
We Trip The Light
FANTASTIC

Editorial office:
Elsevier Advanced Technology
PO Box 150
Kidlington, Oxford
OX5 1AS, United Kingdom
Tel:+44 (0)1865 843645
Fax: +44 (0)1865 853971
E-mail: b.mckenna@elsevier.com
Website: www.compseconline.com

Editor: Sarah Hilley

Editorial Advisors:
Peter Stephenson,US; **Silvano Ongetta**, Italy; **Paul Sanderson**, UK; **Chris Amery**, UK; **Jan Eloff**, South Africa; **Hans Gliss**, Germany; **David Herson**, UK; **P.Kraaibeek**, Germany; **Wayne Madsen**, Virginia, USA; **Belden Menkus**, Tennessee, USA; **Bill Murray**, Connecticut, USA; **Donn B. Parker**, California, USA; **Peter Sommer**, UK; **Mark Tantam**, UK; **Peter Thingsted**, Denmark; **Hank Wolfe**, New Zealand; **Charles Cresson Wood,** USA **Bill J. Caelli,** Australia

Production/Design Controller:
Colin Williams

02065
Printed by:
Mayfield Press (Oxford) LImited

HSBC to secure online business customers

HSBC bank is planning to introduce free physical security devices to protect 180,000 business customers in May.

The portable tokens are for authentication during online banking. The bank is ditching digital certificates in favour of the key-ring sized device that produces new ever-changing security codes for every transaction. It says that the token gives better flexibility because customers will be able to access their account from any computer with Internet access. Customers will use the token with their User ID and password. If they lose the token, a criminal cannot use it as it is linked into the user's profile.

HSBC is the first bank to bring in two-factor authentication in Britain. Simon Wainwright, Head of Business Banking said: "We would urge other banks in the UK to seriously consider following our lead." The bank has already rolled out the devices in the US and Hong Kong where it said they have worked at cutting fraud. It plans to issue them in the 76 countries where it operates. However, the tokens will not go to all of HSBC's 125 million customers. Home users will not benefit from the physical devices. It is only business customers, who mostly have more money in their accounts, that are getting the second layer of protection.

Wainright said: the "announcement will enable us to stay one step ahead of the fraudsters. Our experience in other parts of the world shows that this kind of two factor authentication is an extremely useful weapon in the fight against internet crime."

HSBC said in a statement that banks are increasingly concerned about Internet crime. It said that the token will give the bank another line of defence against keylogger trojans, remote hacking, phishing and screen capturing.

RaboDirect bank promises 100% no fraud – but?

An Irish bank has said that it can guarantee 100% security for its customers. It has also made allowances for the chance that it may not be able to fulfill its promise, however. The bank said that if a customer does get hit by fraud, they will not lose a cent.

Online bank, Rabodirect is relying on a physical security token to fulfill its promises. The token, called Digipass, generates transaction codes that change every 36 seconds. The Digipass can only be used with a PIN.

The bank said that two-factor authentication makes "phishing attacks virtually impossible."

Greg McAweeney, General Manager, RaboDirect, said that static passwords used by other banks for security are outdated.

He said: "Banks need to take their collective heads out of the sand and implement more secure systems for their customers. They cannot expect people to bank online if they don't do this. " He said that customers are entitled to peace of mind when they bank online.

It recommends its customers to take the following precautions:

- Customers should keep their Digipass safe and should not disclose their PIN or Customer Number to anyone
- Customers should notify RaboDirect immediately if their Digipass or PIN is lost or stolen
- Any requests for financial information should be reported immediately to the bank.

Secret Service dismantles criminal web fora

The US Secret Service has arrested seven people who are suspected of using

the Internet to steal debit cards and PIN numbers. A total of 21 people have been arrested in the last three months. Further arrests are expected in the US and UK. The authorities have been working undercover — to disrupt Web forums, where criminals exchange stolen information to steal identities. They sell compromised credit card information, fake identity documents, and viruses and Trojans that let criminals break into people's PCs.

The swoop is part of Operation Rolling Stone, which has been an undercover investigation since 2005. "Cyber crime has evolved significantly over the last two years, from dumpster diving and credit card skimming to full-fledged online bazaars full of stolen personal and financial information," said Assistant Director Brian Nagel of the U.S. Secret Service's Office of Investigations.

He said that the force has to continiously create new techical ways of investigating crimes online to protect the American financial infrastructure.

The suspects are being prosecuted by U.S. Attorneys' Offices in Nashville and Buffalo and by the District Attorney's Office in Los Angeles.

UK business careless with online data

British businesses are failing to adopt the security controls needed to protect their customers' information, according to findings from the 2006 Department of Trade and Industry's biennial 'Information Security Breaches Survey'.

Although 78% of those who accept financial transactions online now encrypt the data they receive, smaller firms are less likely to provide the required protection; and, overall, fewer than a third encrypt the data they receive.

Firms are also not considering the security implications of adopting Voice Over Internet Protocol telephony (VOIP). Despite widespread publicity, only half have evaluated the security risks, the survey found.

In brief

"BREACH RESPONSIBILITY RESTS WITH THE BOARD:" INFOSEC MANAGERS

Research has found that seventy four percent of IT security managers feel that ultimate responsibility for a Web security breach rests with the board. The survey, which was done at the E-Crime Congress by Websense, showed that only 21% believe that responsibility should rest with IT. The survey also found that only eight percent of IT security managers believe that companies take a proactive approach to security. And only 11% of them feel that external hackers pose the greatest threat to security, while 44% rate employees as the biggest danger.

POSTBANK TO USE ELECTRONIC SIGNATURES

The German bank, Postbank, plans to use electronic signatures when emailing its customers to protect them from phishing.

FTC FINES MARKETING FIRM

A US-based marketing company has been fined $900,000 for breaking the CAN-SPAM Act. Jumpstart Technologies allegedly pretended that spam emails were from the friends of recipients. Jumpstart used falsified names in the "from" field. The civil settlement does not include a guily plea and was filed in San Francisco on 22 March.

VIRUS INFECTS BOTH LINUX & WINDOWS

A virus that can infect both the Linux and Windows operating systems has been discovered. Kaspersky Labs released details of the virus that has been named LinuxBi.a and Win32.Bi.a.The virus targets Linux ELF binaries and Windows .exe files.

CSOs BUY FOR COMPLIANCE

Chief Security Officers (CSOs) are mostly concerned with buying security products to comply with regulations according to a survey by Merril Lynch & Co. Regulatory compliance comes above guarding against unauthorised intrusions and downtime. The survey also found that the majority of the 50 CSOs (78%) said that less than 10% of the IT budget went on security.

SCHOOL STUDENTS GET SECURITY TRAINING

US school students in New York State are getting computer security lessons. According to the Daily Orange, the students are being taught encryption, data protection and networking. It is being funded by the Rome US Air Force Research Laboratory and Syracuse University. The Rome labs. specialise in computer forensic research.

DDoS HITS DNS SERVERS

Two domain name system registers, Network Solutions and Joker.com were struck by distributed denial-of-service attacks in March. Joker.com was hit with "massive" attacks against its DNS servers between 20-26 March. There was a short interruption of services on the first day of the attacks. The company said on its website: "Upstream providers reported traffic peaks of about 1.3 Gigabits per second on a single line." More name servers were added to thwart the effects of the attack. Network Solutions faced attacks on 28 March that resulted in slower service for customers.

MS RELEASES PATCH FOR EXPLOITED FLAWS

Microsoft has released patches for 14 vulnerabilities - three of which fix Internet Explorer flaws that are being exploited by hackers. Ten of the total flaws are in IE. According to Symantec most of the issues are critical.

BBC STORIES USED BY CYBERGANGS TO TRICK USERS

BBC news stories have been used by cyber fraudsters to dupe people into going to dangerous websites. When people click on the link in the email, they are transported to a website that downloads a Trojan to their PC that will steal their financial details. The scam exploits a hole in Microsoft's Internet Explorer.

EUROPEAN BUSINESSES OVERWHELMED BY SECURITY DATA

European businesses are unable to deal with the vast amount of data generated from security devices such as firewalls and anti-virus software. The study, sponsored by IBM's Micromuse reports that almost a third (30%) of IT directors questioned admitted that the amount of security data generated is far too great for them to examine to identify potential security threats. Sixty-nine percent of organizations rely on a single IT manager to manually sift through records, or "logs," of security incidents to spot suspicious behavior or potential security threats. This figure rises to 79% in the public sector.

MASTERCARD "ALL-IN-ONE" INCLUDES XIRING AUTHENTICATION

MasterCard International has released a strong authentication product designed and developed by authentication specialist XIRING. This is in response to FFIEC (the Federal Financial Institutions Examination Council), guidance that US banks upgrade from single to two-factor authentication.

Safety in numbers? Early experiences in the age of chip and PIN

**Steven Furnell, Network Research Group,
School of Computing, Communications & Electronics,
University of Plymouth, Plymouth, United Kingdom**

Most of us are now very familiar with the requirement to prove our identity to an IT system. For many, it is a regular task on PCs, mobile devices and online services. However, authenticating ourselves has been a more long-standing requirement in a more general scenario – namely the use of debit and credit cards when we want to get access to our money or pay for purchases. Swiping cards and signing for purchases has been a routine act for many shoppers. Unfortunately, vulnerabilities in this approach have increasingly been exploited by criminal groups, with predictions that annual losses would rise to £800 million by 2005 if changes were not introduced to combat fraud[i].

In the UK, this change was heralded by the introduction of 'chip and PIN' technology, which mounted a two-pronged attack against fraud by upgrading the technology on the cards themselves, as well as changing the means by which the card holder authenticates themselves at point-of-sale. The 'chip' part refers to the addition of a smart chip to store the card data, making it much harder to copy than the previous approach, which used the magnetic stripe on the back of the card. The 'PIN' element refers to the use of a 4-digit Personal Identification Number in place of a traditional signature for verifying purchases – as many cardholders would already have used to withdraw money at an ATM.

