

Featured this issue: Smart security

The rapid consumer adoption of smart devices is driving smartphones and tablets into the enterprise. Yet enterprises are often ill-prepared to secure smart device access to their networks and are having to act fast to support the demand from employees to be able to use such devices.

Tracey Caldwell looks at the benefits and issues surrounding smart device access to the enterprise network. This article looks at a number of implementations of secure smart-device access to enterprise networks and reports on expert and analyst views on the issues facing network managers.

Full story on page 5...

Why mobile two-factor authentication makes sense

Computer security must always tread the fine line between efficacy and usability, but regular two-factor authentication (2FA) using physical tokens crosses this line. Users need to remember their token, while technical services departments are charged with the job of maintaining and administering each token.

This is the overwhelming reason why 2FA has failed to catch on. However, new ways of implementing 2FA have

been developed – the most popular being passcode delivery directly to each user's own mobile phone via SMS. Although computer security measures need to constantly adapt to each new threat, Andy Kemshall of SecurEnvoy argues that tokenless 2FA represents a new way forward for organisations that are looking for the added layer of security offered by 2FA in 2011.

Full story on page 9...

Cracking GSM

The GSM standard is about to reach its 30th anniversary. But although it uses encryption to protect the integrity of the data transmissions – voice calls or data – the technology has been shown to have some serious vulnerabilities.

Many of these stem from the fact that the mobile device must authenticate itself to the network over the air. This is achieved through a combination of the

International Mobile Subscriber Identity (IMSI) – the unique electronic serial number of the SIM card inserted into the phone – and the International Mobile Equipment Identity (IMEI), which is a unique serial number of the mobile. But recent research has shown how these can be intercepted and spoofed. Steve Gold investigates GSM's weak spots.

Full story on page 12...

RSA hack leaves status of SecurID uncertain

Security firm RSA, a division of EMC, has admitted that it has been the victim of a successful cyber-attack. It is being cautious about revealing details

of the breach, but in an open letter to customers, published on its website, said that some of the information that

Continued on page 2...

Contents

NEWS

RSA hack leaves status of SecurID uncertain	1
Few aware of smartphone vulnerability	2
Utilities still under threat	20

FEATURES

Smart security	5
The popularity of smartphones and tablet devices means they are showing up in the workplace. But companies are often ill-prepared to cope with them. Tracey Caldwell looks at both the benefits and issues surrounding smart-device access to the enterprise network, and reports on expert and analyst views on the issues facing network managers.	

Why mobile two-factor authentication makes sense	9
---	---

Two-factor authentication (2FA) has struggled to catch on, largely because of the inconvenience of having to carry physical tokens and the difficulty of managing them. But Andy Kemshall of SecurEnvoy argues that tokenless 2FA represents a new way forward for organisations that are looking for an added layer of security.

Cracking GSM	12
---------------------	----

While GSM uses encryption for voice and data transmissions, over the years it has still been found to be vulnerable. Many of the problems stem from the fact that handsets must authenticate themselves over the air. Recent research has shown how International Mobile Subscriber Identity (IMSI) and International Mobile Equipment Identity (IMEI) numbers can be intercepted and spoofed. Steve Gold investigates the problems.

Information security in the cloud	15
--	----

Organisations are avoiding cloud technology because of security concerns. But you can address these by initially moving to a hybrid cloud and then assessing which services you can move to the public cloud, says Richard Blandford of Fordway.

Learning to love SIEM	18
------------------------------	----

Security Information and Event Management (SIEM) is starting to play an ever-more-important role in securing organisations so that they can meet their regulatory compliance obligations, explains Steve Jenkins of Q1 Labs.

