
                    9a:7f:e2:9e:00:7a:bc:32:cc:c6:59:90:20:1d:cb:
                    11:74:f1:32:c6:83:d3:53:10:30:2e:57:9b:40:48:
                    12:f0:65:b0:2a:28:84:0c:11:e4:dd:bb:60:95:ba:
                    26:27:aa:b0:16:9d:f9:c5:03:54:63:38:c8:8e:90:
                    c8:95:e4:f4:0b:ea:22:42:c3:cd:4c:1a:9b:aa:b4:
                    e0:fe:77:4b:0e:62:76:8a:1e:d9:3a:85:f7:1a:11:
                    aa:84:e0:25:d1:28:57:ef:31:33:4d:2f:3e:c1:93:
                    2a:7a:a4:3f:fb:48:30:76:04:3d:94:ac:68:45:3f:
                    ca:27:39:19:53:b3:c9:5b:58:b3:1b:7d:8f:8a:e8:
                    11:26:59:d9:b1:46:75:ae:96:ce:90:bd:af:24:89:
                    cb:a3:09:de:5a:cd:b2:40:e9:73:2d:1e:bd:79:0a:
                    fc:e0:c3:93:c4:67:d9:73:8a:e3:cc:fd:d0:6b:a6:
                    32:a2:60:3a:40:11:96:0e:2e:43:87:55:3c:4a:15:
                    93:d5:be:e1:cc:d3:9b:ac:d2:90:1c:5d:13:28:33:
                    3e:07:4c:98:57:56:91:6a:1c:f1:d0:ed:d1:df:c7:
                    a2:37:ec:d5:cf:94:67:32:6e:18:3c:89:67:e2:8a:
                    b5:b7:f4:e9:2c:49:53:4f:6e:5a:3c:6f:ed:f5:70:
                    37:da:82:e0:43:90:bc:9c:2e:7d:a7:a8:a7:c6:dd:
                    3c:b5:14:a2:d6:09:ba:25:35:b5:c1:e9:9a:32:48:
                    ab:f0:4c:d5:fe:50:72:da:f6:29:7b:63:11:44:c8:
                    6d:73:2e:06:76:48:3a:8e:e6:ee:5f:0b:93:cb:99:
                    a2:54:1a:29:23:b4:08:4a:40:b9:d9:85:10:f3:8c:
                    71:7e:45:31:3c:1e:0c:c9:cf:83:b5:b3:d1:6f:a2:
                    0b:f2:a9
Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE              #this certificate cannot sign other certificates
(act as Sub CA)
            Netscape Cert Type:
                SSL Server
            Netscape Comment:
                TinyCA Generated Certificate
```

```
X509v3 Subject Key Identifier:
                18:0B:2B:17:21:61:F8:36:52:29:8B:32:82:5A:17:75:94:BD:D1:99
            X509v3 Authority Key Identifier:        #what namespace this certificate
belongs to. leads to Root CA and show which Sub CA (serial 2) was used
                keyid:A2:C3:75:40:F6:90:3F:23:8C:2F:38:58:88:05:F4:E7:F2:01:1C:12
                DirName:/C=UK/L=London/O=Acme Ltd/OU=IT Security/CN=Acme Root
CA/emailAddress=it.security@acme.co.uk
                serial:02