The slogan of the chip and PIN campaign has been "Safety in numbers", and the clear aim has been to promote it a step forward for cardholder security. In spite of this, however, the technology has not been without its share of controversy. Indeed, a number of previous articles have already identified potential flaws with the underlying technology, as well as expressing concern over the potential for cardholders to be held more accountable for fraudulent purchases[ii]. However, rather than re-examining these issues, this article focuses more particularly upon aspects that can be observed from chip and PIN deployment to date, and the fact that some elements of implementation and operation may be less than ideal. Such a review is considered particularly timely in view of the fact that many customers now have no choice but to use the technology.

> "EMV standard addresses skimming"

Why did things need to change?

The chip and PIN approach certainly provides a basis for giving cardholders greater protection against fraud than they received with magnetic stripes and signatures. For instance, there has been clear evidence to show that the magnetic stripes were vulnerable to attacks such as 'skimming', enabling fraudsters to create counterfeit clones of a legitimate card[iii]. Chip and PIN addresses this by being one of the first systems to utilise the global EMV (Europay, Mastercard, Visa) chip standard (see www.emvco.com). Indeed, it is this aspect that distinguishes the UK approach from other countries, such as France, in which customers have been using PIN-based authentication at point-of-sale for many years.

Signatures

Meanwhile, many shoppers will have seen firsthand evidence of the flaw in using the signature to authenticate the transaction – namely the potential for it to be undermined by lack of attention or understanding on the part of the sales assistant. For example, many readers will doubtless have experienced the fiasco of signing for purchases at the checkout and then finding that the assistant did not bother to check that the signature matched the one on the back of the card. While this could often be attributed to a casual or lazy attitude, there would sometimes be a direct indication that the assistant did not appreciate the purpose of the signature in the first place. For example, I have personally witnessed several instances of assistants being presented with unsigned cards, and then proceeding to request that the customer sign it before continuing with the transaction – but without checking to see that the newly-written signature matched that on any other cards that the customer was carrying. Such behaviour suggests that while they had understood the rule that the card had to be signed in order to be valid, they had not grasped the reason why. In either of these scenarios, the signature obviously became redundant and the level of authentication was reduced to the mere possession of the card.

The UK take-over

Chip and PIN was originally introduced in the UK in the autumn of 2004, following a trial in the summer of 2003. Subsequent deployment has been significant, with the UK payments association APACS claiming that 127 million cards (of the 141 million in circulation in the UK) had been issued by the end of 2005, and over 80% of retailers had installed the associated readers[iv]. The approach was initially offered in parallel with the ability to sign for purchases in the traditional manner, allowing time for

customers to receive new cards and for retailers to install the necessary equipment. During this period, customers were not obliged to use their PIN, and those who did not know their number (or were simply unwilling to use it) were able to able to carry on signing their names instead. However, from 14 February 2006 it became mandatory for customers with chip and PIN cards to use their PIN rather than sign for purchases (albeit with some exception cases, such as vendors who had not installed the necessary equipment).

Good start

Although a number of national newspapers preceded the switchover with front-page stories predicting that chaos would ensue as a result of customers still not knowing their PINs[v], there were no large-scale headlines to confirm this in the weeks that followed (although there were reports suggesting that banks had recorded an increase in the number of customers changing their PINs, presumably to set the combinations to something more memorable[vi]). In fact, the switch was shortly followed by positive news regarding reported levels of card fraud in the UK. According to figures from APACS, losses relating to counterfeit cards and use of lost/stolen cards had fallen substantially during 2005, whereas both had previously risen from 2003 to 2004. Specifically, fraud from counterfeit cards had declined 25%, to £96.8 million, whereas the amount attributable to lost or stolen cards dropped by 22%, to £89 million[vii]. Both of these reductions were directly attributed to the increasing distribution and use of chip and PIN cards during the period (with the chip aspect preventing the counterfeiting, and the PIN safeguarding against misuse of lost or stolen cards), with a collective reduction of 24% and a saving £58.4m as a result.

Card-not-present fraud

However, the good news was accompanied by a possible warning, namely a rise in the instances of fraud occurring in card-not-present (CNP) scenarios such as online, phone and mail-order purchases, which increased by 21% and led to total losses of £183.2 million. Some have suggested that this could be a consequence of chip and PIN refocusing rather than removing fraudulent activities, whereas others have observed that CNP fraud has been on the increase for several years anyway (e.g. with the payments industry indicating that the rise has simply tracked the increasing proportion of transactions conducted in CNP scenarios[viii]). Either way, the introduction of chip and PIN has currently done nothing to combat this type of fraud. However, there have been suggestions that future developments could address this, by using chip and PIN cards in conjunction with small handheld readers and enabling cardholders to authorise their transactions remotely[vii].

> **“CNP fraud is up”**

Overall, therefore, the industry statements surrounding the rollout of chip and PIN have (perhaps unsurprisingly) been positive. Nonetheless, it is possible to observe some potential problems in the deployment and implementation practices, and the remainder of this article highlights some of these aspects (note: although a number of the points presented here reflect the UK experience, it is likely that other countries will introduce similar technologies in the future and thus the discussion as a whole may have wider relevance).

Reflecting on the rollout

Given that the previous approach was often flawed by the way it was operated, it is relevant to consider how well the implementation and use of chip and PIN has compared. Doing so quickly reveals that the experience is far from consistent from place to place.

One fundamental point is that banks and stores have collectively taken a rather questionable approach to raising card-holder awareness of the chip and PIN concept and how to use it. Rather than distributing a single, standardised information leaflet, we have witnessed a whole range of them being produced by different sources. This has led to questionable and inconsistent levels of advice, as well as (in some cases) led to statements that are simply incorrect. For example, one of the benefits stated on a leaflet produced by Tesco is that a PIN “is impossible for someone else to guess”. While many customers will realise that this is clearly an over-statement, it may lead to an exaggerated sense of security amongst others. Meanwhile, a January 2006 leaflet from the National Westminster Bank presents the following advice to help card holders select their PIN:

“Make it a set of numbers that has special significance to you, but avoid famous dates, easy number sequences and repetitions”.

On the basis of this guidance, many customers could happily conclude that their own date of birth is a good candidate. After all, it is not a ‘famous’ date and it has special significance to them. However, this would clearly be one of the obvious choices that other advice would recommend against. Meanwhile, the advice to avoid repetitions is also rather dubious – in the sense that doing dramatically reduces the number of PIN permutations.

Increased convenience?

A further comment arising from the promotion of chip and PIN is that much of it has emphasized the benefits to customers. In addition to the fundamental issue of security, another theme has been a claim of increased convenience. One example here is that the process is claimed to be quicker than traditional signatures. However, in practice this is rather debatable, and often depends upon the customer, their ability to read the display, and follow the prompts. A more significant point is that most of the literature implies the simple replacement of the customer’s

signature with a PIN. However, for most people the reality of the situation is more likely to be the replacement of the signature by multiple PINs. For example, the most recent figures from APACS indicate that an average adult in the UK holds 3.6 cards (specifically, 1.6 debit and 2.3 credit cards)[ix]. As such, if people follow the standard good practice guidelines when dealing with PINs and use a different one for each card that they hold, this means that the average person would have 4 PINs to remember – as opposed to one signature that would previously worked across all cards. In this situation, it is conceivable that some people will have difficulty remembering which PIN works with which card, and could consequently find themselves running out of attempts and locking cards at point-of-sale (on the basis that the system only allows three attempts). Of course, the reality in many cases will be that the same PIN gets used for all cards – making things easier for cardholders to remember, but introducing greater risk as a result.

Greater consistency?

Another argument that can be offered in favour of chip and PIN is that it increases consistency in the way cards are used. For example, the use of card in a shop now shares further similarities with its use at an ATM – not least of which is the fact that many point-of-sale terminals now permit the customer to make cash withdrawals on their card, as well as paying for purchases. However, a different culture surrounds the use of cards at ATMs when compared to using them in a shop. For example, when transactions are being performed at an ATM, other customers typically queue behind the person currently using the machine, and maintain an appropriate distance so as to respect the privacy of the person at the terminal. Indeed, many people will be wary of using an ATM if others are standing too close to them, and may even request that people step back if they are in close proximity. By contrast, the culture in a shop is quite different. Depending upon the orientation of the checkout and the queue, it is quite customary for people to stand directly beside you (putting them in potential line of sight of the PIN pad), as well as far more difficult to ensure that no-one is in a position to shoulder-surf (e.g. other customers may legitimately stand or pass close behind a checkout, so it is not really feasible to request a clear personal space around it). In this sense, the approach offers an increased potential for would-be muggers and pickpockets, in the sense that a thief managing to observe the entry of a PIN could subsequently follow the victim (or tip off an accomplice) and steal their card. Of course, having done so, they would then have the ability to withdraw money directly from an ATM as well.

> **“There has been questionable advice”**

Sales Assistants

The problem here can also extend to the sales assistants. Although many stores have keypads on fixed mounts, which are oriented away from the sales assistant to prevent observation, these are not the only form of keypad device. Some stores have movable terminals (either wireless or attached to cables), which get placed flat on the counter in front of the customer – encouraging them to enter their PIN in a far more observable manner. Moreover, despite the fact that it is a recommended practice in the guidelines for staff[x], many sales assistants do not appear to have adopted the practice of averting their gaze during this process. Such practices may, of course, become more standardised in future (e.g. through appropriate emphasis in staff training), but at this stage the staff culture in relation to chip and PIN seems just as variable as the earlier practice of correctly checking customer signatures.