REGULARS

News in brief	3
Product News	4
Calendar	20

Editorial Office:

Elsevier Ltd
The Boulevard, Langford Lane, Kidlington,
Oxford, OX5 1GB, United Kingdom
Fax: +44 (0)1865 843973
Web: www.networksecuritynewsletter.com

Publisher: Greg ValeroE-mail: g.valero@elsevier.com**Editor:** Steve Mansfield-DevineE-mail: smd@contrarisk.com**Senior Editor:** Sarah Gordon**International Editorial Advisory Board:**

Dario Forte, Edward Amoroso, AT&T Bell Laboratories;
Fred Cohen, Fred Cohen & Associates; Jon David, The
Fortress; Bill Hancock, Exodus Communications; Ken Lindup,
Consultant at Cylink; Dennis Longley, Queensland University
of Technology; Tim Myers, Novell; Tom Mulhall; Padget
Petterson, Martin Marietta; Eugene Schultz, Hightower;
Eugene Spafford, Purdue University; Winn Schwartz, InterPact

Production Support Manager: Lin LucasE-mail: l.lucas@elsevier.com**Subscription Information**

An annual subscription to Network Security includes 12
issues and online access for up to 5 users.

Prices:

€1112 for all European countries & Iran
US\$1244 for all countries except Europe and Japan
¥147 525 for Japan

(Prices valid until 31 December 2011)

To subscribe send payment to the address above.

Tel: +44 (0)1865 843687/Fax: +44 (0)1865 834971

Email: commsales@elsevier.com,or via www.networksecuritynewsletter.com

Subscriptions run for 12 months, from the date payment is
received. Periodicals postage is paid at Rahway, NJ 07065,
USA. Postmaster send all USA address corrections to: Network
Security, 365 Blair Road, Avenel, NJ 07001, USA

Permissions may be sought directly from Elsevier Global Rights
Department, PO Box 800, Oxford OX5 1DX, UK; phone: +44 1865
843830, fax: +44 1865 853333, email: permissions@elsevier.com. You
may also contact Global Rights directly through Elsevier's home page
(www.elsevier.com), selecting first 'Support & contact', then 'Copyright
& permission'. In the USA, users may clear permissions and make
payments through the Copyright Clearance Center, Inc., 222 Rosewood
Drive, Danvers, MA 01923, USA; phone: +1 978 750 8400, fax: +1 978
750 4744, and in the UK through the Copyright Licensing Agency Rapid
Clearance Service (CLARCS), 90 Tottenham Court Road, London W1P
0LP, UK; tel: +44 (0)20 7631 5555; fax: +44 (0)20 7631 5500. Other
countries may have a local reprographic rights agency for payments.

Derivative Works

Subscribers may reproduce tables of contents or prepare lists of arti-
cles including abstracts for internal circulation within their institutions.
Permission of the Publisher is required for resale or distribution outside
the institution. Permission of the Publisher is required for all other
derivative works, including compilations and translations.

Electronic Storage or Usage

Permission of the Publisher is required to store or use electronically
any material contained in this journal, including any article or part of
an article. Except as outlined above, no part of this publication may
be reproduced, stored in a retrieval system or transmitted in any form
or by any means, electronic, mechanical, photocopying, recording or
otherwise, without prior written permission of the Publisher. Address
permissions requests to: Elsevier Science Global Rights Department, at
the mail, fax and email addresses noted above.

Notice

No responsibility is assumed by the Publisher for any injury and/or dam-
age to persons or property as a matter of products liability, negligence
or otherwise, or from any use or operation of any methods, products,
instructions or ideas contained in the material herein. Because of
rapid advances in the medical sciences, in particular, independent
verification of diagnoses and drug dosages should be made. Although
all advertising material is expected to conform to ethical (medical)
standards, inclusion in this publication does not constitute a guarantee
or endorsement of the quality or value of such product or of the claims
made of it by its manufacturer.

Pre-press/Printed by
Mayfield Press (Oxford) Limited

...Continued from front page
**was stolen "is specifically related to
RSA's SecurID two-factor authentica-
tion products".**

SecurID is widely used by government
and corporate customers to produce
one-time passwords. Around 40 million
accounts are secured with the system.
But the company hasn't said whether
the security of SecurID has been under-
mined by the hack. For many of the
company's customers, this leaves them
in the situation of having to assume that
their security is compromised.

