

THE MAGAZINE OF THE BCS SECURITY FORUM

iSNOW

WINTER 2010

www.bcs.org/security

FUTURE THREATS

With new, powerful mobile devices come new and dangerous threats

bcs

The
Chartered
Institute
for IT

08 MOBILE BOT THREAT

We all know about the botnet threat to PCs, but now this is extending to mobile devices too.

12 BLOCK CRIMINAL CLOUDS

When you consider the power and capability of the cloud, it's not surprising that criminals use it.



UNIVERSITY OF
OXFORD

part-time study in:
network security
trusted computing
security design
forensics
people and security

msc in software and systems security
www.softeng.ox.ac.uk/security

EDITORIAL

Henry Tucker Editor
Brian Runciman Managing Editor

PRODUCTION

Florence Leroy Production Manager

Advertising

E catherine@atalink.co.uk
T +44 (0) 20 7074 7921

Keep in touch

Contributions are welcome for consideration.
Please email: editorialteam@hq.bcs.org.uk

ISNOW is the quarterly magazine of BCS Security Forum, incorporating the Information Security Specialist Group. It can also be viewed online at: www.bcs.org/isnow

The opinions expressed herein are not necessarily those of BISL or the organisations employing the authors.
© 2010 British Informatics Society Limited (BISL). Registered charity no. 292786.

Copying: Permission to copy for educational purposes only without fee all or part of this material is granted provided that the copies are not made or distributed for direct commercial advantage; BISL copyright notice and the title of the publication and its date appear; and notice is given that copying is by permission of BISL. To copy otherwise, or to republish, requires specific permission from the publications manager at the address below and may require a fee.

Printed in the UK by Interprint, Swindon, Wiltshire.
ISSN 1752-2455. Volume 5, Part 2.

The British Informatics Society Limited
First Floor, Block D, North Star House,
North Star Avenue, Swindon, SN2 1FA, UK.
T +44 (0)1793 417 424
F +44 (0)1793 417 444
www.bcs.org/contactus
Incorporated by Royal Charter 1984.



FUTURE THREATS



04

ISSG PERSPECTIVE

Gareth Niblett, Chair of the BCS ISSG, gives his view on future threats.

06

THE E-CRIME BUSINESS

Cyber crime is now run as a business so what can be done to stop it?

08

THE MOBILE BOT THREAT

We all know about the bot threat to PCs, the risk is there for mobile devices too.

10

OUT IN THE COLD

Small businesses can be left out when it comes to digital forensics.

12

BLOCK CRIMINAL CLOUDS

It's not that surprising that criminals are now using cloud computing.

14

BIOMETRIC REVOLUTION

Is now the time to truly embrace technologies like fingerprint and iris readers?

16

LEGAL

A look at some issues around data sharing and the Data Protection Act.

18

OPINION

When it comes to safeguarding your belongings you need more than just good locks.

Gartner Identity & Access Management Summit 2011

9 – 10 March 2011

Park Plaza Westminster Bridge, London, UK

europe.gartner.com/iam

Improve Your Identity and Access IQ to Improve IAM and Business Performance

HOT TOPICS

Architecture

Authentication

Enterprise Single Sign-On

Entitlements

Governance, Risk and Compliance

Identity Federation

Identity and Access Intelligence

Outsourced/Third Party Challenges

Password Management

Privilege Management

Program Governance

Regulation, Privacy and e-Discovery

Role Management

Stakeholder Engagement and Support

User Provisioning

Web Access Management

View the full agenda online at europe.gartner.com/iam



COMING THREATS

Gareth Niblett, Chair of the ISSG, looks at some of the things we should be looking out for in the security landscape for 2011.



The start of each New Year brings festive cheer and thoughts about what security related treats we might see in the coming year. I think 2011 may bring:

Targeted malware – next generation spear-phishing. The emergence of Stuxnet, which combines traditional malware techniques with a specially crafted targeting mechanism and payload parameters, may signal a new form of

deniable attack. Even with the required time and resources required to develop the intelligence and programming that feeds into such software, it could still be a much more cost effective and politically acceptable virtual approach versus physical alternatives. This attack vector is likely to be picked up by other online ne'er-do-goods.

Secrets revealed – exposing truths.

Wikileaks, Crytome, The Smoking Gun and others have a track record of exposing the secrets of governments, corporations and individuals. State and court sanctions are unlikely to deter all those seeking to expose unlawful, hypocritical and immoral activities. Once details are released on the internet it is too late, however good your censorship capabilities are and if the traditional press get hold of it too it's as good as over. As people learn the effectiveness of such exposure we may see more whistleblowers emerge.

Personal intrusions – self-exposure.

From airport security officials wishing to either irradiate us or touch our junk; governments wanting to know about our worldwide banking arrangements, health,

happiness and online activities; social networks wanting to know where you are, who your friends are and what you're saying; advertisers wanting to know where you are and what you're interested in; employers wanting to know if you're a suitable hire or risk to the business.

Happy New Year – hopefully.

Gareth Niblett is Chairman of the Information Security Specialist Group (ISSG).

www.bcs-issg.org.uk

FURTHER INFORMATION

Information Risk Management and Assurance Specialist Group:
www.bcs.org/groups/irma

BCS Security Portal:
www.bcs.org/security

ISNOW online:
www.bcs.org/forum/isnow



CLOSING THE E-CRIME BUSINESS

Organised crime is run as a business so should we be surprised that the same methods are being used in order to deploy malware? Recent reports have suggested that organised crime in the UK may be moving into e-crime, says **Tony Proctor** WARP Manager at the University of Wolverhampton.

This is happening because of the high rewards to be gained and the difficulty in detecting those who 'do it well'. As legitimate businesses have moved online it is natural that the less legitimate seek to gain the same benefits. Malware and the internet really do make it possible for a global business to be established overnight.