Lack of understanding amongst sales assistants has also contributed to another problem, with individuals who do not hold chip and PIN cards finding themselves refused at the checkout. Although guidelines clearly suggest that this should not happen[xi], and that terminals should instruct assistants to accept a signature if the card does not have a chip, there are still reports of problems occurring. Indeed, during the course of writing this very piece, I was hosting a visitor from Germany whose card was declined because it lacked a chip.

Self-service check-outs

With all the effort that has been made to introduce the new technology, it is rather surprising to find that a different innovation at some checkouts has led to chip and PIN being bypassed altogether. An example has been seen with the leading UK supermarket chain, Tesco, which has introduced self service checkouts, at which customers can scan and pay for their goods without the aid of a sales assistant. These checkouts accept both cash and card-based payments, and have appeared in stores roughly in parallel with the arrival of chip and PIN. However, a notable aspect to date has been that payment by debit or credit card requires absolutely no authentication whatsoever. The customer simply needs to swipe the magnetic stripe of their card through a reader (thus indicating that the chip element of a card is not involved in authorising the transaction), with no subsequent requirement for PIN entry or signature. This results in a significant operational discrepancy, with the staffed checkouts demanding that card payments be authorised via a PIN, while the self service ones allowed it to be bypassed. Although upgrades to self service checkouts are now planned (with Card Watch indicating that stores operating unprotected self-checkouts would be liable for any fraudulent transactions that resulted)[xii], it still seems surprising that the implementation would have occurred in this way when other checkouts were already being upgraded for chip and PIN.

Biometrics

The fact that a large-scale technology upgrade was required to support the new approach is itself a notable issue, and raises the question of why the PIN was considered the appropriate option to take. After all, in parallel with this roll-out, much of the attention in other quarters had been focused around biometric authentication. However, rather than moving towards automated signature-verification (or a stronger biometric option), preference was given to a technique that could be easier to compromise (e.g. users can share their PIN, whereas they could not do the same with the signature). The card industry has explained the choice as follows:

"Finger and iris scanning as well as voice recognition and dynamic signature have all been put forward as possibilities. Such technology, however, is not sufficiently reliable or cost-effective in a point-of-sale environment to meet the requirements of the UK card industry within the next ten years." [xiii]

In spite of this, however, there are already signs that such biometric options are already being actively pursued. Specifically, customer concerns about remembering PINs has prompted a 16-week pilot of finger-scan payment technology in three UK stores[xiv]. This is based upon the 'Pay By Touch' approach, which is in widespread use in the United States and used by around two million customers per week. The approach allows customers to sign up in a store (bringing appropriate official documentation to provide proof of identity), enrolling their finger and associating it with appropriate payments methods (which may include direct debit / eCheck, debit and credit cards) for future use. Once enrolled, customers can pay for goods simply by touching their finger on a scanner at point-of-sale, and then selecting their preferred payment method from those originally registered. The early reports have indicated positive responses from customers, and could suggest that chip and PIN faces some early competition.

Conclusions

In view of figures from bodies such as APACS, it is clear that new measures were needed to guard against both counterfeiting and misuse of plastic cards. In these respects, the chip and PIN approach has certainly made contributions to the solutions. The chip technology in the new cards offers much better protection against threats such as skimming. Meanwhile, the authentication process at point-of-sale has been modified to overcome some of the recognised problems from the past. However, the experience to date has suggested that the technology is far from being a panacea. It still needs to be used and understood correctly by both customers and staff at point-of-sale, and the demands that the PIN aspect makes upon customers in comparison to their signature could lead to usability problems as more cards require them. In addition, with the biometric-based point-of-sale terminals already making an appearance, before many retailers have even switched to chip and PIN, it remains to be seen whether the approach will have the longevity of the signature method that preceded it.

About the author

Dr Steven Furnell is the head of the Network Research Group at the University of Plymouth, UK, and an Adjunct Associate Professor with Edith Cowan University, Western Australia. His current research interests include user authentication and the usability of security technologies, and details of other related papers can be obtained from www.plymouth.ac.uk/nrg.

References

i BBC. 2006. "Chip-and-pin 'cuts fraud by 13%'", BBC News Online, 6 March 2006. http://news.bbc.co.uk/1/ hi/business/4779314.stm.

ii Anderson, R., Bond, M. and Murdoch, S.J. 2005. "Chip and Spin", http://www.cl.cam.ac.uk/~mkb23/spin/spin.pdf (accessed 12 March 2006).

iii APACS. 2005. "Types of card fraud", http://www.apacs.org.uk/payments_industry/payment_fraud_1_1.html (accessed 12 March 2006).

iv APACS. 2006. "The countdown begins - four weeks left to chip and PIN deadline", Press release, 12 January 2006. http://www.apacs.org.uk/media_centre/press/06_01_12.html.

v Derbyshire, D. and Alleyne, R. 2006. "Chaos at the tills as chop and pin comes in", The Daily Telegraph, 11 February 2006, p1.

vi Hoyle, B. and Morgan, J. 2006. "Shoppers in last-minute dash for a memorably sharp PIN", The Times, 15 February 2006. http://business.timesonline.co.uk/article/0,,9558-2041077,00.html.

vii APACS. 2006. "UK card fraud losses in 2005 fall by £65m - to £439.4m from £504.8m in 2004", Press Release, 7 March 2006. http://www9.secure-ssl-server.com/cardwatch/images/uploads/2005%20Fraud%20Figures%20release%2006.03.06.doc.

viii APACS. 2005. "UK card fraud losses reach £504.8M", Press Release, 8 March 2005. http://www.apacs.org.uk/media_centre/press/05_03_08.html.

ix APACS. 2006. "Plastic cards in the UK and how we used them in 2004", http://www.apacs.org.uk/resources_publications/card_facts_and_figures.html (accessed 12 March 2006).

x Card Watch. 2005. Chip and PIN bypass staff guide - Best Practice Guidelines For Staff. http://www9.secure-ssl-server.com/cardwatch/images/uploads/publications/Chip_PIN_Guidelines_for_staff.doc (accessed 12 March 2006).

xi APACS. 2006. "Chip and PIN welcomes overseas cardholders after 14 February 2006", Press Release, 6 February 2006. http://www.apacs.org.uk/media_centre/press/06_02_06.html.

xii "Tesco to Chip & PIN-Enables its Self-Checkouts", ePaynews.com, 15 December 2005. http://www.epaynews.com/index.cgi?survey=&ref=browse&f=view&id=1134649108622215212&block=

xiii Card Watch. 2004. "Chip and PIN programme", in 'Card Fraud Overview', APACS (Administration) Ltd, April 2004. http://www.cardwatch.org.uk/html/overview.html#chip (accessed 3 February 2005).

xiv Best, J. 2006. "Oxford Co-ops test fingerprint payments", silicon.com, 8 March 2006. http://software.silicon.com/security/0,39024655,39157057,00.htm.

Electronic discovery: digital forensics and beyond

Dario Forte (CFE, CISM), Richard Power

Dario Forte Richard Power

"Litigation Lifecycle Management" is a very common legal procedure in the United States. This article provides an introduction to the topic with special reference to its complexities.

Be prepared

When a multinational company is involved in a lawsuit, it may have to defend itself on a variety of fronts. In the class action lawsuits invented in the United States, for example, the company will have to respond to a series of requests for information from the suing party that are "endorsed" by the judicial authorities. The assembly of this information is a process called "Discovery." It may either be forced in response to a suit, or undertaken voluntarily by the company as a sort of internal audit, or perhaps as a show of good faith.

The Discovery process may be handled on the basis of either hard copy or electronic documents or both. In the case of "hard-copy," the company provides originals, or authenticated copies of the requested documents. This is still a common practice (especially in Italy), although with the advent of the electronic document, we are seeing a significant shift toward the latter approach, known as 'Electronic Discovery' or e-Discovery.

e-Discovery: An approach to complexity

Three-quarters of modern-day lawsuits use e-Discovery, and the proportion is even higher in the United States. The procedure entails mapping, collecting, elaborating, and presenting documents in a legal case or an audit. It is a very complex process for two main reasons:

Different sources

1) The electronic data will come from a variety of sources including email, office documents, log files, transactions, scanned files (Optical Character Recognition - OCR), etc., and therefore be very heterogeneous.

Different file versions

2) Apart from the trustworthiness of individual files, there is also the practical problem of file redundancy. Especially in teamwork contexts, there will be various versions of any given file or document, and it may be difficult or impossible to find the most recent one.

There is a systematic approach that is currently indicated for handling this kind of data. This approach has four phases:

1) The data and documents are mapped electronically by type and location within the IT system. A properly done data inventory for the Document Processing System (DPS) will be a great time saver, and one way or another it will eventually have to be done.
2) The e-Discovery platform is chosen. The question here is whether to outsource it or do it internally. Without getting into too much detail, it has been my personal experience that outsourcing is a feasible solution for transnational companies whose data mainly resides physically or virtually outside of Italy. Otherwise an internal solution should be considered. In either case the costs are not low.
3) If the procedure is being carried out in response to a lawsuit, data are gathered, redundancies are weeded out, and detailed checks for malicious code are carried out.
4) The data are then presented for examination or review and further correlation among the various documents. A timeline is developed for subsequent presentation of the data in court.

e-Discovery: How it differs from digital forensics

Terabyte forensics

e-Discovery borders on what is termed in the literature "terabyte forensics."

With this amount of data it is clear that in the initial acquisition and preservation phase the operators are not going to be seeking a perfect image of the hard disks of a workstation. Its output will not be, for example, a set of documents embedded in a distributed file system. The idea is to provide a trusted copy of original documents requested by lawyers or chosen for presentation by the company. This is the first difference with respect to "conventional" digital forensics, where the idea is to preserve every detail of operations performed on the hard disk. Nevertheless, there is chain of custody in e-Discovery. The organization of the originals is the real added value of this type of approach. The original document is preserved and a working copy is used for analysis.