            X509v3 Issuer Alternative Name:
                <EMPTY>

            X509v3 Subject Alternative Name:
                <EMPTY>

    Signature Algorithm: sha1WithRSAEncryption
        8d:b4:b9:0c:84:15:f4:0f:a7:bb:b6:23:e1:db:cf:62:11:71:
        95:af:b8:7e:2b:a5:e2:cb:27:e3:00:de:28:37:08:29:3f:db:
        b7:43:53:2d:fd:25:e7:12:fa:c0:7e:a0:3e:5d:5c:7d:87:78:
        d3:ff:82:2c:2f:c5:24:f6:96:4e:f9:01:cc:bb:28:e1:5e:ca:
        76:1a:32:fa:58:14:da:6e:5b:49:99:f8:aa:a6:4e:67:e6:53:
        53:03:90:1f:f5:f1:65:de:d3:b0:9e:d9:0e:da:b8:7a:40:07:
        5d:1b:f0:45:f1:e2:f6:b5:a1:d5:a7:5a:2d:ff:ac:39:f1:53:
        8c:d3:7a:50:d4:5e:c1:1e:f9:16:41:0a:31:91:e4:e4:23:67:
        46:8a:37:bd:46:da:0d:10:30:35:67:15:9d:23:98:4e:81:66:
        91:ba:a5:a6:b4:ee:7d:93:f5:80:73:ac:86:82:43:9d:a8:52:
        3c:5e:82:ab:cd:4d:95:f8:cd:31:e6:e3:cf:33:7d:b4:2f:64:
        24:4e:de:40:32:ef:37:ce:44:1c:54:29:ee:6b:bb:40:a7:94:
        ea:0b:68:ae:65:07:cb:0b:b9:97:6b:48:73:f5:27:e9:b9:88:
        c7:c3:77:0d:75:f6:0a:4d:ec:73:a4:e7:52:5c:45:a3:48:a6:
        8b:50:34:77:ec:60:1f:c8:d1:16:20:e7:20:21:4c:13:3a:66:
        1a:a3:e2:7f:17:36:22:ce:73:72:57:0b:1a:d4:33:c9:2f:6e:
        47:26:09:d2:96:8e:2c:55:9f:fb:18:e4:0e:63:ec:9a:ae:f4:
        fd:27:94:7c:e4:1d:7c:e7:22:d2:fb:93:c9:60:05:40:d1:94:
        f8:7b:54:90:16:5f:15:61:32:11:d5:50:15:a8:17:0f:d2:4d:
        23:03:85:8a:de:69:f6:5b:13:8a:75:8f:24:6c:29:58:ac:16:
        34:e1:e2:40:6e:24:67:54:c2:81:ea:83:4b:e1:b6:75:eb:e0:
        1b:59:d3:8e:80:9b:4e:19:e0:1f:c5:e8:7d:4c:e1:a6:34:e3:
        e3:49:5d:1e:62:15:b2:5c:1e:ed:3c:84:75:7f:35:15:d8:cd:
        f3:bf:60:08:2b:e9:37:f4:35:ab:79:3e:a7:02:79:12:78:81:
        4b:20:5d:bf:8e:92:e7:aa:ad:d0:52:07:65:80:8b:9b:81:db:
        1c:e5:29:4e:7f:57:c3:0f:a7:79:91:7f:dd:e0:b6:35:49:68:
        51:24:56:6f:01:d9:3c:ac:cf:12:a8:b2:50:48:9e:e1:dc:65:
        b6:48:7d:5f:3a:02:0c:32:fa:9d:ac:41:0c:34:80:78:5d:72:
        a9:9f:58:c1:72:1a:90:1c
```

2. Applying theory in real world - Company Acme

This company is an ordinary small business selling products online. Salesmen travel around the country and sell the company's services to manufacturers. Obviously they need the access to company's resources whilst traveling. They are equipped with laptops and an HSDPA/WLAN network cards. And most importantly they do not understand technology and I think some IT guys could call them "dummy" users. Well, they just need technology to work and they rely on IT guys to make it happen in an easy and secure way.

Security policy of Acme company reflects the business requirement for teleworking or homeworking and the criticality of Acme' assets - information.

2.1 Extract from Acme Network Security policy

• Remote access - remote access to the company network is allowed from authorised computers only.
• Users accessing Extranet applications must be properly authenticated using two-factor authentication.
• Client certificates must have a validity time set to maximum of 1 year.

• Root Certificate Authority must only issue certificates to subordinate certificate authorities.
• All external connections to the Acme's internal network must be terminated on a firewall or in the Extranet zone.
• Direct connections originating from internal network to the Internet are not allowed.

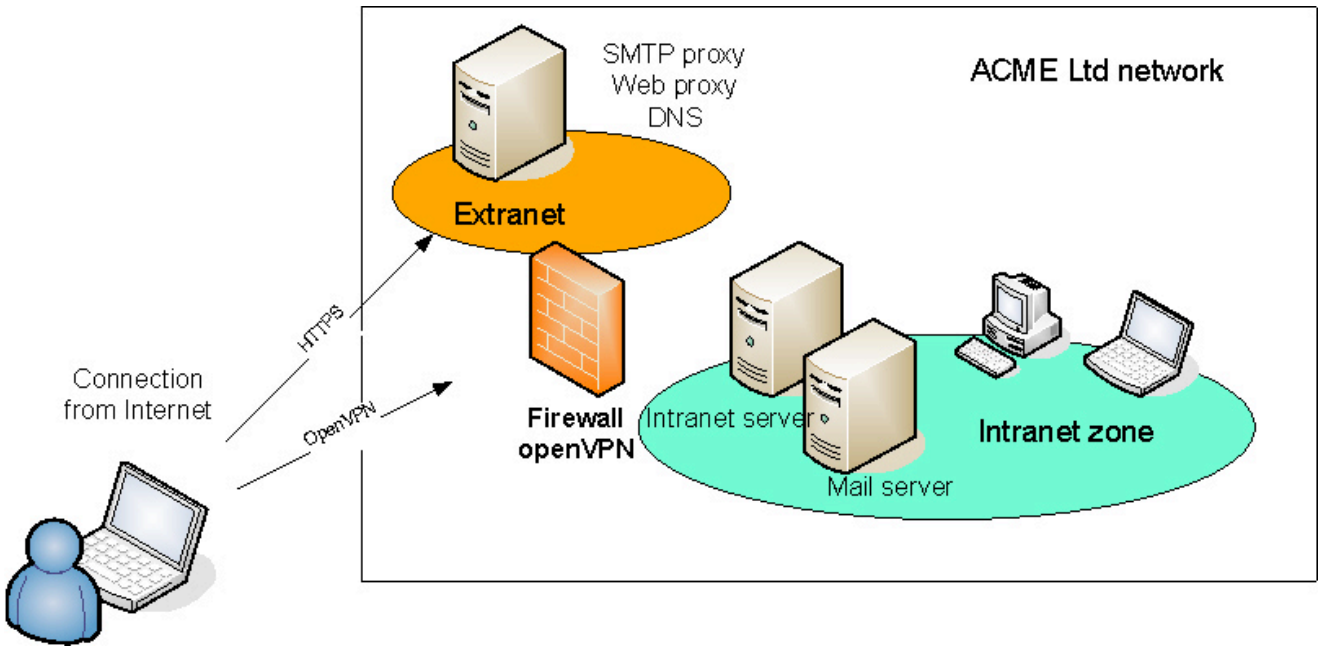
2.2 Security architecture

Translating the security policy into an architecture can be sometimes be rather difficult. That is why the security policy should always be supported by top management and actually be enforceable by processes or technical measures. In my example, the latter can be achieved by segregating internal network into 2 zones:
• Internal zone - all mail servers, Intranet servers, client computers.
• Extranet zone - servers in this zone terminate connection between the Internet and the Internal zone thus act like proxies. This enforces security policy requirements number 5 and 6.

The firewall has 3 interfaces and this the following policy applied:
1. Internet - red or 0 in Cisco PIX terminology. Incoming packets are matched against established connection. No outgoing connections from the firewall to the Internet are allowed. Firewall operates in stealth mode, silently dropping all bad packets.
2. Extranet - allowed protocols from the Internet zone: HTTPS, DNS, Email. Outgoing connections to the Internet: HTTP(s), DNS, Email.
