Zeitschrift: Comtec : Informations- und Telekommunikationstechnologie = information and telecommunication technology

Herausgeber: Swisscom

Band: 82 (2004)

Heft: [1]: A collection of publications of Swisscom innovations

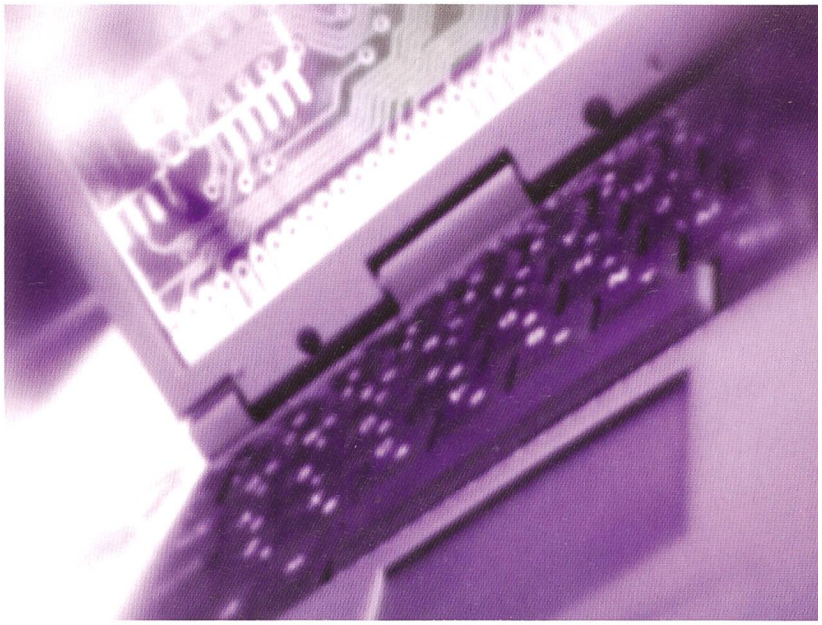
Artikel: Security trends : vendors versus hackers?

Autor: Rouiller, Steve A. / Bove, Marco / Grundschober, Stéphane

DOI: https://doi.org/10.5169/seals-876891

Security Trends – Vendors versus Hackers

STEVE A. ROUILLER, MARCO BOVE AND STÉPHANE GRUNDSCHOBER **The introduction of new technologies, the wide use of mobile devices and the availability of new powerful tools create a digital world of great flexibility and productivity, but also of scary vulnerabilities.**



The introduction of new technologies inside IT networks offers malicious hackers a potentially huge surface of attack. As a consequence, security is a topic that has become increasingly significant during the latest years and major software companies are now starting to implement security in their products. Most noticeable is Microsoft with its Service Pack 2 for Windows XP, thereby introducing a set of security enhancements never seen before in the Windows family.

Mobile devices are not spared from such growing threats, as the deployment and integration of emerging technologies in mobile devices lead to new security issues. People store confidential information on them, unaware of the existing security weaknesses intrinsic to the devices themselves. Additionally, worker mobility and Instant Messaging are also changing the rules of the game.

Traditional services are becoming the target of more sophisticated attacks. It is well known that the spam phenomenon is getting worse, but this is just the tip of the iceberg, masking the latest developments of the security warfare. If on one hand vendors propose automated risk assessments to identify and classify the network elements in order to prioritise the actions to tackle, hacking tools on the other hand are becoming smarter and more refined: By identifying the application underneath a service, they give the hacker a detailed view of vulnerabilities that may be exploited to break into a system. But not only discovery tools become more powerful: The means to disguise one's identity also become more sophisticated, hence allowing hackers to actively remain screened from forensic research and hide their own traces.

Security technology is a market driven by "point solutions" where one needs to change and embrace risk management techniques in order to focus the limited resources onto areas where they are the most effective. In this article we present the latest trends from hackers and vendors.

Mobile Devices Insecurity

The increasing usage of mobile devices, like PDAs, provides a wider surface of attack as such devices are more and more often used to store confidential information, the users being unaware of the existing risks. First of all is the risk related to the nature of the devices: They are mobile and therefore easily stolen; not only the devices themselves but also the small included memory cards are subject to the same risk. A second problem is that data is protected with a password, but most of the time no encryption is used, only a light obfuscation; often the password itself can be easily retrieved from the device. Furthermore, almost no security software is implemented and used on mobile devices; a virus can easily infect a mobile device in many ways, e.g. during the transfer of files, whilst installing applications from a remote desktop, or during the insertion of external memory cards.

Malicious code propagation via mobile devices is a real threat, though not yet fully realised. Vendors seem to begin taking security more seriously and getting more defensive. Security features are designed for Palm OS 6.0, Java, Linux, or Windows Mobile 2003 based devices, but these devices should still be fully tested and analysed before deployment. It should be realised that mobile devices are a pathway to the front door of a company network, and – in this context – employee security education is an important issue.