Log handling

There is, on the other hand, a similarity between the two methods in the handling of log files, complete with chain of custody forms. In my experience mail logs are also important here. Privacy laws aside, the legal consultant's task will be to find the right balance between protecting privacy and workers' rights, and performing the checks required by such laws as the Sarbanes-Oaxley Act, Italian law no. 231, and others.

e-Discovery: Who uses it?

At present, electronic discovery is de facto obligatory in the United States. This is because of a series of laws which require companies to be able to produce documents, media, and communications for oversight activities. Even if there is no lawsuit, the spirit of the law is to ensure that companies are prepared for such an eventuality. Large multinationals or banks are among the main users of this type of procedure — they are also one of the few

who can afford it. Lawyers are the ones who use the results of an e-Discovery process. They are the ones who initially order that certain documents be produced and then are the ones to examine them. It is important that the procedure is well organized to enhance the effectiveness of the court case.

e-Discovery: food for thought

While digital forensics is a discipline that, in theory, could be carried out by "computer nerds" pretending to be analysts by buying dedicated software, the same cannot be said of e-Discovery. This is true for a number of reasons:

1) The average cost of an e-Discovery project is several hundred thousand dollars. This makes it an option for just a few specialized companies operating internationally.
2) An e-Discovery project is advantageous only if backed by strong commitment from top management and the IT department. The support of the latter is critical for undertaking the preparatory phases.
3) The internal or external legal team who will read, analyze, and present the information also has to be versed in the procedure. In the United States there is law offices specialized in this type of activity. The combination of all these factors makes e-Discovery an extremely complex and costly discipline that is beyond the reach of amateurs. But for certain types of companies there is also an extremely advantageous return on the investment.

Issues and recommendations on digital forensics in general

E-Discovery presents even bigger issues and higher stakes than digital forensics. However, even what goes into digital forensics, is still beyond the experience and expertise available in most IT departments. And many of the same issues are in play whether you are preparing digital documents for e-Discovery or whether you are simply using digital forensics techniques in the course of an internal investigation (which, of course, down the road, could turn into some nasty law suit or criminal trial that requires, yes, e-Discovery.

Expert opinions

So we asked two of our colleagues on the "War and Peace in Cyberspace" virtual roundtable for their insights.

Impractical

"Much of what is taken as fact in the forensic community" Justin Peltier (www.peltierassociates.com) remarks, "is basically folklore." Additionally, many of the tried and true forensic practices considered "traditional forensics" are too time consuming, expensive, and interruptive to be practical in today's computing environment. In most environments, digital forensics comes into play during or after an attack of some kind. Therefore, incident response and digital forensics are interdependent. (Unfortunately, most organizations have poor incident handling capabilities.) Policy is the place to start in regard to forensics and incident handling, Peltier asserts. "An organization's policy needs to clearly spell out the procedures for handling suspected incidents. These procedures tell users what constitutes an incident, and what to do if they suspect a computer they are using is involved in an incident. Organizations that take security seriously want to make it clear, to both users, and sysadmins, that incident handling must follow procedures. In short, when an incident is suspected, it must immediately be reported in the recommended manner (sometimes a helpdesk ticket gets created just for tracking purposes, then an incident handler gets called)."

Procedures

According to Rik Farrow (www.spirit.com) such procedures include:

1) Doing as little as possible with the involved systems.
2) Documenting any commands entered to investigate the system.
3) Escalation procedures:
   - When to isolate a system, or even a subnet, from the internal network.
   - When to change firewall rules to block ports or IP addresses, etc.
   - How to handle the data found on a compromised system, (e.g., can data on a compromised system be immediately returned to its owner, and can it be safely returned? It may contain viruses if it includes images, executables, and other application formats such as MS Office files. And what about proprietary or secret content? Can and should such content be turned over to outside investigators?

Business continuity

Peltier recommends that rudimentary forensic understanding about the conservation of data and so on should be factored somehow into the organization's Business Continuity Plan (BCP) or Disaster Recovery Plan (DRP). But, of course, it is not that simple.

"Usually the cost of maintaining and training a staff with CIRT skill sets on staff is far too high for most companies. Typically, the IR procedures only cover the non-destruction of data until a third party can perform collection and analysis of the system. In order to possess the skills necessary to be a team lead or primary CIRT investigator, someone would need a wide variety of skills."

Here are the areas that Peltier identifies as needed:

1. Policies and procedures for dealing with an incident
2. Methods of attack
3. Investigations (interrogation and interview)
4. Computer forensics
5. Social engineering
6. Business Continuity Planning/ Disaster Recovery Planning

"The skills are wide in range, and require a depth of understanding," Peltier adds, "and we haven't even listed the core skills like project management and coordination."

Data retention and destruction policy, in particular as it relates to email, is an issue of vital concern.

Email retention

As Rik Farrow observes, "email retention policies have more often been used in lawsuits against companies than they have been to support that company in a prosecution."

He stresses that security relevant data, such as server logs, firewall logs, network security monitoring logs, should be kept for at least a year if possible.

"Discovering that an incident occurred months ago is quite possible: it might take that long to discover about a leak of proprietary information, and having these traces available makes it possible to look at what was happening at the network level — if the logs still exist."

According to Peltier, most forensic organizations recommend that audit logs be stored for a period of four years. "Most organizations," Peltier adds, "will use an optical jukebox storage solution just to manage the logs."

E-discovery checklist

What recommendations should go into your organization's digital forensics/e-discovery checklist? Here are some suggestions from Farrow:

Documentation
Document everything. A good incident response handler takes careful notes in a paper notebook, includes numbered pages, initials each page and includes a date.

Don't touch
Do as little as possible to the compromised system. In most cases, something will have to be done to establish that a system is compromised. Best practice is to use commands run from a forensics CD, and remember to document what is done.

Remove power
Shutdown the system by removing power. Sometimes systems will be configured to delete evidence (or all files) during a proper shutdown.

Image hard drives
Image hard drives. You want an exact duplicate of the hard drive, as this preserves evidence of deleted files, files hidden in slack space, spared sectors, etc. Work only from duplicates.

Digital signatures
Make digital signatures of the originals, print them out, and store copies of the digital signatures with the originals in a secure place.

Guard originals
Keep evidence (original hard drives, copies of logs) under lock and key. Even better, get a lockbox that requires two keys, like a safety deposit box, so that all evidence is stored under dual custody.

O. J. Simpson

But Peltier cautions that putting together a digital forensics checklist could be difficult, because there are so many types of evidence: full files for proof of an attack, illegal Images (KP), code fragments from malicious code, etc. Furthermore, such evidence can be easily overlooked. And with the new attacker discipline of anti-forensics, it may be also very difficult to find. "This is due in large part to the fact that even though computer forensics is in its infancy the forensics practices and techniques are dated in comparison to the attack and data hiding techniques used by Internet attackers." And then, of course, there are the legal issues.

The O.J. Simpson murder trial offered a glimpse into our future. One of Simpson's lawyers was an expert at arguing DNA evidence in court. Exploiting the sloppiness of the investigation, he went to work cultivating the "shadow of a doubt." The jury's mind was very soon boggled beyond all hope. Simpson was acquitted.

Imagine what a lawyer could do to digital forensic evidence if the client had deep pockets. Farrow concurs that digital records are much less durable than DNA evidence.

"The sysadmin that runs a backup of a filesystem on a compromised system changes the access times of every file on that system, destroying some evidence. With few exceptions, like the flawed event logging mechanism found in Windows Servers, logfiles are ordinary files that can be edited by an intruder. After the fact, any logfile can be tampered with."

The implications are serious.

An investigator could add incriminating evidence, or remove evidence from a system that the investigator feels might 'muddy the case'. For example, during pre-trial investigation, some forensic experts working for the defense could discover electronic records that proved that their client had not been guilty of the crime he was charged with — but was guilty of other, similar crimes. In this case, all they would have are copies of the evidence. Someone with access to the original evidence (perhaps the hard drive itself) could modify that evidence and leave little or no trace that they had done so, making the evidence for prosecution airtight. This is why hard drives MUST BE imaged, and only copies used. The original evidence must be kept sealed after imaging and generation of digital signatures. The digital signatures can be used to prove that copies do accurately represent the originals.

Peltier elaborates: "The most interesting issue that I see know regarding forensics would the possible fallout of the Florida court case that overturned drunk driving convictions because the Breathalyzer software was closed source and could not be verified by the scientific community. The potential fallout of this could mean that large forensic software manufacturers like Guardent and Access Data would either have to become open source or be subject to constant question in court. I've always favored the open source forensic software, because the software is more mature and the code can always be verified…Since there are no true standards for how to perform forensics, folklore is often taken as best practice. There is no universal certification process to become a forensic examiner and in most cases the introduction of evidence and expert testimony is completely at the judge's discretion. In addition trying to explain computer related evidence to IT people is hard enough. I can't image what it would be like to try to explain the evidence to 12 peers who are not information security or even IT people."

Conclusion

In conclusion, few organizations can afford to develop internal expertise on either digital forensics or e-Discovery. But, unfortunately, any of these organizations could at some time or another, and in one way or another, be required to utilize digital forensics in internal investigations or comply with e-Discovery in court cases, or both. So it is critical that all organizations have at least robust incident response plans in place, and an established relationship with third-party experts in these vital areas.

Secure VoIP – an achievable goal


Ray Stanton

Ray Stanton, BT business continuity, security and governance practice

There's no doubt that VoIP is the future of telephony. What started as a rather cumbersome way for budget-conscious enthusiasts to talk via their computers has now developed into a technology of much greater significance.

Introduction

VoIP creates new ways of delivering fully-featured phone services that promise big cost savings and open the way for a whole new range of multimedia communication services. After years of 'will it, won't it' speculation and unfulfilled predictions of universal adoption, Gartner is now positioning VoIP firmly on its way to the 'plateau of productivity' on its widely-respected technology hype cycle. But questions about its security and reliability persist. Given that VoIP is delivered using the same underlying technologies as the Internet and corporate intranets, such questions are inevitable. Will it deliver the seamless voice communications that we have all become accustomed to? What are its weaknesses and vulnerabilities? And how do you protect against them?