The con trick has evolved into social engineering. It plays an increasingly important role in targeting users and helps to establish the credibility required to manipulate users into acting in a way that they would not normally do. The use of online social networks has provided an

assistive environment in which a fraudster can conduct research in order to produce targeted phishing attacks. As new technologies emerge into wider use, they will present business opportunities for e-crime.

Spam spotting

The manner in which a user is enticed to run malware on their computer demonstrates an increasing level of professionalism. For example, it is becoming more difficult to determine an obvious spam email because the mistakes in the use of language and grammar have

decreased. The world-wide uptake of broadband has produced an increase in non-English spam and reports suggest that spammers are recruiting native speakers in order to target particular nations. There remain a number of countries where legislation or enforcement is weak and that can serve as safe havens where e-criminals can operate unhindered.

The methods of coercion also continue to evolve. For example in recent instances a phone caller claims to be from a credible organisation and informs the receiver that they have detected a problem with their computer. As the conversation progresses,



Hence detection can be extremely difficult. The capabilities of terrorists to conduct electronic warfare is often hyped in the media and played down officially. But there

nature of the update that the infected host receives. So something that is on one day a Trojan can the next day become a virus or a worm.

The internet was not designed with security in mind and it lends itself to an entrepreneurial approach that cannot be restricted to legitimate activity.

is a link between some organised crime and terrorists who need to obtain and launder money to support their operations. Equally, those who make malware services available for purchase are unlikely to worry about who they are selling to (assuming that it is even possible).

Why don't we know more about the shady organisations that are behind e-crime? The answer is because they are criminals. You don't tend to know too much about the underworld unless you deal directly with it. So whilst e-commerce racketeers require the web to sell their services, tracking their activity is made difficult by evasion techniques (e.g. the use of money mules) and technology (the anonymity that the web can provide).

Share and share alike

Underground networks exist on the internet where hackers share information and can be contracted to produce malware. Reports suggest that malware can be easily bought

However, 'professional' malware goes beyond developing code simply to compromise a device. Increasing sophistication means that the malware may, for example, install itself at root level and virtualise the machine, running existing applications in a virtual machine. Hence it is much less likely to be detected by AV programs. It then creates a backdoor so that if it is found and removed it can be re-installed. It might install its own AV so that it continues to have the dedicated use of all resources. The aim of professional malware is to support business continuity and hide any trace of its own existence.

The internet was not designed with security in mind and it lends itself to an entrepreneurial approach that cannot be restricted to legitimate activity. The crime is only limited by the imagination of the criminal. Hence prevention, detection and (where possible) prosecution is an inevitable player in a continuous game of catch-up.

E-criminals make use of fast-flux hosting. This means that the spam servers or those downloading updates to compromised hosts will change every few minutes.

'off the shelf' from £200 with various add-ons / customisation available that make it difficult for defensive software to detect. Some reports even suggest the availability of money-back guarantees.

Corrupt networking companies exist too. These effectively act as ISPs for criminal activity. They knowingly facilitate the downloading of illegal material, phishing emails, malware and other criminal activity.

The many tools that are readily available on the internet can be either deadly or useful depending on whether the colour of your hat is black or white. Frameworks such as metasploit can serve as starter kits for malware development. The clarity with which malware can be identified as a virus, Trojan or worm is becoming blurred. Thanks to botnets, the functionality of a piece of malware is determined by the

Vigilance

How can we defend effectively against malware that slips beneath the radar or zero day attacks? The emphasis has to be on vigilance in an effort to identify incidents early. That is to say, we educate and encourage users into noticing and reporting the unusual and we develop and deploy better heuristic based products to detect and react to unusual activity. Perhaps a secure cloud is the answer to many of the problems that we currently experience or maybe e-criminals will simply find new and innovative ways to continue their business.

For more articles go online to: www.bcs.org/articles

the user is talked through downloading a program (malware) to solve the problem.

It is also interesting that despite all the knowledge and experience that exists in the information security world, we still seem unable to accurately identify the origins and purpose of some of the major malware attacks (e.g. the conficker worm). The suspicion is that large botnets of this type are owned by criminals who make them (or parts of) available for hire. E-criminals make use of fast-flux hosting. This means that the spam servers or those downloading updates to compromised hosts will change every few minutes.



STOPPING THE MOBILE BOT THREAT

We all know that we need security software on our PCs, but how many of us have protection for our smartphones? Lannon Rowan MBCS examines the threat of botnets to mobile devices.

The current worst challenges that are faced daily by security and risk management originate from blended threats and Web 2.0. The notion of a blended threat is an attack that targets different areas of the network. Since 2007 attacks have been gaining in complexity and as such require new security approaches. Web 2.0 has added to the problem by allowing users to operate in real-time in any location at whatever time they want. Security research findings show a 250 per cent increase in malware from 2009 to 2010.

Blended threats change continually and this means that signature-based content security systems are often out of date in

less than 24 hours. At the start of 2010 the first genuine threat to mobile devices was reported. The Zeus bot was specifically crafted to steal banking details of mobile phone banking users.

Two things have happened since; the first is that the number of infected systems has risen and the second is that the bots are now able to steal more than just banking details (100,000 currently infected - BBC 4 August 2010). Bots can make calls or send SMS messages to premium numbers as well as other insidious actions without the user knowing.

A criminal is now able to make a profit from these bot attacks and as history has

shown, if there is money to be made, more resource will be used to specifically target users via attacks that are country or company specific to maximise additional revenues.

The application layer in itself is under constant exploit and attack and this also affects mobile users. Adobe has had to implement a fixed security patching cycle because of the number of security vulnerabilities being found on its products. Mobile devices also use some of the products and it could be possible to exploit a mobile phone that accesses a website in the future. When one problem is fixed it sometimes creates another unknown problem in its place.