Mobile Workers

By 2010, nearly 27 million Europeans will become remote workers, or "e-Workers", according to the EU "Emergence" Project. Traditional remote access approaches – such as leased lines and dial-up remote access servers (RAS) – have fallen out of favour because of deployment complexities,

high phone charges, poor security implementations and ongoing maintenance costs. As a result, Virtual Private Networks (VPNs) have emerged as a secure access to corporate resources from a remote location. VPNs allow organisations to extend access to internal networks for external employees and partners over standard Internet public networks, reducing private network and dial-up phone communication costs.

Secure Sockets Layer (SSL) Virtual Private Networks (VPNs) are quickly gaining popularity against IP Security Protocol (IPSec) VPNs as serious contenders in the remote-access marketplace. Analysts predict that products based on SSL VPN technology will rival – or even replace – IPSec VPNs as remote-access solutions. Infonetics predicts a market potential of up to 1000 million $ for SSL VPN by 2005.

SSL uses encryption and authentication much like IPSec. However, SSL only encrypts the traffic between the two applications that wish to communicate to each other. This contrasts with IPSec, which operates independently of the application. However, choosing a remote access strategy is often not based on the superiority of one technology over another, but rather on deciding which solution best fits the needs of the organisation.

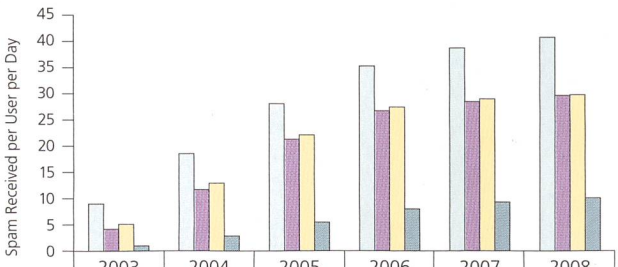
Instant Messaging (IM)

Instant messaging allows to easily see whether a friend or co-worker is connected to the Internet and, if so, to exchange messages with them. The possibilities of IM are text messaging, presence information, voice and video conversations, conference calls, and file transfer.

Instant messaging is very popular in the consumer sector. However, it is not yet as widely used in the commercial sector as email. The major drawbacks of IM are the vulnerabilities associated with this technology, i.e.

- *File transfer:* malwares bypasses the gateways in place
- *Authentication and Identity:* weak or disabled encryption mechanism
- *SPIM (Spam over IM):* The Radicati Group estimates that SPIM will account for roughly 5 percent of instant messages traversing public networks (consumer and corporate) by the end of 2004, tripling from 400 million messages in 2003 to 1200 million.

Trend forecast of the spam problem in various parts of the world according to Ferris Research.



	2003	2004	2005	2006	2007	2008
North America	10	19	29	36	39	41
EMEA	5	13	22	27	29	30
Asia Pacific	6	14	23	28	30	31
Latin America	2	4	6	9	10	11

Ferris Research, Anti-Spam for Businesses and ISPs: Market Size 2003-2008

These security issues have made organisations reluctant to exploiting IM technology. Nevertheless, there are ways to mitigate these issues such as, for example, deploying an IM proxy, integrating an anti-virus function, integrating a content checker, or deploying an effective logging system.

Spam Filters

Spam is not a new phenomenon. The first occurrence goes back to 1st May 1978, originating from Digital Equipment Corporation (DEC), and the first complaint was made one day later by the chief of Arpanet Management Branch. It must be assumed that the spam problem will get even worse in the future, as corroborated by a Ferris Research study (figure 1).

Spam filtering can take place at different locations in the email stream; on the client side, as an outsourced service, or on the server side:

- Client-side filtering refers to plug-ins made available at the end user desktop, either to filter spam into a junk mailbox or to delete it. This is typically the preference for consumers; it is installed and managed on individual PCs.
- Outsourced service vendors provide a centralised filtering solution by routing all organisational email through offsite servers. These servers scan incoming emails and once ensured they are free from viruses/spams, forward them to the email server of the company. Blackspider, for example, offers a range of services to check for viruses, spam and content filtering. The biggest advantage of an outsourced solution is that there is no hardware or software to purchase, maintain or upgrade. However, since most large organisations today consider their messaging infrastructure mission-critical and highly proprietary, the outsourced service model is often considered unappealing, as it introduces unnecessary external risks that are beyond the control of the enterprise.
- Mid to large-sized organisations choose server-side or gateway level filtering. There are many different technical approaches to block spam; message content analysis and blacklists of known spam and spammers are just two examples. One way to control spam in an enterprise is to employ a content filtering device between the firewall and the email server. Protecting the email system at the gateway will block spam prior to it ever entering the email servers. Such solutions are provided by NetIQ or Sophos employing approximately 750 spam-identification tests to assign a "spam probability" to each email message.