The security challenge

The fusion of computing and communications technologies has made VoIP possible. But converged networks are also the source of its potential weaknesses. VoIP is a combined target for the different kinds of attack that are faced by both computers and phone systems.

Attacks have been limited to date, but as VoIP becomes more pervasive, so the number of attacks can be expected to grow. What organizations using VoIP need to do is put in place a comprehensive security programme that ensures that any attempts on its integrity do not cause the damage that the attackers intended.

Much depends on how companies use VoIP. For example, IP phone services that operate over the public Internet are more at risk than other applications of the technology. But they tend to be used by individuals and small businesses, so the results of failure are more likely to be irritating rather than catastrophic. Private IP phone networks that operate within a single organization are inherently better protected, but because the value of the data involved is so much larger, the costs and consequences of service failures are often orders of magnitude greater.

Dangers of VOIP

Telephone fraud
Denial-of-service attacks
Theft of service
Nuisance calls
Eavesdropping
Misrepresentation

Calling over the public Internet

A growing number of services are available to allow people to make phone calls over the Internet, typically taking advantage of unused capacity on the broadband link to a home or office.

Because these services all share network capacity with other traffic, calls can be subject to interference and interruption. This can be as much a result of legitimate peaks in demand as from more malicious threats like a denial-of-service attack launched on the relevant service operator's infrastructure.

There is also the issue of enabling the data packets generated by phone calls to pass securely through PC, corporate and other firewalls. The activity generated by some VoIP applications shares characteristics with hacking attempts and other attacks which, in a well-protected system, makes it difficult for IT departments to allow calls to pass through a firewall without weakening defences.

For these reasons, many organizations prohibit the use of the VoIP services that operate over the public Internet.

Making calls in private

When it comes to the use of VoIP to carry calls within organizations, the situation is somewhat different. Calls are typically received from the public telephone network using standard lines or T1/E1 connections. They are converted into VoIP by a gateway and relayed to specific IP phones using the company's private data network.

Many companies operate logically separate networks, keeping voice and data traffic apart, and this separation can be maintained when sites are connected using an operator's VPN. MPLS networks, for example, can be used to connect converged voice and data systems at different locations, enabling calls between employees to be kept 'on network'.

The isolation of the corporate VoIP network from the public Internet means that the risk of many forms of attack is minimised. However, even where logical network separation is used, some connections between the organization's VoIP infrastructure and its data network will remain.

This means there is the potential for an external attacker to set up a call from an internal IP phone out over a standard E1/T1 interface, which may not be noticed, unless some form of monitoring is used. This form of breach could be used to listen to a conversation in a room, for example, but would require a previous vulnerability, such as a Trojan, to be exploited to get internal access to devices from the outside.

The highest levels of security, including those required by CESG, necessitate a firewall being placed between the IP network and the device connecting to the E1/T1 interface. But at a commercial level the line could be just logged and monitored.

However, since such connections can be exploited by attackers who successfully breach the organization's outer defences, they should be minimized. Softphones – computers equipped with an application to allow them to make IP phone calls – create bridges between voice and data networks. For this reason, the US National Institute of Standards and Technology is among those that recommend they are not used whenever high standards of security and availability are required.

> "Softphones are also vulnerable"

Installation issues

So what's the solution? How do organizations reap the numerous benefits of VoIP without compromising their sensitive data and systems and the availability of their phone system. Whichever type of VoIP service is adopted, the first and most essential step is to ensure that it is correctly configured by qualified personnel with appropriate training and accreditation.

Typical switched-circuit voice solutions based on private exchanges have become a very mature technology that is normally supplied as a 'black box' connected via well-established interface standards and network services. VoIP may be used to replace such installations, but it takes more than traditional telecoms skills to operate them properly.

On the other hand, there are also notable differences for those more familiar with supporting data networks. Factors such as delay are critically important to VoIP services, so those employed to manage and support such networks will need skills above and beyond those normally required for work on data transmission.

As a result, what VoIP needs is a combination of IT expertise, drawn from experience of maintaining secure data networks, along with more traditional PSTN-oriented skills that have traditionally been more focused on delivering high levels of availability.

Basic precautions

Nonetheless, the components of a converged voice and data system make extensive use of software and hardware that form traditional computer installations and, therefore, require the same basic forms of protection.

For example, viruses could exploit weaknesses in the underlying operating systems and in application programmes. But when it comes to hardware, attacks are not limited to routers, switches and other standard network equipment: softphones are also vulnerable.

While such problems will be more frequent in some VoIP systems than others, it is essential that any new patches are applied as quickly as possible to limit the impact of any attacks. Anti-virus solutions will also be required, and these must be designed to ensure that excessive delay in telephony packets transiting the network is not introduced.

It is also important to monitor security sources for details of new forms of attack and register to receive security alerts directly from vendors. Customers that hold support contracts, for example, will usually be informed of any action they must take to protect their installations.

To ensure that VoIP is secure it is important to understand the nature of the specific threats that VoIP systems face and the possible results. With this knowledge, measures to protect the system can be far more targeted and thus more effective. The six threats listed below are likely to be the most common.

Denial-of-service attacks

Denial-of-service (DoS) attacks aim to reduce the quality of the phone system, even to the extent of preventing users from making and receiving calls. Like DoS attacks on data networks, email systems or corporate websites, the perpetrators aim to flood voice services with unnecessary traffic.

In cases where calls are routed through the public Internet, or across another network that shares capacity on a 'first come, first served' basis, interference can result even from legitimate activities, such as downloading large files. The packets of data that carry the call get delayed, causing breaks in the conversation. In severe cases, the line will be cut.

Those wishing to deny users the ability to use VoIP phone services can exploit the weaknesses by flooding the network with spurious data, reducing its ability to carry calls. Alternatively, an attacker can flood a target call manager, phone or IP telephony infrastructure with false service requests or malformed data packets. These will either overload the system and software completely or impede its ability to handle legitimate calls.

> "AV should not delay packets"

Just as with DoS attacks on Web servers and data systems, attackers can enlist so-called botnets to create a distributed DoS assault. Anti-virus solutions that also protect against malware; appropriately configured firewalls; regular security patches; and intrusion detection and prevention are therefore essential to ensure that weaknesses are not exploited to the full.

In addition, where private networks are used, it is possible to divide the available capacity to create two or more logical networks, each with its own capacity limits. This allows phone calls to be kept separate from data transfers and, as a result, from management traffic, minimising the possibility of interference.

Similarly, by assigning different service qualities, voice can be given higher priority to network resources, reducing the impact of delay and bandwidth hungry data transmissions. Quality can be further assured by operating call acceptance controls to monitor capacity and make sure new calls can only be made when bandwidth is available. After that, callers hear the busy tone.

Fortunately, the incidence of attacks on call managers and other VoIP infrastructure has so far been low. However, the problem is likely to grow as usage increases. As it does, it will become increasingly essential for operators to be equipped to take prompt and effective action to mitigate the effects of attacks until they subside or can be brought under control.

Theft of service

Next on the list of possible crimes is theft of service, the aim of which is to make phone calls at someone else's expense and without their permission. This requires the ability to access or connect to an organization's VoIP network, or the theft of log-on details for public services.

Of course there are a number of ways that theft of service attacks can be carried out on PSTN lines – unauthorised access to physical premises, and modifying call routing software to enable dial-through fraud are just two examples.

But with VoIP, opportunities for people to use phone services without permission can also result from inadequate network security, the connection of devices to a network without permission, and infection of IP phones and softphones by software that modifies their behaviour. And because the number of the phone is often defined when the user logs in, it is also possible to use stolen user identification details to charge calls to someone else's account.

Basic security measures are once again essential:

- Limiting entry to premises.
- Closely guarding log-on details.
- Installing anti-virus solutions to stop malware infecting IP phones.

Strong authentication solutions coupled with device identification measures will help prevent unauthorized access. Challenge-response based client authentication – a cryptographic process that proves the identity of a user logging onto the network – can also ensure that only authorized personnel are able to use the phone system.

Telephone fraud

Telephone fraudsters make money by manipulating phone usage and/or billing systems.

As with conventional phone systems, opportunities exist for criminals to make money from users calling premium rate services. The principal difference is that, because VoIP is a computer technology, such services can be dialled automatically.

For example, an application received in a spam email, or inadvertently downloaded from the Web, can install itself on a softphone – and then direct the phone to call premium rate numbers without the user being aware.

Alternatively, devices could be attached to an organization's network without permissions that then make frequent or prolonged calls to premium rate numbers. Such devices could exploit weaknesses in wireless security policy or could be planted by disgruntled employees or even cleaning and maintenance staff, who have access to the office out of hours.

As with theft of service, VoIP call servers can be configured to reduce the opportunity for dial-through fraud. For example, phones on private networks can be given access only to selected number ranges relevant to the jobs of the users involved. Calls to premium rate and international numbers would normally be barred by default, and the call server can be set to ensure that phones that auto-register and are automatically given an IP number are only given access to numbers within the organization concerned and the emergency services. Generally, an option also exists to disable the auto-register facility completely.

Software can also be used to report unusual calling patterns from 'legitimate' phones, drawing attention to any that might be running rogue dialler software.

To prevent fraudsters hacking into billing systems and adjusting records in their favour, conventional IT security measures can be applied.

Nuisance calls

SPIT – or Spam over IP Telephony – can be thought of as a new and potentially more disruptive way for people to make nuisance calls.

Because VoIP is a data service, the rate at which voice messages can be sent isn't limited by the number of lines the caller has available, or the rate at which numbers can be dialled.