- A Fortune 15 company found that five per cent or 25,000 of its mobile devices were infected with malware.
- Calls to high premium numbers could generate revenue for attackers.
- A 250 per cent increase in malware from 2009 to 2010.
- Malware could move from mobile to PC platforms and harvest a lot more information,
- 61 per cent of all reported smartphone infections were spyware, capable of monitoring communication from the device.
- A different kind of big brother is listening to all your calls. Think of the implications.
- 17 per cent of all reported infections were text message Trojans, which charge fees to a device's account holder.
- Attackers want to make money. Mobiles offer a new way for them to do that.

on a regular basis. For example, an analysis of Google Android Froyo's open source kernel has uncovered 88 flaws that could expose users' data. (<http://tinyurl.com/248zngk>).

Coverity has said it will hold off releasing full details until January giving Google time to provide fixes. Functionality seems to have been the primary aim and security a second.

Malware launch pad

According to Adrienne Hall who is the General Manager of Microsoft Trustworthy Computing, 'botnets are the launch pads for much of today's criminal activity on the internet.

In many ways, they are the perfect base of operations for computer criminals. Botnets are a valuable asset for their owners, bot herders, who make money by hiring them out to other cyber criminals to

The attack space has widened further with the availability of smart phones with capable browsers and rich featured operating systems.

'People are using smartphones to access work files, store personal information, conduct banking and download applications,' said Daniel V. Hoffman, Chief Mobile Security Evangelist at Juniper Networks. 'Yet, while most PCs come with security baked in, virtually all smartphones remain vulnerable to even basic exploits and attacks.'

'The Juniper Global Threat Centre identifies, monitors and responds to evolving threats to mobile devices, ensuring that Juniper customers have the highest possible level of mobile device protection'.

Lack of security

This stands in stark contrast to the security that is given to PCs and laptops. Mobile device usage is increasing; Gartner says that mobile phone sales grew 17 per cent in Q1 and 13.8 per cent in Q2 2010 alone. Competition is driving some prices down and it is clear that the threats from mobile devices are here to stay and will rise continually in volume and complexity.

Real time security information is the only defence for this and vulnerability management as a whole. Proactive or offensive security is what is now required as the evolution of risk domains shows. The volume and sophistication of security attacks has forced a shift from traditional reactive security models.

Mobile phone providers have been forced to support numerous new Web 2.0 products such as Facebook and this has stretched the operating system to a point where security flaws are being discovered

use as a route to market for cybercrime attacks such as phishing attacks, spam attacks, identity theft, click fraud and the distribution of scam emails. Bot herders guard their botnets jealously and invest huge amounts of time, effort and money in them.' It makes natural sense that the criminals would be looking to expand their businesses, and mobile devices are the next logical step.

Mobile device manufacturers are constantly bringing out new devices and operating system updates, patches and new releases. The continually evolving market provides a continual security challenge and attack opportunity.

Blended threats

How will user education programs be shaped to include mobile phones and bots? Bots are the next step in the blended security threat landscape, which is evolving on a yearly basis and internet access is now expected by mobile users. But at what risk?

I suggest that organisations should be thinking about and adopting and integrating mobile security into their security strategies. But how will our organisations know about these threats to corporate mobile users and other emerging threats from bots? Users struggle with computer security at the best of times.

For more articles go online to: www.bcs.org/security

Looking at the market progress, the risks are increasing by 250 per cent a year and the threat is originating from blended threats, such as bots that can steal mobile banking details.

The threat is starting to develop teeth and the countdown to widespread security incidents started in 2007.

The following are some of the preliminary findings from the Juniper research centre:

- An analysis of Android Marketplace applications capable of malicious activity showed that 1 out of every 20 applications requested permissions that could allow the application to place a call without the user's knowledge.



OUT IN THE COLD

Ron Tasker MBCS, a lead digital forensics consultant, says that even the smallest businesses may have need for the skills of digital forensics.

Digital forensics is a relatively new field. It could be argued that even law enforcement in the UK is in its infancy when it comes to the prevention, detection and successful prosecution of cybercrime.

In this new, developing field, two main threads of the industry have formed. Those principally involved with law enforcement and those principally involved with corporate consultancy. Subdividing even further, small, independent consulting companies have largely tried to focus on contracts arising from law enforcement

agencies, whilst corporate investigations have for the most part been carried out by large management consultancies.

These days, we often hear stories of large companies who have been subjected to insider and outsider digital attacks. It seems relatively common to encounter instances of financial fraud, employee theft or the simple misuse of IT assets in the workplace. In response to this trend a network of commercial investigation companies, often arms of large management consultancies, has sprung up

to service the demand for digital forensics investigation. Access to digital forensics or eDiscovery professionals via a management consultancy can be extremely expensive, often rendering it prohibitive to small and medium sized companies. It could be argued that digital forensics professionals are effectively out of reach for small companies.

Small businesses, however, still need to be able to check and police employees and customers. Where any suspicion exists of inappropriate computer use, it can be

critical that potential rogue activity is investigated and evidence is obtained. Small businesses suffer from many forms of employee or customer abuse, ranging from inappropriate use of email to fully fledged fraud. Many small businesses do not have dedicated technical staff, which may mean that, if undetected, perpetrators may continue and even escalate behaviour until it becomes a critical factor for the survival of the business itself.

If the person responsible for the abuse is an employee, then things can be very difficult indeed. Simply poking around for evidence of wrongdoing, even if it is found, is usually not enough to satisfy employment tribunals.

Evidence must be gathered in a forensic fashion, with audit trails and, where possible, full repeatability. This ensures that any evidence gathered is more likely to be accepted at tribunal and less likely to be tainted by an investigator. It is even more important, should evidence of criminal activity be found and the matter is passed to the courts. A sound forensic approach requires training. Investigators should, apart from their technical knowledge, be forensically trained and this means that digital forensics professionals are often not cheap to employ.

Vulnerable SMBs

So where does all this leave small businesses? The answer is, surprisingly vulnerable. With no coherent approach to small business from the digital forensics industry, small companies may become the target for employee abuse or worse, cybercrime.

On the other hand, there is a tremendous market opportunity for independent forensic professionals to serve this sector of the market. Due to the nature of most small businesses, the complexity of their IT is often very low.