3. Intranet - No connections to the Internet allowed, incoming connections from Extranet: SMTP, outgoing connections to Extranet: proxy (3128), SMTP (only from Internal SMTP server).

In addition, Internal DNS servers cannot resolve anything on the Internet which is actually not actually needed as they must use Extranet zone for all services anyway.

Salesmen connect with their laptops to the Internet using WLAN or HSDPA cards and use OpenVPN software to connect back. This connection is terminated on the firewall and the firewall rules give them the same privileges as if they were connected to the Intranet zone. Alternatively, they can use a web browser to connect to sales application. Both the OpenVPN and the sales application requires a certificate issued by one of an Acme's CA.



2.3 Certificate Authorities architecture

2.3.1 Tools

To transform Acme's security policy into tangible technology we will need some tools. I have deliberately selected open source and free tools however the similar effects can be achieved with commercial tools.

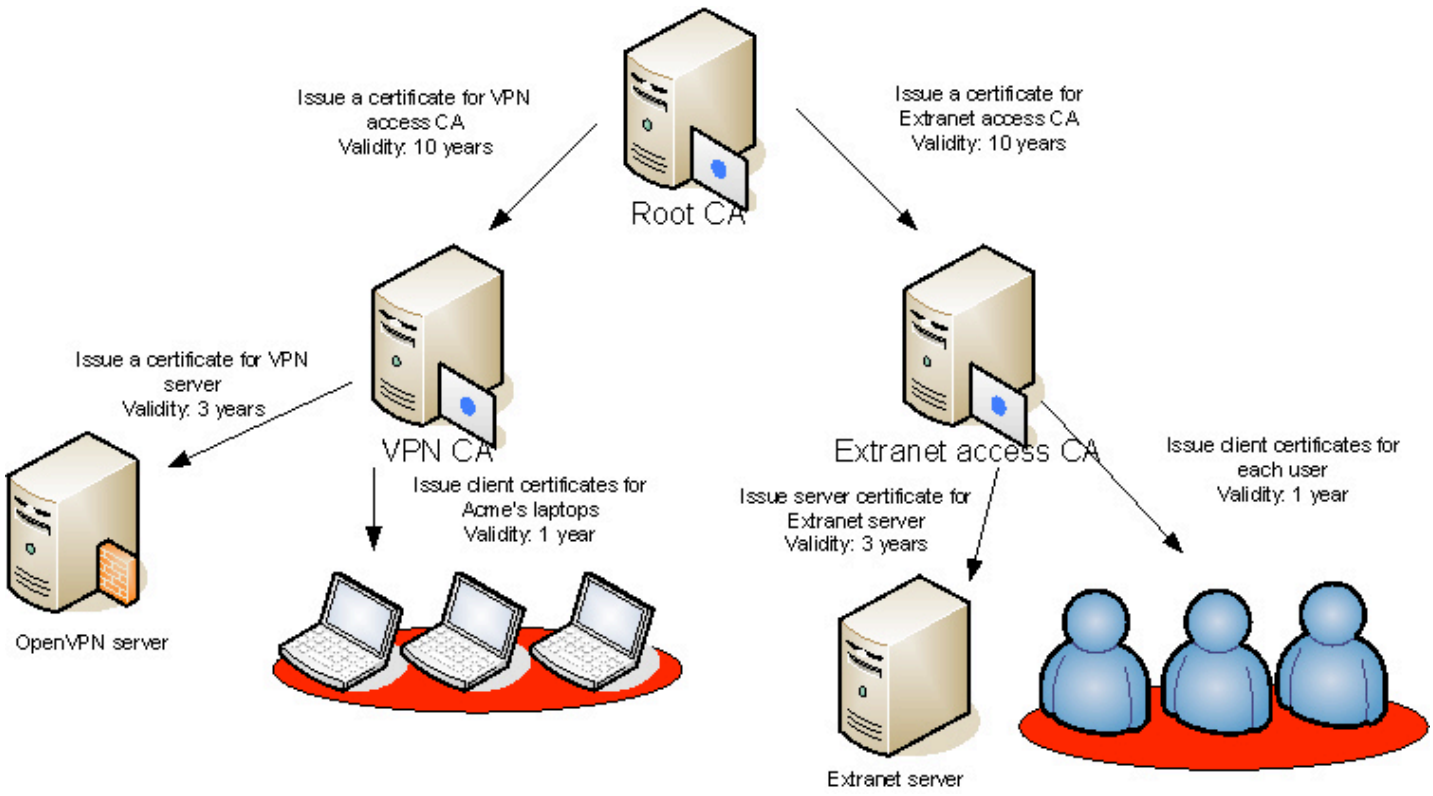
• OpenSSL - this is great software for doing a number of tasks around cryptography, encryption and, certificate management. It available for most operating system, including Linux, UNIX, Mac OS. On Windows you have to download it from the relevant section of www.openssl.org, section Related.
• TinyCA2 - This is a very good graphical interface for openssl and certificate authority management. Go to http://tinyca.sm-zone.net/. This software runs only under X11 environment
• OpenVPN to for secure VPN connections (www.openvpn.se). This is multi-platform software so there's no problem connecting between different systems.
• Apache Web server to act as an Extranet server. (www.apache.org)
• Linux server to act as a OpenVPN server - obviously this function could run on a Extranet server, if budget is an issue. In my example I assign this function to a Linux firewall.

2.3.2 Graphical structure

There are many concept of how the structure of certificate authorities could look like. I personally tend to create Sub CA per function. This has an advantage that if a function is not need in the future, the Sub CA is simply deleted, server un-installed. It has also security advantage such as end user certificates issued by one Sub CA cannot be used to authenticate to different function.

In this example the root CA has validity of 10 years and issues certificates to sub ca for 10 years as well. Bare Bear in mind that the complete structure is created the same day. But even if not, it would not be a problem as the validity of end user's certificates depends on the validity of all certificates in the chain.

So translating security policy into the architecture could look like this:



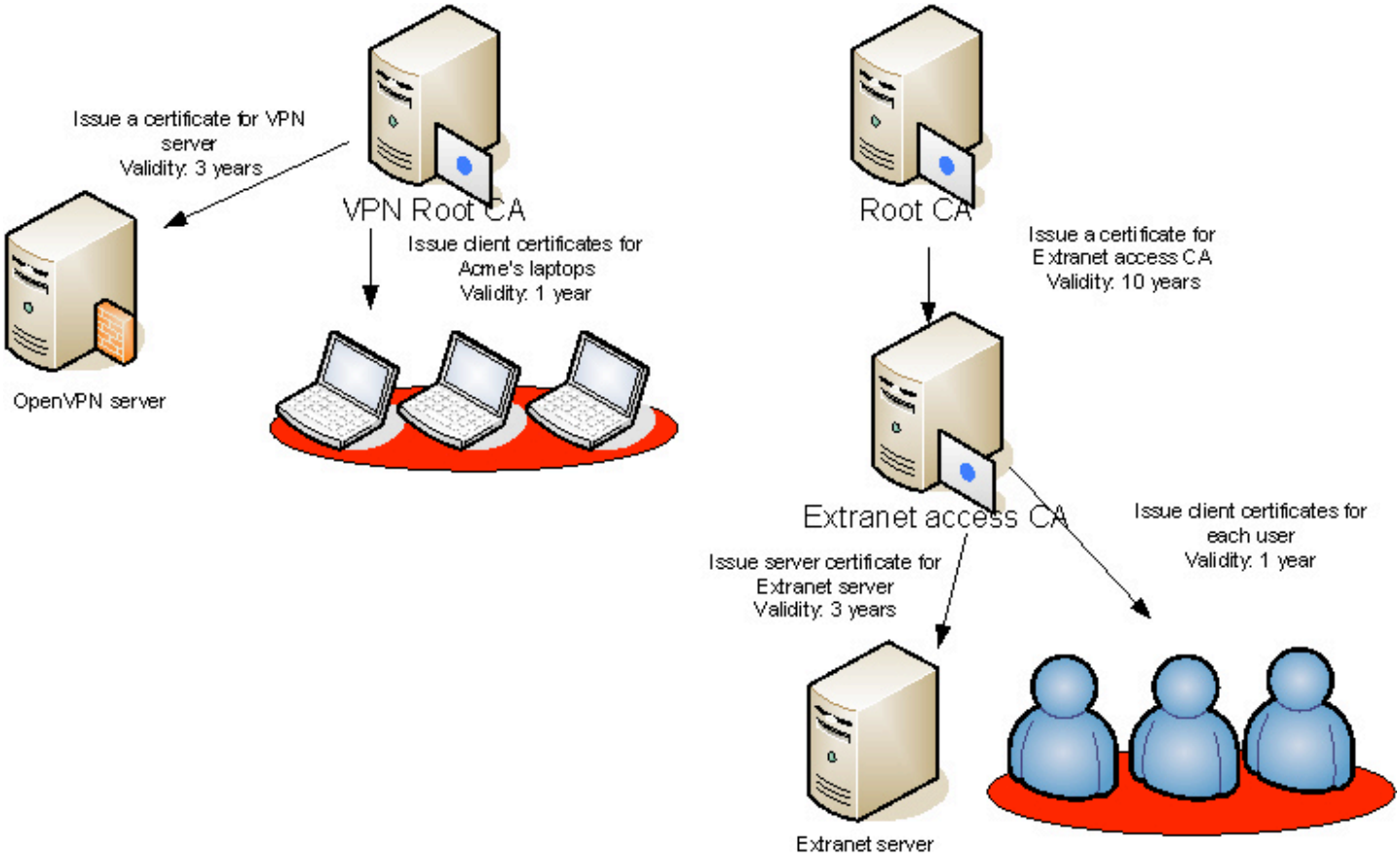
This structure has some weaknesses though. Due to the way OpenVPN verifies certificates (uses openssl verify call) user's certificate issued by Extranet CA can be used to gain access to the VPN server. This is due to the chaining of certificates leading to one root certificate and the implementation of OpenVPN.

To disable this undesirable functionality tsl-verify parameter could be used in openvpn to specify an external script, in bash or perl for example, to return 1 (false) if a certificate presented by a client is not issued by VPN CA.

However to makes things simple I have decided to create separate Root CA just for VPN server. I am fully aware that this does not satisfy security policy of Acme. Well, the risk assessment of this gap shows that the risk to Acme organisation has not increased.

Access to Extranet server does not have this weakness as Apache server, respectively mod_ssl module, can do extensive checks of client's certificate and its issuer.

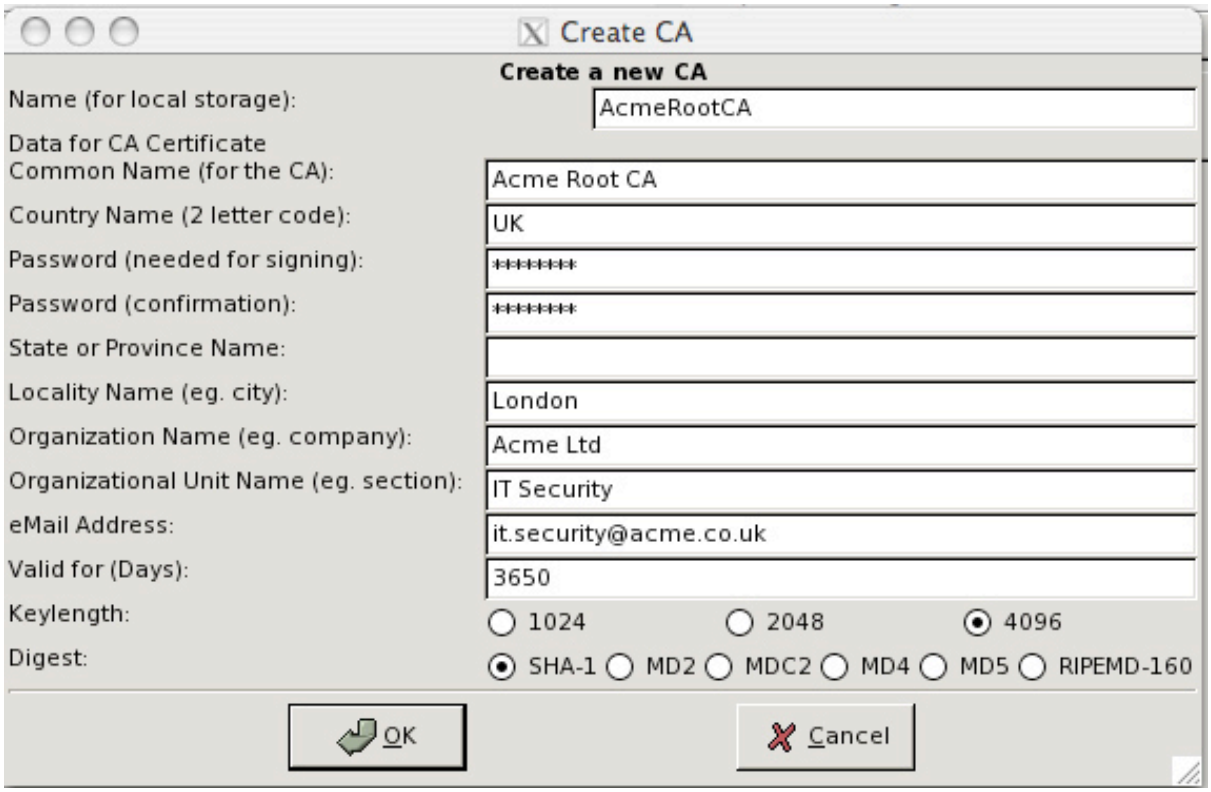
So the final structure of CA is going to be:



2.3.2 Root CA

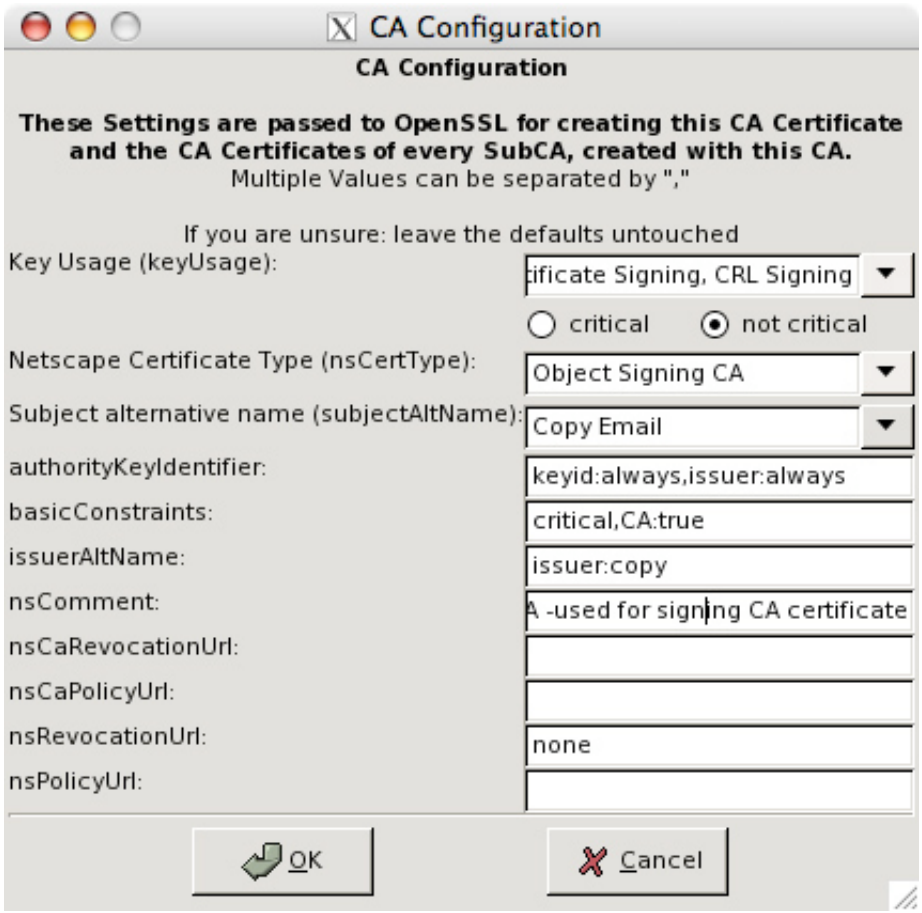
Any root CA certificate has to be self-signed. It then has to be imported into all Acme's computers. If using Active directory, this can be done easily using group policy. To create such certificate open TinyCA and client New CA button.

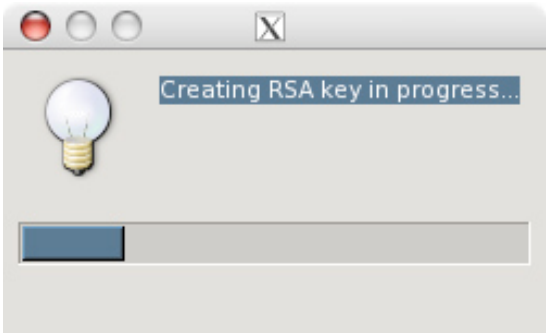
Explanation of some less obvious options:
• Common name - can be any text and is shown when viewing a certificate.