Instead, an audio file could be uploaded to a computer and sent to a list of target IP addresses in much the same way that email spam is sent to people's inboxes. Depending on the performance of the computer and the capacity of its network connection, thousands of calls could be made every few minutes.

These might simply promote products and services that recipients don't want or they could have a more malicious intent.

While not yet a major problem, SPIT has the potential to become an increasing irritation as IP telephony becomes more commonplace. Solutions similar to those used to remove spam messages from email inboxes will be required to prevent SPIT reaching its target.

Eavesdropping

The aim of eavesdropping is to listen in on calls or otherwise acquire confidential information.

One of the techniques that eavesdroppers can use is Voice over Misconfigured Internet Telephony, or VOMIT as the acronym-loving world of telephony delights in calling it. IP telephony packets are captured by a monitoring device connected to the network and are subsequently reassembled into WAV, MP3 or alternative audio files.

The technique can be used for legitimate purposes – to assist in debugging, for example – but also enables eavesdropping. The reassembled files can be collected later, emailed or otherwise sent on to the eavesdropper.

This problem occurs only where voice and data calls share the same logical network – for example in the public Internet – and where physical access is available to eavesdroppers.

It can be addressed using a combination of logical separation of voice and data networks, and physical security measures. Management and signalling traffic, as well as the voice and data

being transferred, can also be encrypted by a combination of secure socket layer (SSL), transport layer security (TLS), IPSec, and secure shell (SSH) authentication to protect sensitive data further.

Misrepresentation

The last of the major VoIP challenges is using misrepresentation to trick someone into taking action that enables theft or fraud – rather like social engineering techniques used by today's spammers, hackers, phishers and fraudsters

Phishing attacks on VoIP networks involve attackers faking the number of the phone they are using, making it look as though a legitimate organization is making the call. This increases the chance that the person on the receiving end will give away confidential information. However, anti-spoofing packet filters in the network will help prevent hackers or spammers hiding behind acceptable addresses.

Alternatively, a technique called 'call sink-holing' modifies network behaviour and, in addition to its legitimate uses, can be used to redirect calls to an impostor. This makes it essential for those operating VoIP systems to secure them effectively, limiting the ability to modify their configuration to appropriately authorized individuals.

> **"Phone calls will be separate from Internet traffic"**

Networks for the 21st century

Over the coming years, operators will be using IP networks to replace their current public switched telephone networks and older types of data networks. As a result, VoIP will eventually become the dominant – and potentially the only way of providing public phone services.

These new networks will, however, be more like the current converged corporate voice and data systems than the pubic Internet. The available capacity will be split to create a number of logically-separate networks that will carry different types of traffic. Phone calls will therefore be kept separate from other types of transmission, notably Internet traffic.

The way in which networks operated by different companies will be interconnected is yet to be fully defined but what is sure is that these new public phone networks will, in effect, be private. Each one will be owned and operated by a single company and will give assurance that the highest possible levels of security are being provided.

In the meantime, users of VoIP need to ensure they have a robust, resilient and effective security policy and appropriate precautions in place. The good news is that as VoIP is becoming more widely available, so are the tools to protect it.

About the author

Ray Stanton is global head of business continuity, security and governance at BT Global Services, a business with more than 30,000 staff who, between them, deliver services in more than 170 countries worldwide.

Zero Day of the Dead

William Knight

As you read this, zombie programs are flitting across the internet like a pestilence to infect and drain the life from innocent computer systems. Yet, for all the aggravation and grief they cause, you may never know you are part of a global invasion of system snatchers. Unless…

Once upon a time script kiddies were happy simply to infect computers with a virus and unleash an unexpected cascade of tumbling letters. But filthy lucre has corrupted the intellectual curiosity that drove those exploits; now there's big money in delivering insidious programs that hide, waiting silently for instructions from distant masters.

In this underground world, infected computers are called zombies. Programs that wait for commands are bots (short for robots), and a collection of bots is a botnet.

IT analyst firm Gartner says: "Although botnets are not new, they were previously referred to as zombie networks, their use as a vehicle for DDoS (Distributed Denial of Service) attacks has been the biggest concern. However, organisations are now realizing their impact in other forms of attack, for example in spam relays and as hosts for phishing web sites."

Gartner estimates that bots generate more than 70% of spam, and that through 2007, half of internet-active firms that do not implement prevention technologies will suffer service or financial losses due to botnet attacks.

Waspish attractions

According to Thorsten Holz, co-founder of the German Honeynet Project, there are thousands of botnets and millions of zombie computers. "It is hard to give exact numbers since we see only a limited amount of them," he says. "We observed a couple of hundred botnets and estimate that several million zombie computers are out there."

The Honeynet Project is a non-profit organization dedicated to improving the security of the internet by providing cutting-edge research for free. The project uses deliberately vulnerable machines to study the movement and influence of malware on the internet. Like wasps to a picnic, so malware is attracted to unprotected computers. "The mean time to compromise for

un-patched Windows 2000 systems in my network is less then 10 minutes," says Holz.

> "Zero-day attack has great value to botnet owners."

Botnets can contain tens of thousands of compromised machines. A botnet with only 1000 bots can cause a great deal of damage due to their combined bandwidth. A thousand home PCs with an average upstream of 128kbit/s can provide more than 100Mbit/s. If they are set to work in a DDoS attack, flooding enterprise networks with bogus requests, this is enough bandwidth to create major difficulties.

Legitimate origins

Bots have been used for many years to monitor and control Internet Relay Chat (IRC) automatically. IRC is an informal communication medium where subscribers send and receive text messages via a central IRC server. Messages sent are distributed to subscribers and categorised into channels (subjects or chat rooms, based on themes). Users subscribe to different channels depending on authentication or invitation.

So far so good, but users need help or even chastisement (for using profanity, for example) and bots help fill the need. A bot automatically responds to events while appearing to be a normal user on the channel. The bot may protect the channel from abuse, allow privileged users access to special features, log events, provide information, or host games. A quiz program is a typical example. Source code for bots is freely available (for example, www.energymech.net or www.eggheads.org).

While there are many legitimate uses, bots and botnets add an extra dimension to malware security. Richard Ford, research professor at Computer Sciences' Florida Institute of Technology, says botnets are "a great illustration of the maxim 'your insecurity makes my system insecure'."

You can be damaged by botnets without being infected, he says, and yet defensive strategies currently concentrate on endpoints—preventing individual infections—not on the botnet itself, and not on the fact we contribute to each others' security.

Ford likes an insect metaphor: you can squash one ant but it makes no difference. It is only when you destroy the queen you know you are safe. "If we don't kill the centre of the 'colony' we're simply engaged in a war of attrition with an enemy who always has the upper hand," he says.

Yet he cannot say for certain how a botnet might be destroyed, "Killing the colony might require attacking machines you don't own, this opens a whole bunch of difficult legal questions."

But if you can't shut them down, making sure your neighbour's machines are not used to launch an attack is also difficult. Their security arrangements may be, legitimately, less bullet-proof than your own. The internet will always be a hotchpotch of machines with different vulnerabilities, and there is no way of forcing a "duty of care" on the whole world, says Jon Fell, partner at IT law firm Pinsent Masons.

> "You cannot enforce a duty of care to the whole world"

But according to Fell, the US doctrine of "attractive nuisance," may apply to IT users that fail to keep their systems

Documented uses of botnets from the Honeynet Project

Distributed Denial-of-Service Attacks

Botnets flood a company's servers with thousands of data requests until the servers are unable to respond. Higher-level protocols can be used for specific attacks, such as running search queries on bulletin boards or recursive HTTP floods.

Spamming

Attackers are able to send bulk unsolicited commercial email (spam). Some bots also harvest email addresses to send phishing emails.

Sniffing Traffic

Sniffers are used mostly to seek sensitive information like usernames and passwords. If a machine is compromised by multiple bots, sniffers can gather security keys of the other botnets for a hostile take over.

Keylogging

Most bots contain keyloggers and filtering mechanisms (e.g. "I am interested only in key sequences near the keyword paypal.com.") to steal passwords and other secret data that may be protected by virtual private network or encrypted connections.

Spreading new malware

All bots implement mechanisms to download and execute files via HTTP or FTP. Botnets can launch mail viruses. The Witty worm is suspected to have been started from a botnet.

Click fraud

Using Google's AdSense companies can display targeted advertisements on their websites and earn money for each visitor that clicks on the advert. Botnets can automatically and repeatedly click on these advertisements, fraudulently increasing the click count.

Attacking IRC Chat Networks

IRC networks are flooded by service requests or thousands of channel-joins from the botnet. The victim IRC network is brought down as with DDoS attacks.

Manipulating online polls and games

Online polls/games are rather easy to manipulate with botnets. Since every bot has a distinct IP address, every vote has the same validity as a vote cast by a real person. Online games are manipulated in a similar way.

Identity theft

Phishing emails are generated and sent by bots via their spamming mechanism. The bots host multiple fake websites that pretend to be eBay, PayPal, or other bank, and harvest the sensitive data. Keylogging and traffic sniffing can also be used for identity theft.

secure and thus unwittingly participate in acts that damage others.

"The example usually given," says Fell, "is that of a child who sees a swimming pool in a garden, enters the pool and subsequently drowns. A homeowner could be liable for the death if he had failed to take sufficient precautions to prevent such an event, for example, by installing fencing around the pool.

"There is certainly a risk that an party who fails to take sufficient steps to keep hackers from entering their systems could be found negligent if the hackers disrupt others via his system," he says.

But the risk is small, he says. "To date there have not been any cases decided on this point. Even a business whose lax security allows a hacker to launch attacks via its systems may escape liability."

> **"A criminal with no significant assets can target over a billion potential victims"**

And recent analysis of the doctrine suggests that by itself it will not be enough to launch a successful case for damages. "The person who suffers loss is in the wrong category," says Fell. "They haven't been attracted to the computer in the first place."