A later statement by the company
said: "Our investigation to date has
revealed that the attack resulted in cer-
tain information being extracted from
RSA's systems. Even with this informa-
tion being extracted, RSA SecurID
technology continues to be an effective
authentication solution for customers."

However, some commentators have
noted that the term 'two-factor' is notable
by its absence from that statement. RSA
sent an advisory to its customers suggest-
ing they strengthen the personal identifi-
cation numbers used alongside passwords
and the SecurID-generated one-time pass-
words. This suggests that RSA considers
the authentication provided by SecurID
to have been seriously weakened.

The company did later release some
details of how the attack was mounted.
The attacker probably carried out recon-
naissance via social networking sites before
targeting RSA employees with phishing
attacks. In a blog post, Uri Rivner, head of
new technologies, identity protection and
verification at RSA, wrote:

"The attacker in this case sent two dif-
ferent phishing emails over a two-day
period. The two emails were sent to two
small groups of employees ... The email
subject line read '2011 Recruitment Plan'.

"The email was crafted well enough
to trick one of the employees to retrieve
it from their junk mail folder, and open
the attached Excel file. It was a spread-
sheet titled '2011 Recruitment plan.xls'.

"The spreadsheet contained a zero-
day exploit that installs a backdoor
through an Adobe Flash vulnerability
(CVE-2011-0609)."

This led to the installation of the
Poison Ivy Trojan. The attack used priv-

ilege escalation techniques to gain access
to staging servers at key points, from
which the attacker used FTP to transfer
password-protected RAR files. But RSA
still isn't saying what was in these files,
which is making it difficult for SecurID
customers to plan mitigation strategies.
However, security testing firms NSS
Labs had some advice:

"NSS Labs recommends that RSA
clients who use SecureID to protect
sensitive information should consider
eliminating remote access until this
is resolved; perform an impact assess-
ment of systems using this technology
and identify critical assets and potential
risks. Furthermore, RSA clients should
consider alternative two-factor authenti-
cation solutions."

The RSA open letter to customers
is here: <http://www.rsa.com/node.aspx?id=3872>

Few aware of smartphone vulnerability

**Two recent reports have highlighted
the vulnerability of smartphones
while another shows that few people
are aware of the dangers.**

In the US, the Ponemon Institute, on
behalf of AVG, surveyed 734 adult smart-
phone owners. Among its findings were
that 84% of them use the same device for
both business and personal activities. This
means that sensitive data is being carried
around beyond the reach of corporate
security measures. Some 66% of users
keep personal data on their smartphones.
And while two-thirds worry about being
targeted by advertising, less than half
(44%) worry about being infected by
malware while browsing.

More than a third of smartphone
owners make online payments via their
devices, though only 14% use them
for banking. Less than half use keypad
locks or passwords to secure the devices
and only 29% have considered install-
ing anti-malware. But 42% are happy
for applications such as Facebook to
access their keychains or passwords.
Only a tenth of users disable the 'dis-
coverable' setting on their devices.

Continued on page 20...

In brief

DNSSEC finally on .com

The last, and biggest, of the major Top Level Domains (TLDs), .com, is finally supporting the DNSSEC security protocol. VeriSign, which operates the .com TLD, has just signed up to make the technology available to its 80 million registered domains. Although this is a milestone in the adoption of DNSSEC, which has been around for more than a decade, it only makes the system available: the next big hurdle will be getting people to actually use it. A survey of security professionals by Internet Identity (IID) found that half either hadn't heard of DNSSEC or had no idea how it worked. And an earlier survey by Forrester, last summer, found only 11% of firms implementing it to some degree.

Leaking firewalls

Testing firm NSS Labs has issued a new report on firewalls, covering products from Check Point, Cisco, Fortinet, Juniper, Palo Alto and SonicWall. It found that five of the six products allowed external attackers to bypass the firewall and become an internal 'trusted' machine. Three of them failed to remain operational when subjected to stability tests, even though they are all ICSA Labs and/or Common Criteria certified. And the NSS Labs report concludes that claimed performance, based on RFC-2544 (UDP), is not an accurate measure of how they measure up in real-world environments. More information at: <<http://www.nsslabs.com/research/network-security/firewall-ngfw/>>.