• Valid for (Days) - an important parameter as this affects how long the whole CA structure is going to be valid for. It is actually better to set this parameter to longer time and if, say in 5 years, technology progresses such so as tools which could spoof a certificate, you can always close the whole CA structure, create new root CA with improved security. It is your choice and I prefer to choose than to be pushed by shorted validity times.
• Key length - another important parameter. The usual rule, the bigger the better applies here as well. Today the minimum length deemed to be safe is 2048 bits.
• Digest - this might be a problem in few years. as much as MD5 algorithm has security weaknesses, SHA-1 has been found vulnerable as well. The current secure standard is SHA256 or higher which produces longer digest with no (currently known), at the moment, weaknesses.



In the following screenshot, the CA can add some X509 extensions to the certificate.
• Key usage: This defines what the certificate should be used for. Ultimate differentiator is whether the certificate is going to be used by a sub CA or end entity, like client or server. Functions performed by a CA are Certificate Signing and CRL Signing.
• Netscape certificate type - specific extension for Netscape browsers and server.

Next step is to generate a key, in my example RSA key.





This can take some time. On my test machine with 600 MHz Via processor this activity took good the best part of 5 minutes to finish.

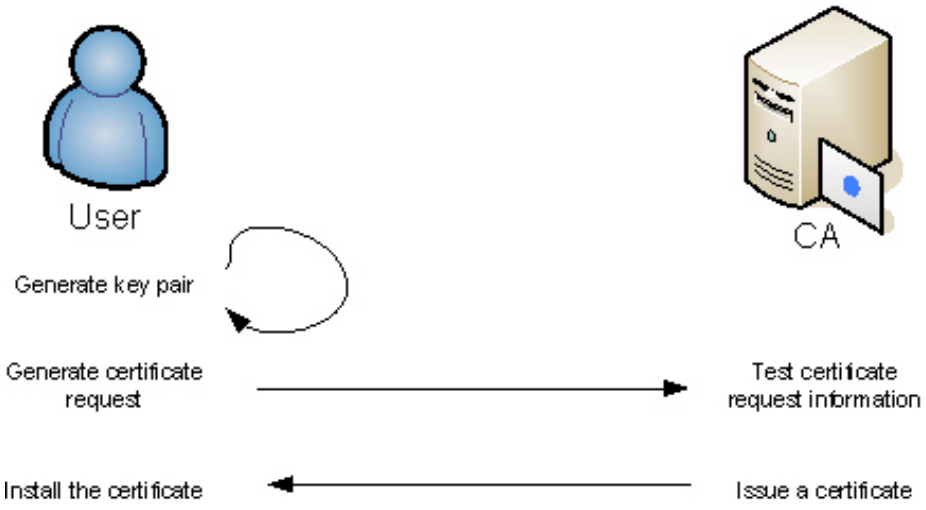
This step should be repeated for VPN Root CA and after this is done we should have two independent Certificate authorities:
• Acme Root CA
• Acme VPN CA

3. Configuration for VPN Access

After we have created VPN Root CA we will use it to issue certificates for VPN server and couple of client computers.

However in our case we will also generate keys and, certificate requests in addition to actually issuing certificates. TinyCA software makes it really easy to do these steps in comfort.

It is important to understand the process of issuing certificates. The golden rule is that the private key should be kept secret by the subject that is going to use it. This would be in our example VPN server and each laptop. This would mean installing openssl on each computer and generating key pair and certificate request as per this schematic:

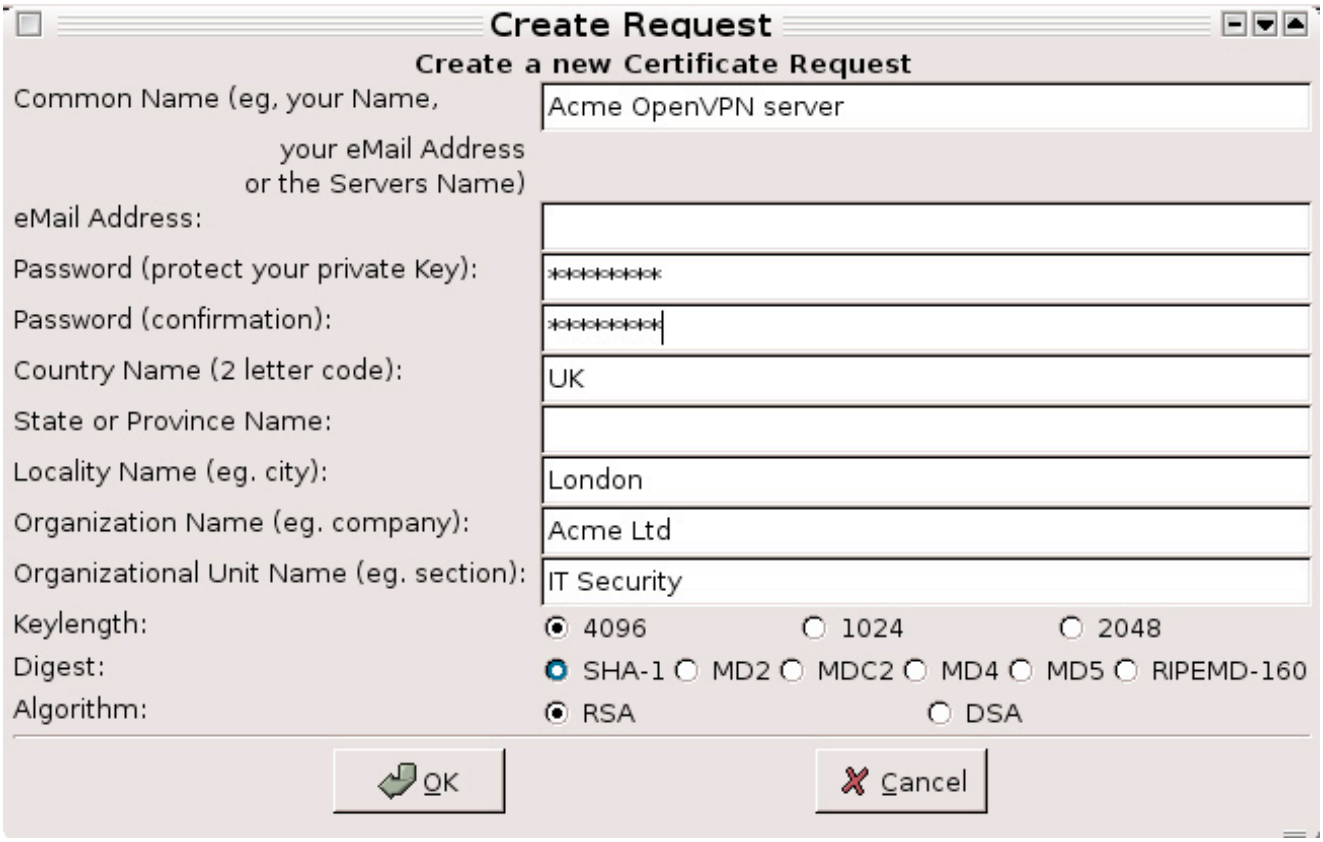


The important bit to understand is that private key NEVER leaves the client. CA actually does not need to see private key at all. On the other hand, whoever controls a CA is capable of issuing ANY kind of certificate.

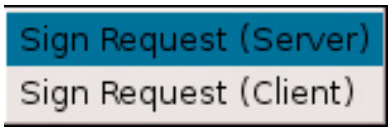
In other words, if the access to the network or information system is secured only by certificates, there is a substantial risk if the CA is compromised.

However in my example it would be impractical to use this process so the operator of the CA is going to do all the tasks and send users and server issued certificate and corresponding private keys.

TinyCA actually makes it really easy and it does not require you to generate a key first but you can go straight to certificate request step:



Then click on newly created certificate request and select Sign (server). In the new dialogue enter number of days this new certificate should be valid for.



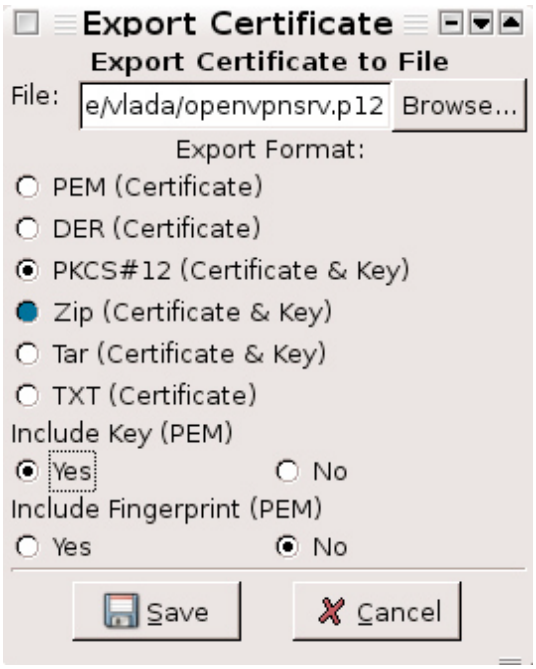
And repeat this whole process for all client certificates.

Now we have everything we need to configure OpenVPN. OpenVPN has two options of configuring certificates:
• specify ca certificate, key and server certificate
• specify PKCS12 file.

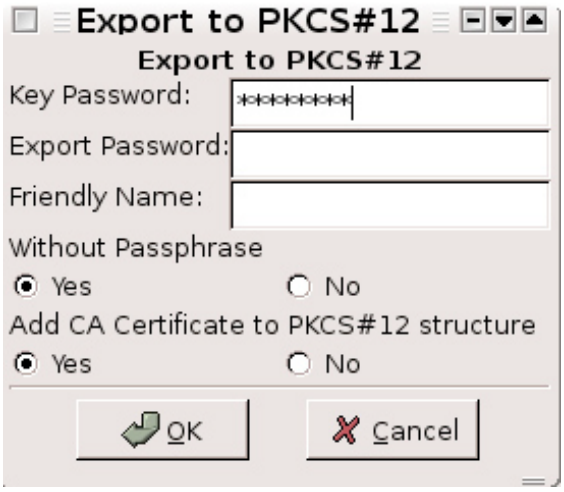
I personally find it easier to use latter as it is just one file to store on the file system.

PKCS12 format is kind of a vault that holds all the above files above in one place and can protect them using a passphrase. For OpenVPN server I do not specify any passphrase to pen PKCS12 file as it would have to be entered when OpenVPN starts. On the other hand PKCS12 for clients must have passphrase set to enforce dual factor authentication (know & have principle).

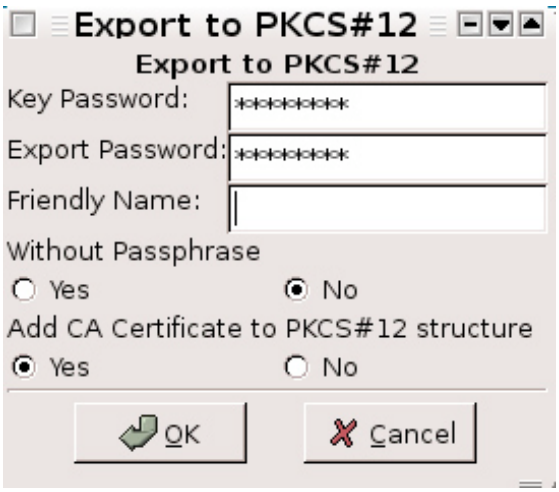
Export OpenVPN server PKCS12:



In the next step enter private key passphrase and leave Export password empty.



Export a client PKCS12 - This is the same as export for server except the Export password must be specified. Ideally we want this to be different for each laptop.



In the end we should have 2 PCKS12 files, one for VPN server and one for one laptop, the former without passphrase.

3.1 Configuring OpenVPN

Server config

In this example I have installed openvpn from a Debian package:

```
#apt-get install openvpn
```

and configured it accordingly. First we want to use some reasonable encryption.

Available ciphers and key sizes:

```
# openvpn --show-ciphers
DES-CBC 64 bit default key (fixed)
RC2-CBC 128 bit default key (variable)
DES-EDE-CBC 128 bit default key (fixed)
DES-EDE3-CBC 192 bit default key (fixed)
DESX-CBC 192 bit default key (fixed)
BF-CBC 128 bit default key (variable)
RC2-40-CBC 40 bit default key (variable)
CAST5-CBC 128 bit default key (variable)
RC2-64-CBC 64 bit default key (variable)
AES-128-CBC 128 bit default key (fixed)
AES-192-CBC 192 bit default key (fixed)
AES-256-CBC 256 bit default key (fixed)    #this is what we are going to use as
fixed cipher

/etc/openvpn#openssl dhparam -out dh1024.pem 1024

/etc/openvpn/openvpn.conf
port 1194
proto udp      #use UDP protocol - generally better as it is stateless and we leave
the control of traffic on encapsulated protocols
dev tun
pkcs12 openvpnsrv.p12            #server key and certificate - this is not pro-
tected by passphrase so the process does not need manual input
crl-verify crl.pem #CRL file generated by CA to verify validity of certificates
dh keys/dh1024.pem      #used for generating symmetric keys for encryption
server 172.20.22.0 255.255.255.0      #use server mode - many clients at the same
time. specify IP pool for clients
push "redirect-gateway"      #change default gateway rout on clients
push "dhcp-option DNS 172.20.20.4"         #use internal DNS server, essentially the
same one as for clients connected via LAN
keepalive 10 120        #keep the link open using ping commands
cipher AES-256-CBC      #use the strongest cipher available. this has to match the
client config
comp-lzo           #compress
max-clients 20
user nobody
group nobody
persist-key
persist-tun
status openvpn-status.log
log-append  /var/log/openvpn.log
verb 3

On Debian (Sarge) you might need to do:
mkdir /dev/net
mknod /dev/net/tun c 10 200

start the server:
/etc/init.d/openvpn start

At this point openvpn should start and you can easily check it by showing the proc-
ess:
# ps ax | grep openvpn
12391 ?        Ss     0:00 /usr/sbin/openvpn --writepid /var/run/openvpn.openvpn.pid
--daemon ovpn-openvpn --cd /etc/openvpn --config /etc/openvpn/openvpn.conf
```

Client config

The client config is also rather straightforward. What is needed on a client is:
• OpenVPN package - this exists for Linux, Windows and Mac OS X.
• GUI for configuring and managing OpenVPN.

Install the client and configure the .ovpn file openvpn directory. On Windows, users must be local administrators to be able to use the software.