That leaves legal recourse difficult to pursue, undermining reasons to invest in protection. None the less, modifying a system without a user's express permission remains punishable by up to five years under section three of the UK's Computer Misuse Act (CMA) 1990.

Detective Inspector Chris Simpson is with the Economic and Specialist Crime Directorate of the Metropolitan Police Computer Crime Unit (CCU). Speaking at (ISC)2 Secure London event, he said: "If an individual is concerned in any one of the following: authoring the malicious code behind the botnet; managing the botnet itself or being responsible for funding or initiating its creation, that person could potentially be convicted as part of a conspiracy to commit offences under the Computer Misuse Act."

Which appears to leave the owner of an infected system in the clear.

Simpson stressed the importance of traditional approaches to information security. "People should consider how to prevent or manage infections and DDoS attacks, and also how to raise awareness of IT security within the business environment. Many of the cases investigated by the CCU were infinitely preventable, if only policy was in place and supported by procedure and appropriate management systems," he said.

Ford thinks the botnet phenomenon will worsen. With commercial reasons to create zombies growing stronger (see sidebar), the value of exploits that install bots is rising. "If a botnet owner wishes to expand his network, and that network makes money, it stands to reason that a zero-day attack has value to him. The goal of a botnet is to spread under the radar, so using an unknown exploit and keeping that exploit out of sight makes sense."

Simpson is optimistic the CCU can combat the growing zombie armies, even with the cross-border complications inherent in investigations. "There is extremely good co-operation between international law enforcement and industry. Results in the UK, US, Canada, Holland and Eastern Europe are evidence of this." (See sidebar.)

But it is the immensity of scale that makes a zero-day exploit so valuable. As Simpson points out: "In the physical world the number of crimes an individual can commit is limited by their physical capacity. In contrast, across the internet, a criminal without any significant assets can target over a billion potential victims."

This rich field of potential victims and the value of infection makes it inevitable botmasters will try to grow their legions of zombies. A zero-day attack is perfect for their diabolical plans: use your head; make them lose theirs.

What vendors say you should do

"Companies should install software to identify bots on their networks and close those communication channels. Bots can use any protocol they want to communicate. Stopping IRC will never be enough." Jose Nazario, Arbor Networks' senior security advisor.

"Anti-spam applications will greatly reduce this problem but real-time blacklists become less useful. Companies should be backing initiatives that counteract spam like Sender Policy Framework (SPF)." Simon Heron, Network Box Defence Systems.

"Web browsers are probably the most frequently abused port of entry. It's harder to take down Firefox than IE by spyware, so consider switching." Mark Stevens, chief strategy officer at WatchGuard

"A holistic approach to security is essential. It's no longer sufficient to rely on traditional anti-virus techniques." David Emm, senior technology consultant, Kaspersky Labs

"Companies should definitely be looking to shore up their IM channels. Many of the hacker groups we monitor are moving away from web page drive-bys in favour of spreading their payloads via IM." Chris Boyd, security research manager, FaceTime Communications.

Court in the act

December 2004, UK and Canada
A British convicts a 16-year-old Briton of releasing the Randex Trojan, used to relay spam. Canadian police charge another 16-year-old with writing and distributing the worm. Randex quickly infected more than 9,000 computers.

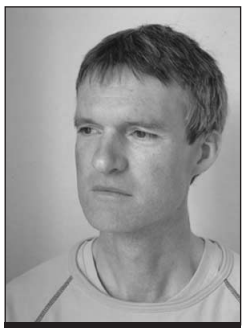
August 2004, US
Operation Cyberslam results in indictment of Jay R Echouafni and Joshua Schichte on charges of conspiracy and causing damage to protected computers. They allegedly used a botnet to send bulk mail and set up DDoS attacks against spam blacklist servers.

January 2005, US
Jeanson James Ancheta pleads guilty to installing and controlling tens of thousands of zombie computers used for spam, DDoS and adware. Ancheta allegedly makes over US$60,000.

October 2005, The Netherlands
Dutch police arrest three people for building a 100,000 PC botnet. Compromised machines were infected with the W 32.Toxbot Trojan. Investigations surround DDoS attacks, Paypal and eBay fraud.

February 2006, US
Christopher Maxell and two juvenile accomplices allegedly made US$100,000 with pop-up adverts on compromised computers. Their botnet is also suspected of DDoS attacks of Seattle's Northwest Hospital in January 2005.

ISP data retention becomes a reality


Philip Hunter

Philip Hunter

Data retention has suddenly become the hottest issue for ISPs and telecommunication operators now that the European Union has at last brought in its controversial directive on the subject after more than four years of wrangling since 9/11. In the event the EU beat the US to the draw, although the major surfing sites run by Google, Yahoo, and Microsoft have come under intense pressure from the federal government to release search data.

Privacy

The EU's move has naturally enraged privacy groups, which clubbed together to condemn the directive in an open letter arguing that it represented an irreversible decline in civil liberties and consumer rights. It is hard to dispute such arguments, but the fact is that in the post 9/11 era, the public's fear of violent crime and terrorism has leapt ahead of its desire for privacy and civil liberties. As a result privacy groups have had little success rousing widespread public opposition to data retention legislation.

Next Summer

Member countries have until August 2007 to implement the directive, which compels ISPs along with fixed line and mobile operators to retain details of their customers' communications for between six months and two years. Although this does not extend to message or conversation content, it does include all information needed to pinpoint source and destination, including the location of both parties in the case of mobile sessions. It also includes details of websites visited during browsing sessions.

Listening in

Although the privacy lobby appears particularly concerned over the ability of police to monitor the location of parties to mobile phone calls by exploiting triangulation data from base stations, the most Orwellian aspect concerns remote activation of the microphones in hand sets. Although not part of the directive, which deals only with electronic communications of some sort, more recent mobile phones capable of having software downloaded to them can have their microphones switched on remotely by the cellular operator without the user's knowledge. This gives the police the potential to listen in not just on telephone calls, but the user's private conversations with people nearby, providing the handset is switched on. It has been reported that in the UK, police have an informal agreement with mobile phone operators to ask for appropriate software to be downloaded to specified handsets to activate this eavesdropping facility, although it is not known whether this has yet been done. It is also unclear how valuable this capability will be in combating terrorism and crime, any more than access to conversation or messaging content will be, although it raises the question of whether police could also turn on voice over IP (VOIP) phones remotely.

The fact that content has been excluded from the EU directive is not so much a handicap for law enforcement, given that serious criminals and terrorists will avoid use of public networks to arrange their activities, or if they do they will perhaps resort to private encryption schemes. It is the ability to monitor sources, destinations and locations that is potentially valuable in identifying patterns of activity that might suggest a crime or terrorist act was being planned. Such information combined perhaps with surveillance data from increasingly ubiquitous video cameras will help track activity, given that criminals need to communicate somehow via face-to-face meetings, even if they avoid electronic communications.

Costs

Be that as it may, ISPs and telcos face a nightmare conforming with the emerging regulations. It appears that they will have to pay for storing and managing the data, although in the UK Home secretary Charles Clarke has indicated that the government may help, without spelling out precisely how.

Inevitably costs will be incurred by operators and passed on to customers. There is wider concern that the directive will reduce European competitiveness as a whole, running counter to other EU measures to boost it, such as investment in fibre-based broadband infrastructure. Indeed it is for this reason that the US has been notably more reluctant to impose data retention on its telcos and ISPs, even though it has been quite happy to deploy other draconian measures.

> **"Content is excluded from EU Directive"**

Until recently the US Justice Department still maintained that data retention imposes an unacceptable burden on Internet providers, and even now after hardening its position is still hoping that voluntary cooperation will be sufficient.

This burden is not purely the cost of storing the data. That is relatively straightforward, with ISPs and telcos already recording a lot of information for other purposed related to billing, customer relationship management, and corporate governance. Many of the real costs are related to making the data secure, for one of the ironies is that ISPs and telcos will be held responsible for leakage of personal information covered by legislation such as the Data Protection Act. So they

could be penalised both for failing to record certain information, and then for failing to protect it properly when they do record it.

But the spotlight is not just on service providers. Increasingly corporate compliance and anti-terrorism laws are bearing down on their business customers, and in this case content of both emails and telephone conversations sometimes does have to be recorded. So in effect police and other agencies often do have potential access to all aspects of a communication, including:

- Content.
- Time.
- Duration
- Identity of the parties.

But it is all a mess, with the information distributed between different locations and jurisdictions. It could make more sense to log the information in one repository, accessed according to strict rules, although there is little sign of that happening.

In practice data retention had become a reality before the EU directive, through voluntary schemes in some countries such as the UK. Indeed police clamed that access to retained telephony data helped them find both the culprits and accomplices of the 7 July 2005 London bombings, as well as the Madrid 2004 Madrid train bombings.

> **"Telephony found London bombers"**

In theory such data could help thwart such attacks before they take place, but in practice it is impossible at present to sieve such information from the almost bottomless pit of data about all telephone conversations and Internet sessions. In reality police only access retained data after the event has taken place, so the argument for having it is to assist in finding the culprits rather than to prevent the act taking place.

Italy and Ireland

Two European countries, Italy and Ireland, did predate the EU directive with compulsory data retention. In Italy this came in July 2005 with a decree compelling mobile and fixed telephony data to be retained until the end of 2007, and for Internet providers to keep it for six months with a possible extension for another six months, in this respect conforming in advance to the EU directive.

Ireland was first to introduce measures in 2002, requiring fixed and mobile telephony data to be retained for three years, but excluding location data, emails and Internet activity at that stage. The rules were introduced in secret through agreement between the government and telephone companies, but became statutory early this year, although without prior warning or consultation. So it could be argued that the preceding arrangement was voluntary, although it was clear that failure by a telephone company to comply would not be acceptable.