Barracuda hacked

Security firm Barracuda Networks has suffered its own breach. A hacker calling himself 'Fdf' claims to have broken into the company's databases via a SQL injection attack, gaining access to employee details – including email addresses and passwords hashed using MD5 – sales leads and other information. Some details of the hack, including screenshots and a list of database tables were posted to a Tumblr blog (hmsec.tumblr.com).

Email malware soars after Rustock takedown

Following the beheading of the Rustock botnet by Microsoft, email-borne malware has increased by 400%, claims security firm CommTouch. The sudden increase happened in the last week of March, two weeks after spam levels dropped by 30% – from 168 billion messages a day to 119 billion – as a result of Microsoft's action. The most prevalent methods of attempting to spread malware, witnessed by CommTouch in the first three months of this year were: 'parcel tracking information' scams, in which victims are told that UPS or DHL is attempting to deliver something to them; Facebook chat messages from compromised accounts, which lead to phony pages and then to malware;

PDF files with embedded malware scripts; the Kama Sutra virus spread via a supposedly pornographic PowerPoint presentation; and the abuse of T-Mobile's personal homepage feature. During the quarter, around 258,000 zombies were activated each day, a drop from 288,000 in Q4 2010 and 339,000 in Q3 2010.

Mass attack claims few victims

A large-scale attack on thousands of computers seems to have had little effect. Dubbed 'Lizamoon', because the website infections attempt to redirect victims to fake AV software site lizamoon.com (as well as 27 other domains), the attack seems to have compromised as many as 4 million web pages, according to Websense. However, researchers believe that only a small number of people actually followed the links. The domains used for hosting the malicious software were quickly shut down and most of the compromised sites had low levels of traffic. The attacks used SQL injection to compromise the sites, but SpiderLabs believes this is an example of a blended attack in which the goal was to exploit Cross-Site Scripting (XSS) vulnerabilities.

IPv6 take-up still slow

Although IPv4 addresses are running out, the adoption of IPv6 is still proceeding at a snail's pace. This is according to EURid, the Top Level Domain (TLD) registrar for .eu. The problem, according to Marc van Wesemael, general manager for EURid, is that too few service providers have IPv6 solutions commercially available. This is in spite of .eu registration systems having been IPv6-enabled since the TLD was launched in 2006. Van Wesemael expects the pace to pick up by the time World IPv6 Day rolls around in June.

USPS falls for Blackhole attack

The US Postal Service (USPS) is one of the latest victims of what is proving to be among the most popular malware toolkits – Blackhole. The toolkit, which sells for \$1,000-\$1,500 on the black market, allows point-and-click creation of a website infection attack. It exploits injection techniques (mainly SQL injection) to place iframes and obfuscated Javascript on target sites in order to deliver a variety of malware. USPS had to take down its Rapid Information Bulletin System, which provides services such as parcel tracking and logistics.

Criminals increase malware production

According to Panda Labs, cyber-criminals appear to be increasing the volume of malware they're producing in an attempt to overwhelm organisations' defences. The first quarter of 2011 saw 73,000 new strains of malware created each day, an increase of 10,000 compared with the same period in 2010. Trojans formed the bulk of this

malware (70%), followed by viruses (17%) and worms (8%). Other forms of malware, including once-popular threats such as adware, have fallen away to trivial levels. The malware is most successful at infecting machines in China, Thailand and Taiwan, according to Panda's on-demand virus scanning, with infection levels reaching 70% in some places. Panda's full report is available here: <<http://press.pandasecurity.com/press-room/reports>>.

IBM opens new European security initiative

The European IBM Institute for Advanced Security, based in Brussels, is a new initiative designed to help companies and academics better understand cyber-threats and how to deal with them. It hopes to provide a link between public and private sector organisations in addition to providing better access to IBM's own research, services, products and experts. More details here: <<http://www.instituteforadvanced-security.com/>>.