This makes for small, quick and clean investigations where an investigator need only invest a small number of billable hours per investigation. If competitively priced, small companies will use digital forensics consultancies in cases where computer misuse is suspected. Digital forensics in this sector is a volume business and the industry must respond.

If this potentially lucrative market sector is to be tapped, digital forensics must lose some of its mystery and operate at a level that small business people can understand. Digital forensic services must be marketed as essential and basic business needs at a price conducive to the pockets of small companies. Every employer needs peace of mind, regardless of the number of staff employed. A forensic check for computer misuse should be carried out regularly by all

Access to digital forensics via a management consultancy can be extremely expensive, often rendering it prohibitive to small and medium sized companies.



companies and not just when abuse is suspected. After all, the best way to approach this type of misconduct is to prevent it or at least catch it early. Regular health checks at the doctor or dentist are accepted as necessary, so why not a regular sweep by a digital forensic professional? Even the deterrence value alone may prevent transgression.

More graduates

The number of digital forensics graduates from universities has increased drastically over the last few years. This should have made the supply of digital forensic services to all sectors of the business market easier to access.

Recession and the lack of work arising from law enforcement contracts has been blamed for the relative stagnation currently experienced by many small digital forensics consultancies. The truth may simply be that, as digital forensics professionals, we are not moving with the new demands of the market place. Large practices are not best structured to deal with volume investigations, each of small duration. Small practices are.

Trust relationships must be built with the local business community in order that they may begin to understand the essential nature of digital forensics to their business

operations. In the same way as accounts are audited periodically, why aren't IT systems forensically checked to ensure that there are no issues?

If trust is established, the digital forensics professional can be seen as the independent ally of the small business person, the third party check and balance that gives peace of mind to entrepreneurs who have many other commercial worries without worrying constantly about how their IT is used.

After all, company directors will become liable for any illegal activity perpetrated on the company's site using company assets, such as software piracy or theft of intellectual property, should they fail to take reasonable preventative precautions. It certainly could be argued that regular checks for computer misuse, whilst never comprehensive or infallible, show some attempt to take reasonable precautions.

The issue may be that there are not enough entrepreneurial digital forensics professionals who are willing to look into providing services to the small business sector. While this situation prevails, small businesses will continue to be easy prey for the abuse of company IT.

For more articles go online to:
www.bcs.org/articles



BLOCK CRIMINAL CLOUDS

Cloud computing is the latest IT buzz word, and for good reason, as it provides businesses with highly flexible, low cost computing. However, according to Ben Ward MBCS, criminal gangs have also spotted its potential.

There are many different ways a criminal can steal your valuable data. The most common vectors are via malware installed on your machine, brute force password attacks or intercepting data in transit. The cloud concept assists in all of these paths of attack, and enables a much more efficient (and reliable) method of distributing workload.

The term cloud applies not only to 'friendly' services such as Amazon's EC2, but also to botnets, created by networks of

infected machines under the control of criminal gangs. These networks of 'zombie' machines can be every bit as sophisticated as standard cloud offerings, and the vast scale of these networks (reaching hundreds of thousands of hosts in some examples) means that a huge amount of distributed computing power is available for the right price.

Compromised services

Malware vectors, such as the infamous

Salinity virus, store a local copy of URLs from which to download payload executables and updated URL lists. Once a 'live' URL has been located, the malware will download the files and then pass stolen data back to the control centre. These URLs are provided by the ever changing botnet that has been created by the criminal gang behind the malware.

Usually in this case, if the local list of URLs doesn't contain a 'live' link, then the malware is unable to send back sensitive

data. This is where cloud computing comes in. In a recent case, the Zeus bank-detail-stealing Trojan managed to infect a vulnerable account on Amazon's EC2 service. While it had control of this, it operated as a back-up to the URL list, enabling infected machines to pass all of their data back to the criminal gang through Amazon's cloud infrastructure.

What about the use of cloud services to distribute malware? This is a strong possibility, and there are already signs that this is occurring. It isn't just the generally accessible cloud that is affected, but social networking sites such as Twitter, Facebook and MySpace have also been compromised. The ability to create your own apps within these sites has created scenarios where malware can make call backs to applications based in the vast social network cloud.

Happy hacking

Another criminal application for the cloud is in the realm of data interception. For \$17, the 'WPA Cracker Service' markets itself as a way to quickly brute force WPA hashes, enabling subscribers to crack the encryption on wireless networks within 20 minutes, instead of the five plus days it would usually take. It does this by utilising a cloud-based cluster equivalent to over 400 CPUs.

A quick price check on Amazon's EC2 service shows that 400 instances of their 1 CPU (eCPU) option would cost just \$8 (£5) for one hour, a tiny price for what could be a very powerful weapon in the wrong hands. Marlin Spike, creator of the above tool-states: 'Security is moving into the cloud...so the attacks will follow security into the cloud as well. Password cracking is an obvious thing. Normally, it is cost-prohibitive to run CPU-intensive jobs. [With cloud computing] it costs a lot less money than doing it yourself.'

Sincerest form of flattery

Wily criminals have also been copying the business model of cloud-based technologies to maximise the profit out of their own botnets. One China based group has created an attack-as-a-service website, allowing customers to launch DDoS attacks against a target of their choice. Other 'companies' have used a subscription model, with the ability to rent your own botnet for as little as \$60 per day.

The distributed nature of these botnets means that a DDoS can be deadly and can render a company's internet presence unusable for as long as the attack continues. The aggregate bandwidth of all of these machines can also be astounding, with the largest reported DDoS attack coming in at a hefty 49GBPS, enough to take out even the largest sites globally.

The distributed nature of these botnets means that a DDoS can be deadly and can render a company's internet presence unusable for as long as the attack continues.



So in light of all of these new threats from cloud-based computing, is it time to panic and shut down all external facing services?

There are many ways to protect your business from cloud based attacks. Paradoxically, one of the best ways is to host your services within the cloud. The only way to truly beat a distributed threat is to make sure that your infrastructure is also distributed, and using cloud-based services is the cheapest and most effective way to do this. The 'safety-in-numbers' approach that can be offered by either a third party or a private cloud can really enable a business to keep nodes running when under attack.