```
ACME.opvn:
client
dev tun
proto udp
remote <your server DNS name> 1194
resolv-retry infinite
nobind
persist-key
persist-tun
pkcs12 Laptop1-cert.p12     #certificate and key file protected by a passphrase (i.e.
encrypted). Different passphrase per laptop
ns-cert-type server         #make sure the server certificate has X509 extension SSL
server
tls-remote Acme VPN Server  #make sure we only connect to our VPN server by checking
server certificate DN (distinguished name)
cipher AES-256-CBC      #use the most secure and available cipher
comp-lzo                    #compress traffic
verb 3
```

3.2 Testing all together

Finally we need to test whether a laptop can connect. Laptop users should be asked for the passphrase to decrypt the private key.

The user should be able, subject to firewall rules, to ping an internal IP address.

In the server log you should be able to see, apart from other messages, which laptop tried to connect and if the certificate presented was successfully verified.


```
Mon Mar  5 21:28:10 2007 192.168.0.1:64227 VERIFY OK: depth=1,
/C=UK/L=London/O=Acme_Ltd./OU=IT_Security/CN=Acme_V
PN_Root_CA/emailAddress=it.security@acme.co.uk
Mon Mar  5 21:28:10 2007 192.168.0.1:64227 VERIFY OK: nsCertType=CLIENT
Mon Mar  5 21:28:10 2007 192.168.0.1:64227 VERIFY OK: depth=0,
/C=UK/L=London/O=Acme_Ltd./OU=IT_Security/CN=Laptop
1
```

On the client these messages can bee seen in OpenVPN GUI window:

```
Mon 03/05/07 09:54 PM: VERIFY OK: depth=1
Mon 03/05/07 09:54 PM: VERIFY OK: nsCertType=SERVER
Mon 03/05/07 09:54 PM: VERIFY X509NAME OK:
/C=UK/L=London/O=Acme_Ltd./OU=IT_Security/CN=Acme_VPN_Server
Mon 03/05/07 09:54 PM: VERIFY OK: depth=0
Mon 03/05/07 09:54 PM: Data Channel Encrypt: Cipher 'AES-256-CBC' initialized with 256
bit key
Mon 03/05/07 09:54 PM: Data Channel Encrypt: Using 160 bit message hash 'SHA1' for
HMAC authentication
Mon 03/05/07 09:54 PM: Data Channel Decrypt: Cipher 'AES-256-CBC' initialized with 256
bit key
Mon 03/05/07 09:54 PM: Data Channel Decrypt: Using 160 bit message hash 'SHA1' for
HMAC authentication
```

As you can see mutual authentication is performed, i.e. both parties have to verify each other's certificate. Well, and as you can see it is all OK and our users are happy. But is it secure? What are the outstanding risks:
1. users still can use their home laptops by simply copying opevpn directory
2. users do not have to be authenticated against an user database
3. if a certificate is compromised or an employee leaves the company there is no way of stopping access

3.3 Mitigating risks with OpenVPN

1. using home laptops
Unfortunately there is no easy solution that would mitigate this risk using OpenVPN. Commercial tools are available that import certificates to protected area in a computer OS and this cannot be exported. Such solution is Microsoft Active Directory and using MS PKI solution. Obviously other solution is to use PKCS11 compliant hardware module on laptops, like hardware security module that could store private key and certificate.

2. authentication of users
This can be easily achieved with OpenVPN as it supports user authentication against internal or external database, most preferably using PAM modules.
add this line to the server config:

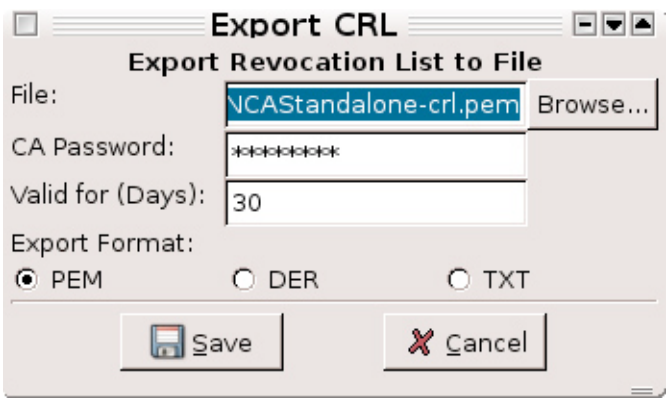
```
plugin
/usr/share/openvpn/plugin/lib/openvpn-
auth-pam.so
login
```

Look into OpenVPN documentation for instruction how to setup this plugin.

3. Compromise of a certificate
This risk can be mitigated by checking Certificate Revocation List by the OpenVPN server. Add this directive to openvpn config file:

```
crl-verify /etc/openvpn/AcmeVPNCA.crl
```

What is CRL? It is basically a text file containing Serial numbers of all certificates that have been revoked by the Certificate Authority so far. To generate this list open VPN Ca and click on Export CRL button. This step must be done every time a certificate is revoked and should be done in a timely manner.



4. Access to Extranet applications

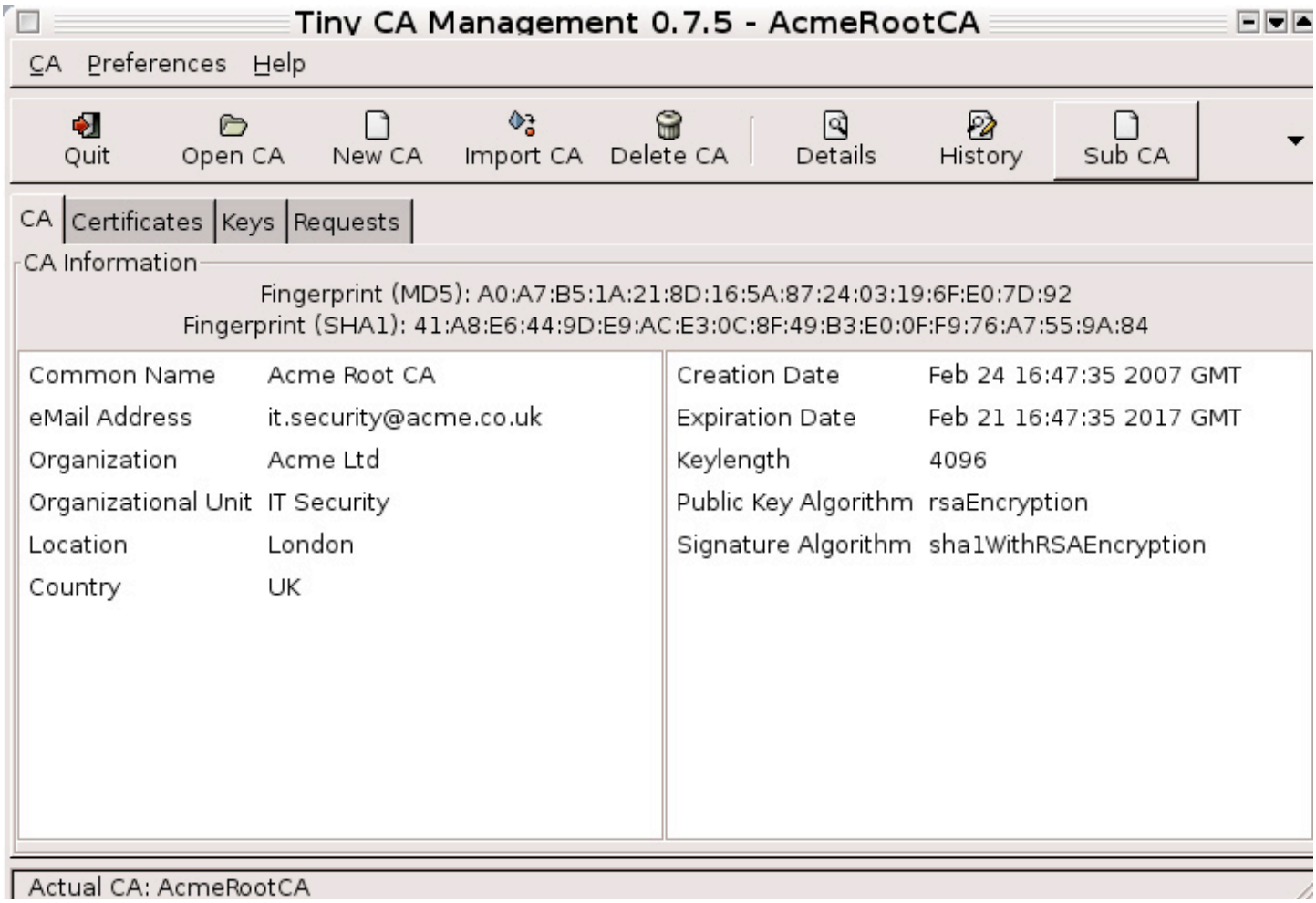
In first part of this article I have shown how to enable full IP access to internal network. Sometimes it is just enough to enable access to Web based applications. In that case we do not really need VPN access but can easily use certificates to securely access web applications.

Surprisingly, the number 1 risk that we identified and could not solve with OpenVPN is actually mitigated by using certificates for web applications. It all comes down to how web browsers store certificates and do not allow, if set, exporting of these certificates.

4.1 Extranet Sub CA

The first step is to create Sub CA that would issue certificates to users and Extranet servers. Sub CA certificate is nothing more than a certificate with CA X509 extension set to true. Therefore it is trusted to issue certificates on its own.

To create new sub CA open the Root CA and click Sub CA button:

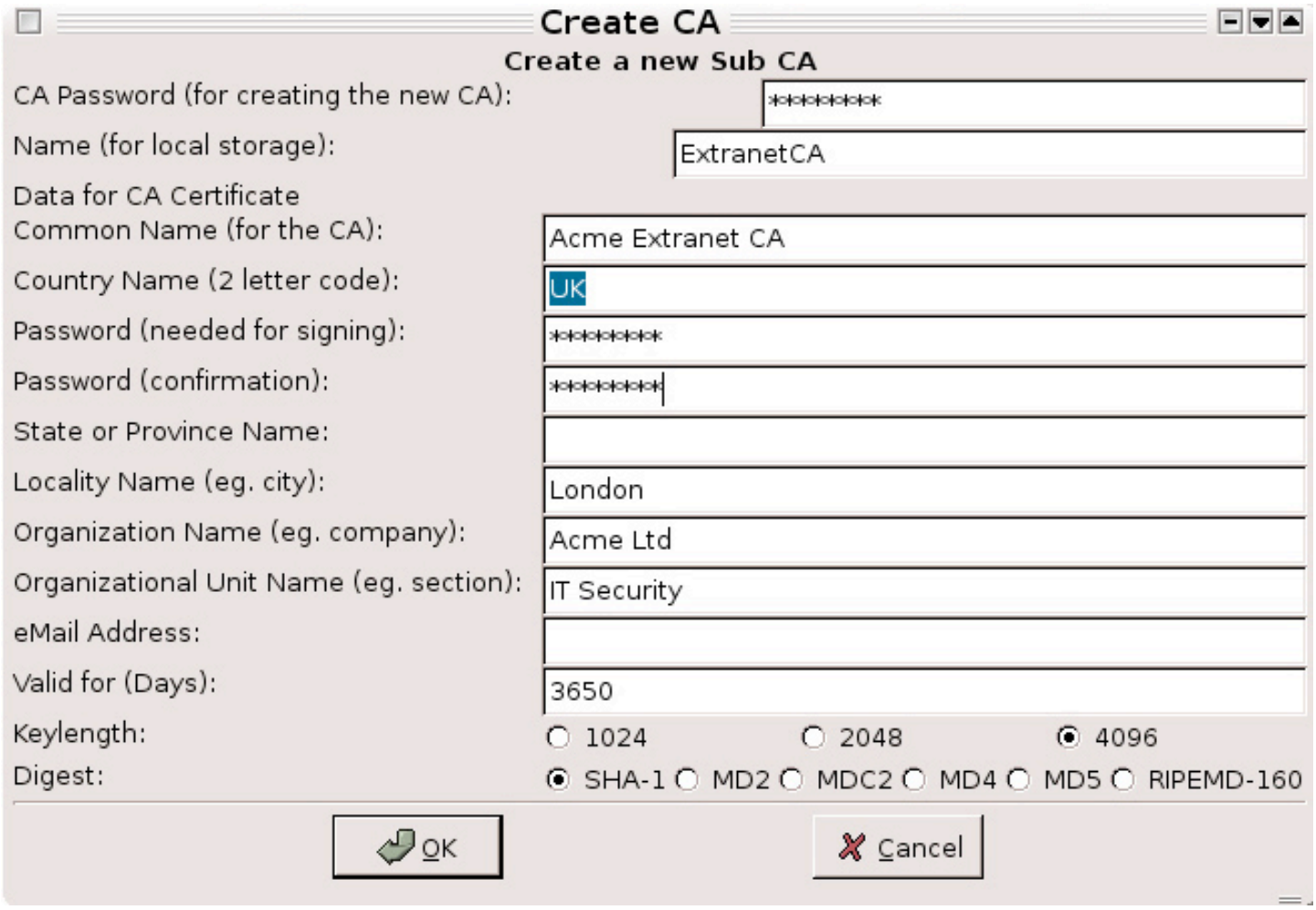


In the first dialogue on the following page, set Sub CA parameters, usually same as for the Root CA.

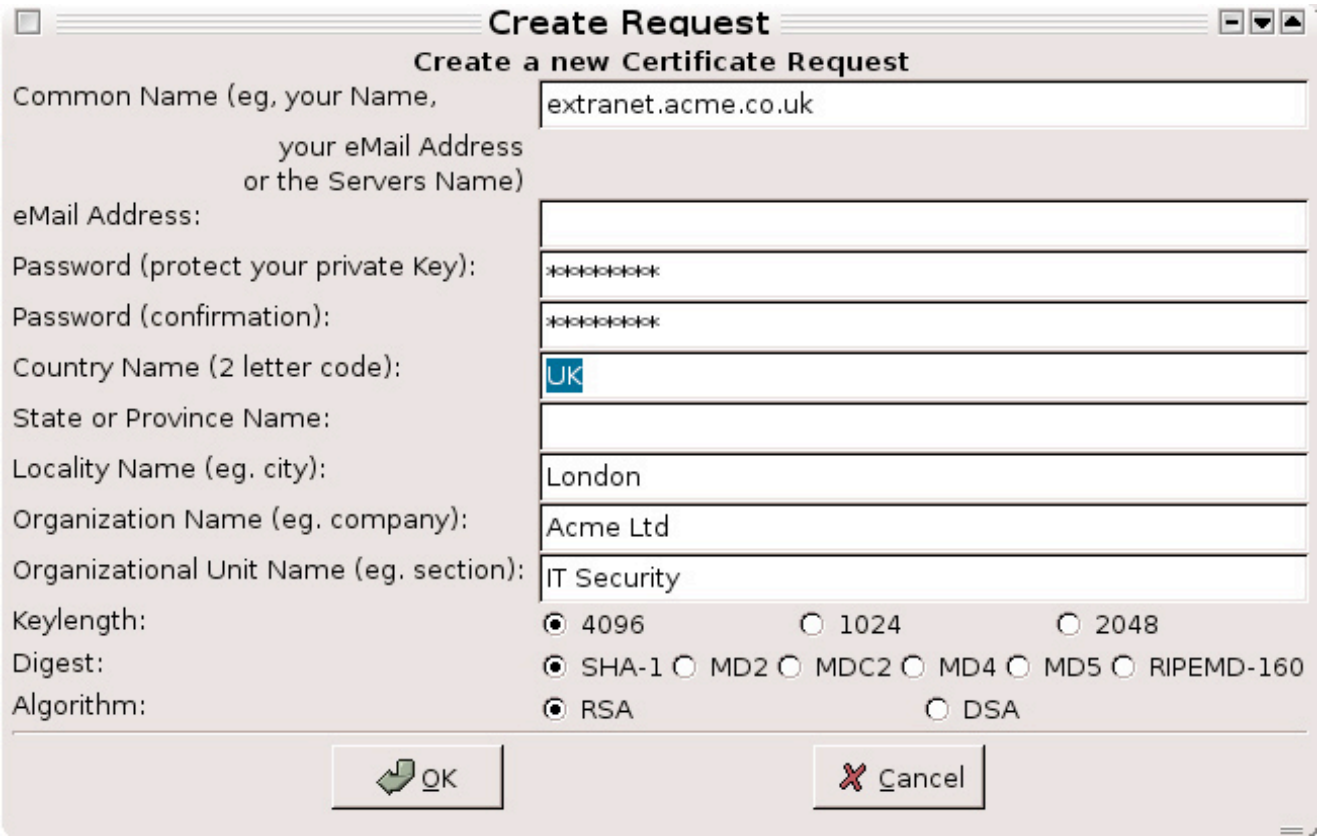
Next step is to issue a certificate for the Extranet server and certificates for users. These steps are identical as for openvpn server and laptop computers.

When generating certificates for users I advise you to set Common Name to actual login name of the user in the network.

The reason is that Apache server can fake authentication and extranet DN and use it in basic authentication, giving users password less access to applications.



As for the certificate for the Extranet server make sure that Common Name equals to the DNS name that users will use to access the site. IIf not, user would get errors when trying to accessing the site even though the certificate is valid and trusted by the web browser.