Evolution of Hacking Techniques

Nowadays, the knowledge of the application underlying a certain service is very crucial. Since vulnerabilities of applications and how to exploit them are well known, the identification of the applications running on a target machine is the first necessary piece of information that a hacker will collect.

Until now we have seen tools, like *nmap,* capable of identifying the operating system of a remote machine, whereas the identification of the applications was mostly based on the banner provided when connecting to the

application itself. This method is now less effective, as there are many tools available to obfuscate the banner, giving the hacker false information about the application.

Just grabbing the banner is therefore not enough and tools capable of properly identifying applications have started appearing. The first and most important one is *httprint*. It allows to identify the nature of a web server using deviations from the HTTP RFCs or behaviours not specified in the RFCs. These deviations and behaviours are characteristic to the implementation of each application and hence provide a fingerprint uniquely identifying the web server application. The information obtained in this way is very critical, since most of the time a web service is the only service visible from the external world and therefore the only one that can be used as a starting point to hack, attack or gather information of the company network.

Not only are discovery tools getting more and more powerful, but also the way a hacker can actively hide himself from forensics is getting more complex. Forensics recover, parse and analyse data on the physical disk of the compromised machine in order to reconstruct the activities of the hacker. A first technique used is to hide evidence into bad blocks of the disk. This method allows to store data in a hidden way and to retrieve it when needed. Another relatively new technique is to prevent data from reaching the file system. The hacker can transfer files and execute commands directly using the RAM of the compromised machine without leaving useful evidence of his activity on the disk.

Automated Vulnerability Management

How much patching is needed? How can an enterprise avoid under-patching and, even worse, mis-patching? A classical way to manage this issue is to perform regular audits of the network; as an alternative, attack simulations can be carried out.

QualysGuard, like Foundstone, automates the entire process of vulnerability management from discovery and assessment to on-demand reporting and remediation tracking for large distributed networks. It provides a best practice security approach to manage vulnerabilities and ensures remediation without incurring the burden or cost of deploying and maintaining complex software and hardware. Vulnerability management provides reliable protection from worms and hackers through continuous

- discovery of hosts, services, and unauthorised devices;
- assessment of online assets for the full range of vulnerabilities;
- analysis of vulnerabilities, trouble tickets, and trend reports;
- remediation based on prioritised policies.

Where can an attacker go? What could the damage be? Skybox Security answers these questions with attack simulations and analysis performed on a virtual model of the IT environment. Through this new approach to vulnerability management, enterprises can find the minimum set of an attacker action, which, if prevented, would mitigate the entire attack. Moreover, what-if scenarios can help simulate the effect of remedies before applying them to the IT infrastructure. Finally, enterprises will know what, when, and in what order they should patch.

Seven Golden Rules to reduce Spam

Find out how best practice regarding email account usage can minimise the chances of receiving spam. To help combat spam, email users should follow these recommendations:

1. Never make a purchase from an unsolicited email.
2. Delete unsolicited email message from unknown sender.
3. Never respond to any spam messages or click on any links in the message.
4. Avoid using the preview functionality of the email client software.
5. When sending email messages to a large number of recipients, use the blind copy (BCC) field to conceal their email addresses.
6. Never give your primary email address to anyone or any site you don't trust.
7. Have and use one or two secondary email addresses.

Conclusion

In 2002 there were 70 vendors with security technology revenues above 70 million $ (Gartner Group). In 2003, there were over 420 separate security technology vendors selling their products (Aberdeen Group). Therefore, selecting security technology vendors is a daunting task.

Companies should evaluate the security needs especially when switching to mobility. A cost-benefit analysis of security risks against the benefits achieved by increased productivity or profit will help companies decide on the direction. Looking at the variety of products and services that are out in the market, it is very clear that mobility is here to stay and the demand for mobility will continue to grow over the next few years, as the technology becomes robust. Last but not least, it is worth noting the UK Council gets ready for e-government with SSL VPN technology.

Finally, one should be aware that every security system is useless if users are not educated. History shows that information security breaches are often much more important than technical IT security failures, as many measures can be bypassed by a determined attacker with basic social engineering techniques. Security awareness training is therefore as important as any other security measure, if not more so. ■

Steve A. Rouiller, Ing. Dipl. Systèmes de communication EPFL, Security Team Swisscom Innovations,
steve.rouiller@swisscom.com

Marco Bove, Ing. Dipl. Ingegneria delle Telecomunicazioni Politecnico di Torino, Security Team Swisscom Innovations,
marco.bove@swisscom.com

Stéphane Grundschober, Ing. Dipl. Systèmes de communication EPFL, Security Team Swisscom Innovations,
stephane.grundschober@swisscom.com

References

- Reaction to the DEC Spam of 1978 – www.templetons.com/brad/spamreact.html
- Security expertise is built and maintained at Swisscom Innovations in the context of the programme "Software and Security Technologies", led by Dr. Bruno T. Messmer.