Preventing malware infections is also another way to prevent your business from becoming part of a botnet. The tried and

tested process of ensuring that anti-virus and malware protection is up-to-date and that only authorised ports are open to the outside world is the best protection for your valuable computing resource.

Planning

As with all new technologies, criminals are amongst the earliest adopters of cloud computing. But with a little forethought, planning and best practice, the cloud need not be feared.

References:

www.securityweek.com/rise-small-botnet
www.technologyreview.com/web/24127/

For more articles go online to:
www.bcs.org/articles



BIOMETRIC REVOLUTION

Peter Craig, Chief Technical Officer at Delaney, debates the issue of biometric authentication and the importance of human factors when dealing with confidential and sensitive data.

To protect sensitive data, organisations need an authentication solution that is both easy to use and delivers an effective technical control against unauthorised access. Biometric authentication solutions appear to offer some easy answers to this challenge, but do they really work?

What's the problem with passwords?

Password authentication is a widely used method of identifying users on applications, databases and operating systems. It's quick to implement, easy-to-use and widely available. Gartner estimates that it costs around \$50 for each password-related call to the IT helpdesk, and 30-50 per cent of

calls relate to password issues. Not only is password authentication expensive to manage, it is often the weakest link in the security chain.

The easiest way to gain access to sensitive data is to trick the end-user into revealing their password. There are external threats from key-loggers, screen-capture software and other malware that can be introduced through known vulnerabilities or social engineering. There are real internal threats from written-down, guessable and shared passwords. The human factors are the most difficult to manage and pose the greatest threat to an organisation's data

security. Do passwords, even complex password, really offer adequate protection when the human factors are considered?

Which authentication solution is best?

The common alternatives to passwords include biometric (fingerprint, vein, iris), smartcard and token-based authentication solutions. Commonly organisations deploy these solutions as single-factor, dual-factor and multi-factor authentication solutions to offer greater degrees of protection.

Due to the ease of use and deployment, biometric authentication has traditionally had the lowest total cost of ownership. There are different qualities of biometric

The biometric myths make good movie scripts but are irrelevant in commercial situations.

The retail industry has widely deployed smartcards for EPOS system authentication for example. The introduction of PCI-DSS, encouraged retailers to reconsider the risks of smartcard sharing between staff as well as the risks of lost and stolen cards. SecuGen and DigitalPersona OEM fingerprint modules have been widely deployed in EPOS solutions such as Sharp and Toshiba to reduce these risks. Despite the convenience of smartcards; the risks of sharing, loss and theft of cards (and passwords/PINs in two-factor implementations) remain key obstacles, even as a two-factor authentication solution.

Multiple factor

Token solutions, such as RSA Secure-ID, are popular two-factor authentication mechanisms particularly for remote access. Tokens offer a good level of security via a randomly generated code on the hardware token together with a user PIN number. The risks of stolen and shared PINs and tokens are real. Users may not use the process regularly enough to remember their details, and they often use the service when the helpdesk is unavailable or for emergencies. They often write the PIN or password details down. In September 2010, DigitalPersona launched DP Pro 5.0 that offers a software token generator delivered via mobile smart-phones. The 'virtual PIN number' is generated by the fingerprint swipe process and cannot be lost, stolen or forgotten. It is potentially a strong challenger to the traditional dominance of token solutions for remote access, especially when packaged with whole-disk encryption.

Lastly, there are multi-factor authentication solutions such as Authasas's Advanced Authentication and M2SYS Hybrid solution. Authasas offers a complete range of token, smartcard and biometric authentication options to meet legacy and operational requirements. Acting as a central authentication server, and without expanding the Active Directory tree, it delivers secure single or dual-factor sign-on for Windows, Lotus Notes, SAP, Citrix, Oracle and SWIFT Payment Systems to name a few.

Does biometric authentication work?

The answer is certainly yes. The biometric myths, such as using dead body parts make good Hollywood movie scripts, but are largely irrelevant in commercial situations. A fingerprint becomes useless after about 10 minutes, with the iris quickly

clouding. Issues with ethnic minorities and children are already resolved by improvements in image resolution quality. In fact, children using library system and cashless catering solutions are some of the biggest users in the UK. The fingerprint template is encrypted in certified solutions. If it were possible to replay the template submission, certified commercial biometric solutions automatically implement anti-spoofing countermeasures to prevent this. Additionally, it is not possible to steal and reuse the biometric information from commercial systems, as the fingerprint template stores only a small percentage of the actual fingerprint. Non-commercial systems such as US-VISIT store complete biometric information, but their purpose is different from commercial authentication solutions.

Reducing risk

All multi-factor authentication mechanisms offer improved security over passwords, however, modern biometric authentication works best at reducing the human risks such as loss, theft and sharing of passwords the most. With independent certification, solutions are available to meet the requirements of ISO27001 and PCI-DSS. Fingerprint authentication and iris authentication have anti-spoofing measures that operate effectively as part of a package of multi-factor authentication. Vein readers offer a level of single-factor authentication security that is beyond the security requirements of sensitive data protection.

The only downside is that vein reader hardware is currently priced around £260, around three to four times the cost of a fingerprint reader. With the current challenges of cost reduction,

IT managers with a long term view on security and cost management should look at the reduced help desk calls for password management as a result of biometric solutions.

The operational savings estimated at around \$50 or £35 per helpdesk password related call would typically cover the reasonable hardware costs in around 12-18 months. The medium term case for biometric security is getting stronger, and the worldwide market is growing at 20 per cent per annum. Secure, easy to use and affordable biometric authentication may finally be within sight of the average organisation.