EU under attack

The day before a European Union (EU) summit on economic strategies and the conflict in Libya, officials announced that the European Commission (EC) and External Action Service had been hit by a serious cyber-attack. Microsoft Exchange servers were among the machines targeted, which led to the EC suspending external access to email and its intranet as well as resetting passwords for all EC staff. There are suggestions that the attacks had been underway for months before they were detected. There were also unsubstantiated rumours that infected images were involved in the breach. As usual, some commentators hinted at state-sponsored attacks from China – as with the attacks that preceded the Paris G20 summit – although there's no firm evidence available. Shortly after the EC attacks came to light, the European Parliament detected compromises of its systems and had to suspend web-mail services. The Parliament network is separate from the EC one, but there are strong suggestions that the two attacks were co-ordinated.

Wifi hacking no crime for Dutch

Wardriving or hacking into other people's wifi connections is not a crime in the Netherlands, a court there has ruled. Providing the freeloader does not attempt to enter any other computers using the wifi connection, this activity does not contravene the country's anti-hacking laws, which date back to the early 1990s. These laws were designed to protect machines that are used for the "storage, processing and transmission of data" – and a router does none of these things. However, people or organisations whose wifi connections are being leached in this way still have recourse to the civil courts.

Products

BOOK REVIEW

Security for Microsoft Windows Systems Administrators

Derrick Rountree. Published by Syngress (ISBN: 9781597495943, e-ISBN: 9781597495950). Price: €25.95/\$34.95/£21.99, 204pgs.

Anyone faced with securing Windows systems for the first time would do well to make this book their first port of call. It's a well-balanced overview of all the facets of Windows system management that need to be addressed from a security perspective.

In fact, it's a useful book for anyone, working on any platform, who needs to understand where security issues reside within corporate systems. That's because, although it is focused on Windows, and all the practical examples, screenshots and step-by-step instructions relate to that platform, the author also devotes considerable portions of the book to the conceptual groundwork.

The chapters provide overviews of the key issues and technologies, including security standards, cryptography, network security, system security, organisational and operational security (including subjects such as risk analysis and disaster recovery) and security assessments and auditing.

In a book of around 200pgs – and where many of those pages are taken up with very handy screenshots – it's clear that none of this is going to be in very great depth. Seasoned security professionals will find the introductory nature of much of the material to be too general. But IT practitioners who need to get to grips with security issues will find the book a valuable briefing on the most pressing issues, along with a great deal of practical, hands-on advice on how you go about putting the principles into action in a Windows environment.

The book has a distinct bias towards networking security – you'll look in vain, for example, for any detailed advice on using features such as BitLocker and AppLocker. And most readers are going to find themselves doing additional research when they need to cope with the finer details of Windows security – or have to deal with unforeseen issues. Nevertheless, this book gives you a kind of 'to do' list of features and functions that need to be addressed.

BOOK REVIEW

Microsoft Windows 7 Administrator's Reference

Jorge Orchilles. Published by Syngress (ISBN: 9781597495615, e-ISBN: 9781597495622). Price: €28.95/\$39.95/£24.99, 636pgs.

This is a useful companion volume to *Security for Microsoft Windows Systems Administrators*

(above). Its more general nature is reflected in both the size and scope of the book. But, like the Rountree volume, it is arguably of greatest benefit to those IT professionals who need to get up to speed with managing Windows systems (or, given its focus on Windows 7 specifically, who need to update their skills for the new platform).

The book's subtitle – 'Upgrading, Deploying, Managing and Securing Windows 7' – shows that there's something specifically for security professionals in here, too. The security section is just under 100 pages long and delves into a few subjects – such as AppLocker and BitLocker – not covered by Rountree. There is less high-level material here, too: the book is very much about the practicalities.

Security often hinges on skilful system management and so following the guidelines in this book – even some, such as remote desktop management, that don't appear to have immediate security implications – will help create an environment with fewer weak points. And there are subjects outside of the security chapter – such as security settings within the management tools and the troubleshooting section – that most certainly do have a security angle.

Taken together, this book and the Rountree volume cover both the conceptual and practical levels of running Windows systems securely.