Ironically Ireland, after leading the campaign in Europe for data retention, is now threatening to challenge the EU directive, with Minister for Justice, Michael McDowell threatening to take it to the European Court of Justice. The argument though is not over the directive's content but whether the European Commission and Parliament rather than national governments should settle such sensitive matters. This position, supported by the government of Slovakia, has been backed by the privacy lobbying group Digital Rights Ireland.

Ambiguities

For ISPs and telcos though it is largely academic whether legislation is forged by national governments or the EU, although regional differences could muddy the waters even further given that conversations and messages often cross country boundaries. The key point is that legislation is coming, whether from individual countries or EU-wide. Perhaps the real problem is that ISPs and telcos have to shoot between moving and fuzzy goalposts. The basic rules may appear clear enough, but the mechanisms for implementing them are ill defined and may well only be clarified when tested in courts and procedures for protecting information are found wanting.

There are also plenty of ambiguities and uncertainties. VOIP is one of these, for it has not been defined whether this falls under the rules governing voice or data, given differences between the two over what information should be recorded. There are no rules either governing the level of protection that should be given to recorded data, and yet ISPs and telcos would be in trouble if they could not furnish the data on request from an approved agency such as the police or Inland Revenue.

> **"Customers need to be made aware"**

Customers

Yet another potential pitfall for ISPs and telcos concerns disclosure to their customers that data is being retained. An issue here is the potential conflict between the new data retention laws and privacy legislation that predated it. In order to enforce data retention, some countries have to override certain aspects of existing privacy or confidentiality laws. When Italy adopted the EU's e-privacy directive of 2002, its government immediately legislated for an exception to the obligation to erase traffic data, in order to avoid any obstacles to subsequent data retention laws.

Customers however could not reasonably expect to know of such exemptions, and so ISPs and telcos need to make them aware both that they are collecting the data and that existing data protection or privacy legislation does not prevent disclosure to specified parties. If in the process of such disclosure, data leaks to other parties, it is not clear who would be responsible.

The upshot is that the costs and implications of data retention will only gradually emerge over the next few years, although there is little doubt that privacy will continue to be eroded.

Cisco gets physical with video surveillance camera acquisition

Sarah Hilley

Will Cisco's acquisition of video surveillance company SyPixx kick start the long anticipated convergence of IT security and physical security? Sarah Hilley reports.
Cisco's move into video surveillance, with the acquisition of SyPixx Networks, could give companies a Big Brother' view of employee activity.

The network giant says the acquired video surveillance will make video more useful and accessible. Cisco's product offering of converting analogue video to digital, with integration into the network, will make surveillance film more manageable and easily searchable, it promises.

Easy searchability is also the selling point behind many email compliance solutions that have been springing up to help banks and such cope with having to store and produce email records for regulators.

Easy search

Marthin De Beer, Vice President of Cisco's Emerging Market Technologies Group says that it can take time to search video tapes, but it becomes a non-issue when the video is in digital format. Cisco will sell an encoder device that does the job of conversion. De Beer also says that IP network-connected cameras "can dynamically retrieve video from anywhere to investigate." Also, old analogue could only be viewed on site in a special central control room. But now "you can stream video across the network to a central control room." You can also timestamp the video, and digitally record it.

The integration holds the potential for some futuristic security checks. De Beer says: "The network with security capabilities is a big opportunity that can bring new intelligence. As things converge, customers will have less administration and one source of truth.

"In the future, if someone walks by a camera and presents a badge to enter a building, it will be possible to scan the face and make sure it is the right person holding the badge." He also believes that event triggered recording will be feasible. "Imagine the ability to set physical security policies after 10pm at night - if I get movement, I start recording and notify certain people - and begin streaming video across to different offices."

Last night's video

Cisco's new portfolio from SyPixx includes analogue to digital (IP) video camera encoders, digital (IP) to analogue video monitor decoders, analogue video transmission equipment, video recording and management software and servers. The digital video recording software gives the ability to merge recorded and live video streams, showing what gets recorded where and when. It will allow for a network-based video surveillance team. It will be possible to bring up, for instance, video from the night before at, say, 12 requested locations.

The target of integrating video into IP is not just Cisco's idea. Other vendors are already making headway. "They are all moving towards IP," says De Beer. The trend has been around for about three years now.

"The market has grown by 40% in the last three years - it is expected to be worth $2 billion next year." And Cisco has spent $51 million in cash and stock on Connecticut-registered SyPixx Networks to get a slice of the pie. The deal is expected to close at the end of April. SyPixx was only founded in 2004 and has 27 employees based around the US.

However, Cisco will not be taking on the bigger players, like Siemens, GE and Sony, with the newly acquired Sypixx, says De Beer. "We don't intend to challenge them - they make money on their cameras. We provide network infrastructure - but they will sell less legacy wiring."

He also says that Siemens sells proprietary packages, and Cisco will have to cooperate with them to make sure its encoders and decoders are interoperable with their cameras. De Beer believes that Cisco's position as a network provider gives the company a unique perspective. "The network is the only entity that touches everything in the IT world. It is the only common piece."

First foray into physical

De Beer said that he is not aware of any other IT companies getting into the space. It is Cisco's first venture into physical security but the company already has experience selling IT security gear - through the Self Defending Network strategy. The new physical security products and the IT security offerings are both classified as 'advanced technologies' within the company's hierarchy. The physical security gear belong to a new unit in Cisco's Emerging Market Technologies Group, headed by De Beer.

The target customers are in retail, transport, banking, financial services and gaming. De Beer refuses to name any of SyPixx's existing customers.

Integration of video into the network is happening with or without Cisco's presence. Whether the conversion into digital will kick-off the long anticipated convergence of IT security and physical security, remains to be seen.

Sarah Hilley is the freelance editor of Computer Fraud & Security. *sorchahilley@hotmail.com.*

2,000 Mastercard details swiped

MasterCard is delving into the theft of 2,000 sets of credit card details. *The Scotsman* reports that one Clydesdale Bank customer found out that her card details were in the hands of a fraudster. The theft had been detected and the card was stopped before it could be used.

The Scottish bank would not comment except to say it was advised of the problem by MasterCard.

It is believed that the details were stolen following a security breach at a shop based in the UK.

MasterCard, meanwhile, has insisted that their own security systems have not been breached and that they are monitoring credit card transactions for signs of suspicious activity.

A source at MasterCard is quoted as saying: 'MasterCard is aware of a potential security breach at a UK-based retailer. But because this is an ongoing investigation, we cannot disclose specific details regarding the incident or comment, other than to say that we are cooperating and we have notified the banks that issue MasterCard cards to monitor for any suspicious account activity and take the necessary steps to protect cardholders.

'MasterCard's systems have not been breached and no MasterCard data have been compromised. MasterCard International is concerned whenever cardholders are inconvenienced and we will continue to monitor this event.

'As usual, if a MasterCard cardholder is concerned about their individual account, they should contact their issuing financial institution'.

EVENTS CALENDAR

22-14 May 2006
IFIP AND SEC 2006
Location: Karlstad, Sweden
Website: www.sec2006.org

4-7 June 2006
TECHNO SECURITY CONFERENCE
Location: Myrtle Beach, CA, USA
Website: www.techsec.com/html/Techno2006.html

5-7 June 2006
GARTNER IT SECURITY SUMMIT
Location: Washington DC, USA
Website: http://www.gartner.com/2_events/conferences/sec12.jsp

8-9 June 2006
BIOMETRICS INSTITUTE AUSTRALIA CONFERENCE
Location: Sydney, Australia
Website: www.biometricsinstitute.org

12-14 June 2006
CSI NETSEC
Location: Scotsdale, Arizona, USA
Website: www.www.gocsi.com/netsec/

14-16 June 2006
INFOSECURITY CANADA
Location: Toronto, Canada
Website: www.infosecurity-canada.com

16-21 July 2006
IEEE CEC 2006 SPECIAL SESSION ON EVOLUTIONARY COMPUTATION IN CRYPTOLOGY AND COMPUTER SECURITY
Location: Vancouver BC, Canada
Website: http://163.117.149.137/cec2006ss.html

29 July-3 August 2006
BLACKHAT USA
Location: Las Vegas, USA
Website: www.blackhat.com

24 August 2006
IDC's 5. Security Conference 2006 Switzerland
Location: Zurich, Switzerland
Website: www.idc.com/getdoc.jsp?containerId=IDC_P11637

4-6 September 2006
INFOSECURITY RUSSIA
Location: Moscow Russia
Website: www.infosecurity-moscow.com/index.en.html

7 September 2006
IDC's 5. Security Conference 2006 Germany
Location: Frankfurt, Germany
Website: www.idc.com/getdoc.jsp?containerId=IDC_P11635

12-14 September 2006
INFOSECURITY USA
Location: New York, USA
Website: http://www.infosecurityevent.com/App/homepage.cfm?moduleid=42&appname=100004

13 September 2006
SECURITY CONFERENCE 2006, SWEDEN
Location: Stockholm, Sweden
Website: www.idc.com/getdoc.jsp?containerId=IDC_P10573

20 September 2006
IDC SECURITY FORUM
Location: New York, USA
Website: www.idc.com/getdoc.jsp?containerId=IDC_P11568

20-22 September
INFOSECURITY INDIA
Location: Bangalore, India
Website: http://www.infosec-world.com/page.cfm/link=186

11-12 October 2006
INFOSECURITY NETHERLANDS
Location: Utrecht, The Netherlands
Website: http://www.infosecurity.nl/sites/www_infosecurity_nl/en/index.asp

23-27 October 2006
SYSTEMS IT SECURITY AREA 2006
Location: Munich, Germany
Website: http://www.it-sa.de/index.php?id=89&L=1&PHPSESSID=faf92a83813690da57e9d464b8e39a35

6-8 November 2006
CSI 33rd Annual Computer Security Conference & Exhibition
Location: Orlando, Florida
Website: www.gocsi.com/annual/