For more articles go online to:
www.bcs.org/articles

security authentication from fingerprint readers, iris scanners and vein readers. Fingerprint solutions offer simple single factor solution, and certified solutions offer protection equivalent to smartcard or token in two-factor authentication deployments. Iris and face recognition software tend to have more specialist applications. Vein readers are increasingly popular and easy to deploy and use. They are more secure than fingerprint readers, as it's not as easy to replicate the vein data. Such is the new-found confidence in vein authentication that Poland's Bank BPS SA deployed Hitachi vein-readers as an alternative to PINs on its ATM machines under trial from May 2010.

Smartcards are often a convenient and easy to use authentication mechanism.



DATA SHARING AND THE DPA

Charlotte Walker-Osborn and Jennifer Liddicoat, Technology Group, Eversheds LLP, look at recent data protection updates and cases.

The Information Commissioner's Office (ICO) has launched a consultation on a new data-sharing code of practice, which aims to clear up how organisations should best handle data-sharing within the framework of the Data Protection Act (DPA). The closing date for responses is 5 January 2011. After that, a paper summarising the responses will be published by the ICO.

The code covers a number of areas, including:

- what factors an organisation must take into account when coming to a decision about whether to share personal data;
- the point at which individuals should be told about their data being shared;
- the security and staff training measures that must be put in place;
- the rights of the individual to access their personal data; and
- when it is not acceptable to share personal data.

The ICO aim to set out a model of good practice for public, private and third-sector organisations, and cover systematic, routine data-sharing where the same datasets are shared between the same organisations for an established purpose, as well as one-off instances where a decision is made to release data to a third party. Some efforts have also been made to

compel updates to the law and reflect best market practice.

For example, the EU Model Clauses were updated earlier this year.

Hopefully, this consultation will go some way to helping businesses deal with data protection, but the draft code does not help explain some key areas of confusion that businesses grapple with.

For example, currently private sector organisations, in particular, often find it difficult to determine whether the specific act of sharing they are contemplating is covered by one of the conditions set out in the DPA and the draft code does little to flag this up. The ICO constantly appears to take a 'reactive' stance to market conditions when, instead, perhaps what is needed is a wholesale update of the law in this area. The challenge facing the ICO will be making any new law sufficiently clear, workable and flexible.

An interesting example of the importance of this area can be found in a recent Swiss case. A Swiss federal court has ruled that Logistep's use of file sharing monitor software to identify IP addresses violates data protection laws. Logistep was using the software to locate the IP addresses of copyright infringers who were illegally downloading music and passing them on to the copyright owners so that they could prosecute.

The court ruled that IP addresses come within the definition of 'personal data' under Swiss data protection laws and processing that data without the knowledge or permission of the person concerned was illegal.

Switzerland is not subject to EU rules on data protection, including the Data Protection Directive. Could this result be replicated in EU countries? The position is the subject of heated debate; the rationale in this particular instance being 'Why should file sharers be able to evade detection due to legal loopholes?'

Of course, there are policy reasons why an indiscriminate approach cannot be taken, but some countries have addressed this issue directly.

France's data protection regulator, CNIL, is reported to have authorised four collective societies to collect IP data, which will later be used in the application of the three strikes (HADOPI) law. But this was not without considerable initial resistance from CNIL (and a sharp rebuke of CNIL from France's highest court, the Conseil d'Etat).

The EU's Working Party, which was established to act as an advisory body, has directed that, unless an internet service provider can say with absolute certainty that the user cannot be identified, it will, to be on the safe side, have to treat the IP address as personal data and therefore cannot share it without the infringer's consent. The key is that, even if the IP address cannot identify an individual by itself, there may be potential for the individual to be identified through other means.

The UK's regulator, the Office of the Information Commissioner, has provided guidance on personal profiling using dynamic and static IP addresses, but it's hard to see how this would apply in this situation. Given that successful prosecutions have been brought in the UK and Germany against file sharers, it is strange that this issue has not yet been tested.

There is a fine balance to be struck between protecting copyright holders' interest and the legality of infringing IP address collection methods. Organisations will need clear guidance on when it is and is not acceptable to share personal data. Logistep has opened the debate; it will be interesting to see how this plays out and whether it influences the approach of the ICO in its new consultation.

Please note that the information provided above is for general information purposes only and should not be relied upon as a detailed legal source.

www.bcs.org/legal

BOOK REVIEWS

Practical Lock Picking. A Physical Penetration Tester's Training Guide

Deviant Ollam

Syngress Media

ISBN: 978-1-59749-611-7

£24.95

9/10



It's often said that to the man with a hammer every problem looks like a nail. A chapter on bypassing locks and doors in a creative manner provides the extremely important function of getting the reader to consider all aspects of physical security, rather than immediately attempt picking the locks when carrying out a security

review.

Although the subject of lock-picking may not seem immediately relevant to the world of the IT professional, the practice has a long association with information security. Physical security assessments of IT departments and server rooms involve assessing both the type and the quality of locks used.

The book begins with an excellent 'ethics test', which would not go amiss in other hacking books, serving as a good reminder of how to make correct usage of information provided by the book.

We then move on to the fundamentals needed for an understanding of how common lock types are manufactured and how they work in practice. The remainder of the book builds upon this foundation.

The clear explanations and plentiful diagrams leave the reader with a clear idea of how lock mechanisms work, and the practice exercises that follow build on this knowledge to allow the reader to quickly progress before moving on to the simpler techniques, shimmying and bumping.

We cover the old favourites, such as triggering a motion sensor by pushing devices under the door, along with the effective, often missed, possibility of passing wire hooks through gaps to operate catches.

Overall the book does much to dispel the myth that lock-picking is an arcane, difficult art and puts the reader in a position to carry out more effective physical security reviews, although it would have been nice to see more detail on how to carry out physical security reviews for locking mechanisms and how to select appropriate mechanisms to secure a facility.

In summary this is an excellent practical introduction to the subject and the publishers are to be congratulated for producing another good niche penetration testing book.