NEWS IN BRIEF

Credant Manager for BitLocker

BitLocker is a key security feature of Windows Vista and Windows 7, but is often under-used because of the complexity of managing it in a corporate environment. Credant Manager for BitLocker, part of Credant Enterprise Server 7.1.1, attempts to address this issue. It provides: centralised key management; reporting and auditing functions; Federal Information Processing Standard (FIPS) compliance through secure recovery of keys; automated Trusted Platform Module (TPM) initialisation and management; simplified policy creation and enforcement through the management console; and integration of BitLocker management with encryption management for Windows, Mac, removable media and smartphones. Credant claims the solution reduces the workload of managing BitLocker, addresses some of the security concerns associated with the storage of the BitLocker recovery keys in active directory, and improves auditing and compliance reporting.

Go to: <<http://www.credant.com>>.

Secunia has more VIM

Secunia has enhanced its Vulnerability Intelligence Manager (VIM) product. Among the improvements in VIM 3.1 is a revised reporting functionality that has been rebuilt into a modular structure, allowing for greater

customisation of reports. There's also a report configuration wizard, giving the option of including tickets or advisories within customised reports. VIM is compliant with the vulnerability database requirements defined by the NIST Interagency Report 7511 Revision 1 (Draft) and the Security Content Automation Protocol (SCAP) Version 1.0 Validation Program Test Requirements (Draft), April 2009. It also includes support for Common Platform Enumeration (CPE).

The new version also features additional portlets and new Common Vulnerability Scoring System (CVSS) options. You now have the ability to set custom environmental CVSS parameters for an asset list, save a custom CVSS score for any advisory, and receive a custom CVSS score for every relevant asset list in the advisory window, which the firm says are important for risk management and compliance purposes.

Go to: <<http://www.secunia.com>>.

Access rights solution from Protected-Networks

Access rights management specialist Protected-Networks has launched the latest version of its 8MAN solution in the UK. This is part of a general expansion into the UK market by this German company. The 8MAN 3.1 product allows IT managers to assign and manage access and usage privileges in enterprise-wide IT environments.

According to the firm, it provides easy access to the Active Directory structure in Microsoft environments and provides a simple overview of privileges in general, for individual directories or for groups of directories and of group compositions. There is also a visual display of duplicate privileges and the routes by which users have inherited these privileges. When assigning privileges, 8MAN is able to take into account existing workflows within the organisation. The company's internal organisational structure can be mapped and used as the basis for creating groups – eg, by location, department or cost centre. Domains, shares and directories can optionally be assigned to file owners, specialist departments or the helpdesk. Logging of all user and directory-related changes makes all changes fully traceable.

Go to: <<http://www.protected-networks.com>>.

Lifetime anti-virus from GFI

GFI Software is offering its anti-malware and PC security suite Vipre with a new pricing model. Rather than annual renewals, GFI Vipre Business Lifetime and GFI Vipre Business Premium Lifetime are available for a one-time purchase fee that lasts the lifetime of the PC on which the software is installed.

Go to: <<http://www.gfi.com>>.

Smart security

Tracey Caldwell, freelance journalist

The rapid consumer adoption of smart devices is driving smartphones and tablets into the enterprise. Yet enterprises are often ill-prepared to secure smart device access to their networks and are having to act fast to enable this.



Tracey Caldwell

According to research company Gartner, in 2010 worldwide smartphone sales were up 72.1% from 2009 and accounted for 19% of total mobile communications device sales.¹ The security concerns accompanying a whole raft of new mobile operating systems, coupled with an increasingly mobile network endpoint

may be giving network managers sleepless nights. But as well as bringing productivity gains to the enterprise, mobile devices may be a way to improve security. There is less mobile malware around for smart devices than for a Windows PC, for example.