```
< ~$openssl x509 -in ExtranetCA-cacert.pem -noout -subject         > subject= /C=UK/
L=London/O=Acme Ltd/OU=IT Security/CN=Acme Extranet CA

extranet.conf
SSLEngine on
SSLVerifyClient      optional
SSLVerifyDepth       2
SSLCertificateKeyFile /etc/apache2/ssl/extranet.acme.co.uk.key.pem
SSLCertificateChainFile /etc/apache2/ssl/web-ca-chain.chain #concatenated CA certifi-
cates
SSLCertificateFile /etc/apache2/ssl/extranet.acme.co.uk.pem
SSLCARevocationFile /etc/apache2/ssl/extranet-ca-crl.pem #Certificate revocation file
of Extranet CA
SSLCACertificateFile /etc/apache2/ssl/extranet-ca.pem

CustomLog /var/log/apache2/ssl_request_log "%t %h %{SSL_CLIENT_S_DN_CN}x %{SSL_PROTO-
COL}x %{SSL_CIPHER}x \"%r\" %b"

<Location /Extranet>
Allow from all
SetEnv force-proxy-request-1.0 1
SetEnvIf User-Agent ".*MSIE.*" \
 nokeepalive ssl-unclean-shutdown \
 downgrade-1.0 force-response-1.0
SetEnv proxy-nokeepalive 1
SSLVerifyClient      optional
SSLVerifyDepth       2
SSLOptions           +OptRenegotiate +FakeBasicAuth
#test whether the client's certificte has been issued by particular CA
SSLRequire       %{SSL_CLIENT_I_DN}  eq "/C=UK/L=London/O=Acme Ltd/OU=IT Security/
CN=Acme Extranet CA"
#Require 128 and more bits
SSLRequire %{SSL_CIPHER_USEKEYSIZE} >= 128
</Location>
```

4.3 Test with openssl

It is actually a very good exercise to test functionality of web server using openssl. First, it shows detailed messages and is very good for debugging problems, second it is a command line tool as opposed to web browsers. And we love it.

Export user's key and certificate, either from TinyCA interface or using openssl pkcs12 command:

```
~$openssl pkcs12 -in john.smith\@acme.co.uk-cert.p12 -nodes -out
john.smith-keycert.pem

< ~$openssl s_client -connect extranet.acme.co.uk:443 -CAfile AcmeRootCA-cacert.der
-key john.smith-keycert.pem -cert john.smith-keycert.pem

Output should be (">" means output, "<" your input):

New, TLSv1/SSLv3, Cipher is DHE-RSA-AES256-SHA
Server public key is 4096 bit
Compression: NONE
Expansion: NONE
SSL-Session:
    Protocol  : TLSv1
    Cipher    : DHE-RSA-AES256-SHA
    Session-ID: 1F9F89F8FB9F96F039EFD654F75AC2599F194B453FD4EB3FC83763F7B26440DD
    Session-ID-ctx:
    Master-Key:
6B098E908F9B5AB9D3484869D1AA0D7CB423222BDB7901AF148D3305CB483BF7371EA3E37A4450C5D9A0DE
C9CC19965B
Key-Arg   : None
Start Time: 1173465000
```

```
    Timeout   : 300 (sec)
    Verify return code: 0 (ok)
----
< GET / HTTP/1.0
[double enter]
>HTTP output

Output in the ssl log file should be:
[09/Mar/2007:18:24:10 +0000] 192.168.0.101 jsmith TLSv1 DHE-RSA-AES256-SHA "GET /
HTTP/1.0" 487
                              [remote IP]   [CN]  [SSL v][Cipher]
```

4.3 User's test

Configuring Web browser
The final action in this exercise is, of course, to give this new shiny website to our users. Simply import Acme ROOT CA as described in the beginning of this article and then import PKCS12 file for each user. users are not allowed, by default, to export these certificates so can only access Extranet from company laptops. Obviously it is important not to give PKCS12 file to users with the encrypting passphrase.

5. Backup

As usual backup and restore must be an integral part of each IT process. In this case backup is rather easy as all information for CA function is stored in the TinyCA directory of the user running TinyCA.

So simple command:

```
~/tar cvfz backup-ca.tar.gz
```

TinyCA should create a backup of complete structure.

Restore is also straightforward:

```
~/tar xvfz backup-ca.tar.gz
```

Which will replace directory with older files.

6. Conclusion

In this article I have tried to show some useful use of client certificates. They can really help make your network secure but it is important to understand both concepts and implementation limitations. These examples were made using publicly available open source tools but they should work even when using commercial tools or purchase certificates.

7. References

www.openvpn.net
tinyca.sm-zone.net
www.openssl.org
rfc2315, rfc 2986

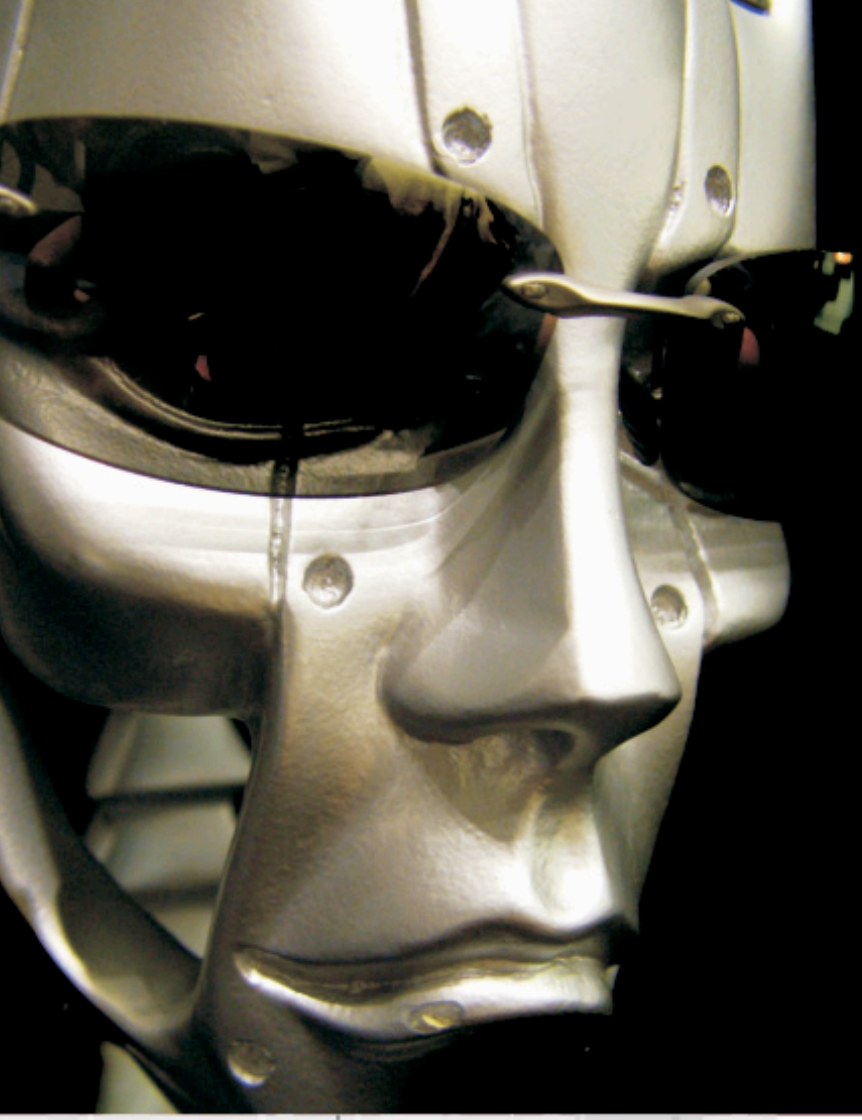
Vladimir Jirasek is an experienced security professional currently working as the Head of system security at T-Mobile UK. Recently migrated to Apple's Mac OS X operating system and is loving it. He holds CISSP, CISM and MCSE certifications. He can be reached at vladimir.jirasek@googlemail.com

Stop gambling your safety...

hakin9

Hard Core IT Security Magazine

www.en.hakin9.org



INTERNATIONAL
SECURITY
CONFERENCE

Ever got hacked?

IT UNDERGROUND

Dublin | **Warsaw** | Prague

Security or disaster?
The choice is yours ...

Meet hackers.
The good ones.

Be sure of only one thing:
To Bring Your Own Laptop!

Details:

WWW.ITUNDERGROUND.ORG