Vick Dunn

IT Security Metrics: A Practical Framework for Measuring Security & Protecting Data

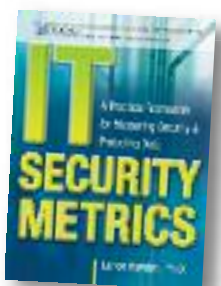
Lance Hayden

McGraw Hill

ISBN: 978-0-071713-40-5

£37.99

4/10



of ideas too familiar to a (security) reader.

Not too often do I come across a book as verbose as this: page after page, there is text (and, I am afraid, jumping from one idea to another) and more text. This makes it difficult to follow even a simple idea. This is a classic example of a book where illustrations could have helped (along with relevant editorial support).

If I had to choose one chapter to recommend, I would choose chapter 8, as the author delves into interesting detail about security compliance and auditing standards. This is good as it acknowledges existing initiatives to tackle some of the problems mentioned in this book.

I would not recommend this book to the wider (security) readership. Those new to the concept of security metrics may find parts of it a good introduction to some of the underlying motives for such efforts.

Siraj A. Shaikh MBCS CITP

Amongst the plethora of books published these days on security, there are a wide range of topics being tackled with often too much prescription and too little focus. This leaves one to wonder if much of this should simply be ignored and we should focus on basics; however, some of it is too good to be let by.

I have a similar dilemma with this book. The author presents an extensive treatment of security metrics, starting from the context, then basic definitions and then on to case studies and some valuable practical advice. Much of this, however, is not new and the first part (first three chapters) does not serve to motivate as it discusses a set

BOOK OF THE MONTH

Managing Information Security

J. Vacca

Syngress Media

ISBN 978-1-597-49533-2

£30.99

9/10



This book covers the complex and huge area of information security and includes information that practitioners and IT managers can use in strategy formation, management and day-to-day operation of their information security management systems.

The book begins with raising the reader's knowledge of security essentials such as impact of security breaches, types of breaches and the various elements of the fundamentals of an information security management system and the contents thereof.

Procedures

Elements of procedures and policies, information risk management, contingency planning, physical and data security are covered in brief. The book quickly gets more informative and interesting for the technical reader and gives clear explanation and examples, which enable the reader to go further in the particular areas of ID management, intrusion detection and prevention systems, computer forensics, network forensics, firewalls, penetration and vulnerability assessment.

In some areas the book is not a 'light' read, and readers would be expected to have general networking knowledge. However the individual chapters themselves are primers for each subject and references for further reading are given with every chapter so that areas can be followed up. Both non-technical and technical readers are therefore catered for.

Overall this is an excellent primer to the complexities of information security and is an ideal read for anyone involved in or about to manage an organisation's information security functions or information security management system.

Georgette Banham FBCS CITP



IT'S NOT JUST ABOUT LOCKS

Recently the Americans lost communication with around 70 of their nuclear tipped missiles for some 50 minutes and Russia has previously taken Estonia off-line, but John Mitchell is more concerned about a text to his mobile and a Ghanaian email address.

I know that I should be more concerned with the two previous threats, but the text informing me I'd won lots of money was closer to home. The email address looked decidedly dodgy and when I checked the sender's number it was from Ghana.

The interesting thing about these scams is that they rely on three common things to succeed: greed, gullibility and technology.

It is the last one that enables the scammers to operate remotely, hit large potential audiences and put forward any persona that they believe will tempt you. Whereas you may have concerns about the integrity of person in a far off land carrying a Kalashnikov, these may be somewhat allayed if you see a photograph of a person in a smart suit sitting in an office.

Even respectable businesses are not adverse to using a little technology to steal our electronic assets, as was revealed when Google reluctantly owned up that its Street View cars were, inadvertently,

collecting details of Wi-Fi networks as they cruised by. Now whatever the intent, the fact that we can be robbed remotely means that we have to think wider than the locks on our doors.

I recently advised a client who was based in a shared tenancy building that he couldn't rely on door locks as the outsourced cleaning company had free access to the building overnight. So on top of the logical security we built a CCTV recording system with motion sensors and off-site transmission of any triggered recordings and SMS alerts. It didn't cost a bundle, although the warning signs and legal advice were almost the biggest budget items.

When the system was operational, the chief security officer had a few busy and heart-stopping days while the system was bedding-in and he watched the cleaners systematically opening any unlocked cupboard or drawer.

Curiosity killed the proverbial cat and it certainly killed the cleaning contract when he drew this to the attention of his CEO. Despite the lawyers saying that evidence collected covertly was likely to be inadmissible in court, the CEO was not intimidated and the contract was cancelled. So although electronic threats should not be ignored we need to remember that our secrets may be just as vulnerable from a physical threat.

Security in depth is what I desire when I am asked to provide assurance that things are OK, but as we all know a chain is only as strong as its weakest link. I have a pseudo-mathematical technique for measuring control effectiveness, which although not perfect, does remove some of the judgemental errors in reaching a conclusion.

On balance I find that most control systems are based on trust and optimism, rather than hard-nosed pragmatism. The trust mechanism is usually there out of an unwillingness to face the reality that if you take trust out of the equation, then most control processes are pretty useless. I rely on my security officer colleagues to identify the current and future threats and to suggest appropriate controls. I then sit down with them to evaluate the effectiveness of the proposed controls. Will this control manage the likelihood or the consequence? Is it preventive or detective?

They often retort that, as the likelihood of a particular threat crystallising is low, it doesn't matter too much if the control is weak. I answer that they may not as yet have suffered a heart attack, but it would be useful if they could detect the symptoms early enough to get to the hospital before a full cardiac arrest took place. So we kick the thing around a bit and find that, even with our best intentions, the residual risk remains stuck in the 'amber' zone. But that is life. Not everything is 'green'. Even more so now that the threats and controls may no longer be under our direct control. Outsourcing and cloud computing, reliance on third-party security statements and lack of understanding mean that we are more vulnerable than ever to changes in the use of technology.

Providing that managers are aware of and are willing to tolerate a risk at a particular level, then my job is done. Despite that, it is still the people risk that fascinates me. I have never known a computer to attack me of its own accord. Even those 70 million zombie hosts that are waiting out there still need a human hand to direct their attack.