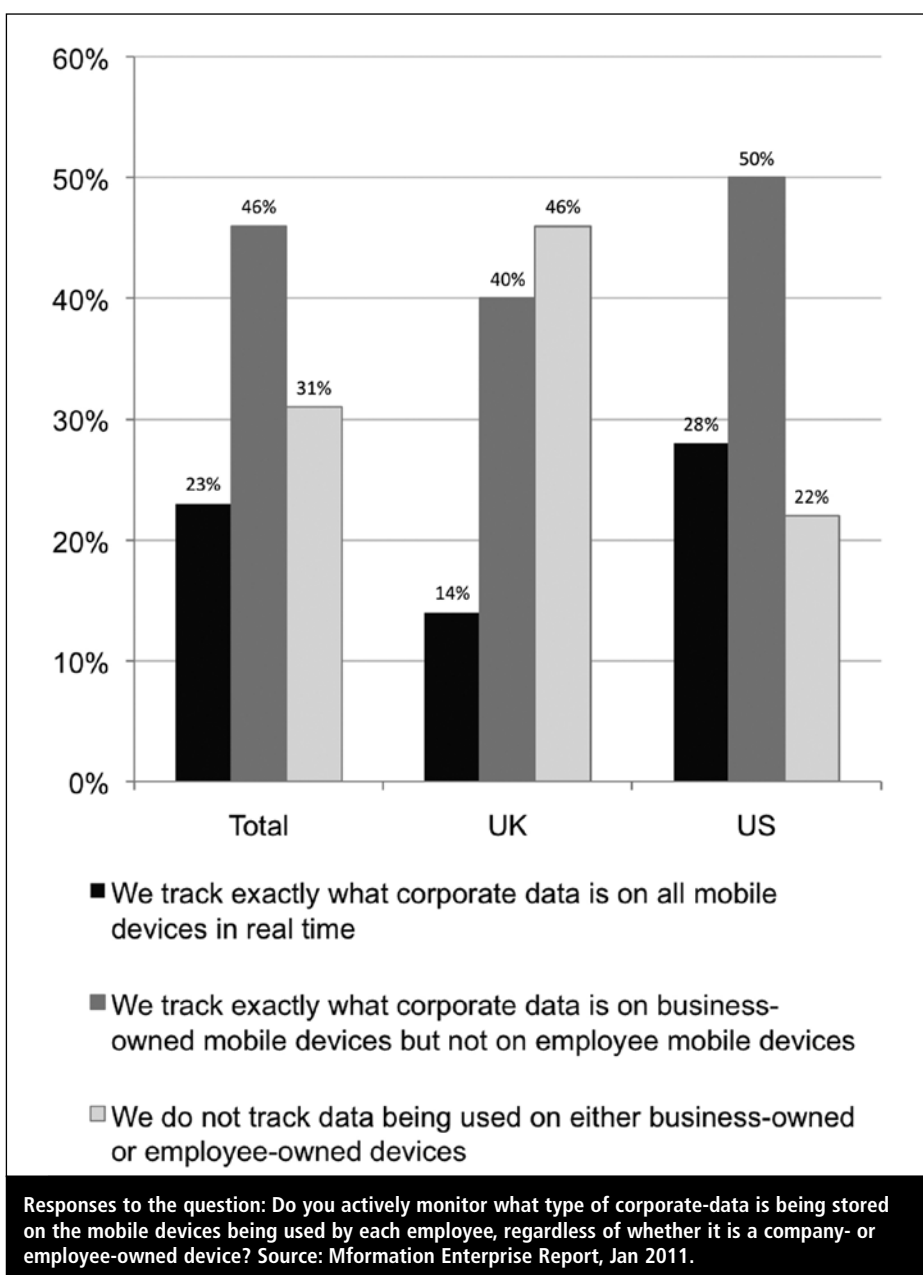
A survey carried out by mobile device

management supplier Mformation of 300 CIOs across the UK and US paints a bleak picture of CIOs' grasp on smart device security. Some 76% of CIOs are concerned that employee-owned mobile devices entering the corporate network through the back door are creating security headaches, 78% don't know what devices are connected to the corporate network and 77% of enterprises have no idea what data is on all of these devices. One in three aren't able to track data on devices that they issue to employees. If devices are lost or stolen, only 56% of businesses are able to secure them. And 77% of CIOs say that limited time and budget, coupled with increasing complexity, has led to a lack of maturity when it comes to managing mobile devices.