For additional articles please visit:
www.bcs.org/articles

Securing your information with LRQA

Choosing certification of your information security management system to the international standard, ISO 27001 shows that you're prepared to open up your systems to external scrutiny.

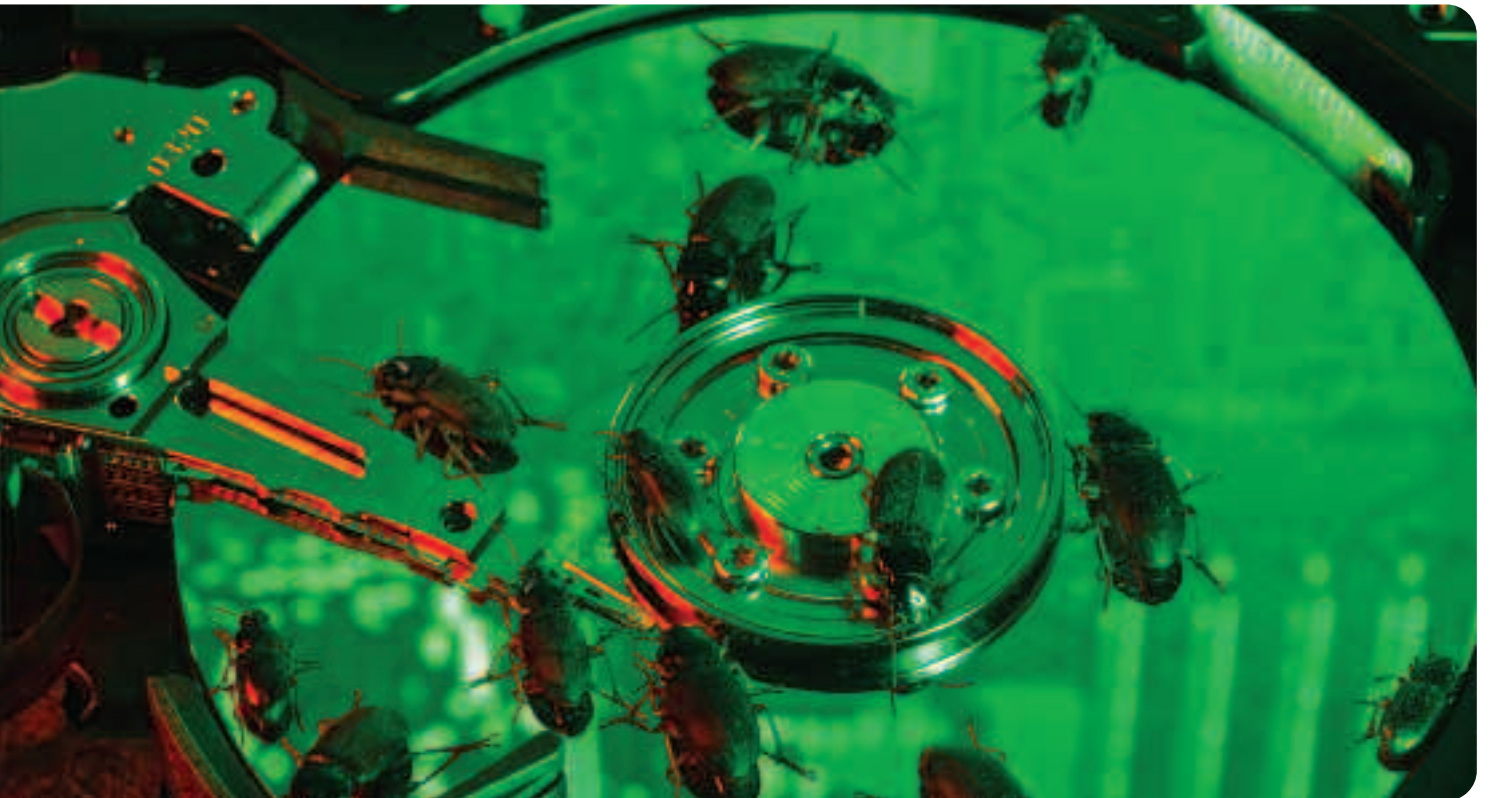
Importantly, certification gives you – and your customers, trading partners and other key stakeholders – the confidence that you have addressed all security risks including IT, people, physical and business continuity.

As a leading certification body, LRQA has the knowledge and expertise to help you meet your information security objectives. With training, gap analysis and certification, our information security experts will help you drive improvement through your management systems.

Choosing LRQA means you'll be working with one of the world's most trusted and respected management system bodies providing you with business assurance.

LRQA Business Assurance

Improving performance, reducing risk



Sales
0800 783 2179
enquiries@lrqa.co.uk
www.lrqa.co.uk

Training
0800 328 6543
lrqatraining@lrqa.com



Services are provided by LRQA and other members of the Lloyd's Register Group.
For further details please visit www.lr.org/entities





The Open University

“ Develop your IT workforce without disrupting the working day ”

Our professional development programmes can give your organisation a competitive edge and your employees the relevant practical, technical and managerial expertise they need to work in today's constantly changing global IT & Telecoms environment.

Solutions range from IT professional practice, enterprise software development, information security management, systems integration, computer forensics and project management, to awards in IT business and management including our triple accredited MBA.

Your employees can study outside of working hours using the latest learning technologies alongside ongoing support from us and what they learn one day can be applied the next.

Did you know?

- Our specialist programmes are developed by experts in association with professional bodies, sector skills councils, IT vendors and IT & Telecoms employers
- We're the largest and fastest growing Cisco Academy in the UK and among the top 5 universities for computer science
- Our triple accredited business school is in the world's top 1%.



CYBER SECURITY CHALLENGE.ORG.UK



Develop your workforce

- ▶ www.openuniversity.co.uk/it
- ▶ corporate-enquiries@open.ac.uk
- ▶ 0845 758 5097 Quote: ZAMAAC

INSPIRING LEARNING