Another survey of 200 UK IT directors at large enterprises with over 1,000 employees, commissioned by solutions provider Damovo and carried out by independent research company Vanson Bourne, found that 92% of respondents stated that as more employees are using mobile devices to work remotely and access corporate networks, the number of security threats they faced had increased.

The majority of IT directors had a number of security concerns: 63% admitted that they found enforcing mobile usage policies a headache; 88% said that they would like better visibility of their employees' mobile usage in order to better manage costs and improve mobile security across their organisation; and 82% believed that inconsistent upgrade cycles were leading to increased mobile security and performance concerns.

Procurement was also an issue, with 94% believing that their organisation's mobile devices should be decommissioned in a more secure manner and 81% finding it difficult to manage and secure their mobile phones when they



were not purchased through or specified by the IT department.

“More and more it is becoming economically attractive to build malware for smart devices because they are interacting more with things of value”

IT departments seeking to control employee use of smart devices to access the enterprise network are facing a very fragmented vendor landscape as new vendors emerge and existing ones adapt. Managed service providers are looking to extend services to cover mobile devices while some observers suggest that mobile service providers that currently manage smartphones might look more broadly at enterprise network security.

Smart device malware

Tim Watson, head of the Computer Technology department at De Montfort University, heads the computer forensics and security group that works with government and industry. He also sits on the UK national body for ISO 2700 standards for network security. Watson is already seeing security compromised due to attacks via smart devices: “It is happening,” he says. “Everything from IP theft and industrial espionage.”

“There is a whole host of legal and ethical issues that need to be worked through as well as the technical security aspect”

He adds: “We are no longer carrying just phones in our pocket, we are carting round computers and they have all the same strengths and weaknesses as a computer. We know the primary way in which machines are compromised is through client-side attacks. More and more it is becoming economically attractive to build malware for smart devices because they are interacting more with things of value. Combine that with data leaks where you can get information as to where the connections are – enterprises quite often give far too much away – and it means that for a determined hacker it is quite easy to work out where the weak points are.”

Watson outlines three approaches to the problem: “Many IT departments would like someone to present them with a shopping list so that they could buy a shrink-wrapped solution that you install and then it is not your fault, and you deal with the problem by paying out money and following good advice. The second approach is to let people bring in whatever they want, wherever they want and try to help with client-side security and enterprise-wide sweeps to try to make sure that the device is kept as clean as possible. The third approach, between the previous two, tries to allow people to bring devices and integrate them with the network in a way that is controlled and safe: that is really difficult but perhaps it is the best solution.”

He adds: “The majority of ways in which people try to secure the enterprise network, when connecting smart devices to it, focus on the outset, when authenticating interaction, but we need some mechanism to allow us to continually monitor in a supportive environment.”

According to Watson, there is a whole host of legal and ethical issues that need to be worked through as well as the technical security aspect. For example, the telephone and data suppliers, ISPs and telecoms companies don’t want to be seen in legal terms as publishers.

“If you ask an ISP to block malicious activity, as soon as they start deciding what goes across their network and what doesn’t, they are acting as a publisher,” he says. “They are more comfortable with the body of legal precedent of being simply the pipes. They don’t want a mission creep that would mean that in legal terms they are seen more as the publisher, as that would mean incredible costs.”

Smart device security comparisons

Nigel Stanley, analyst at Bloor Research, is researching the comparative security of smart device platforms: “People say ‘which is more secure?’. We have seen recently a number of issues with Android apps being rescinded because they were shown to have malware. Does that mean it is less secure than the iPhone? People are only just starting to get their heads

around this issue of smartphone security. I have seen a change in the past year, even on a daily basis, as people think ‘what do we do about it?’.”

Despite the issues with Android apps, the security comparison with the iPhone is evolving, he believes. “Android is very interesting as it is an open operating system, open to anyone to modify and change, in stark contrast with the likes of the Apple iPhone, which is a very closed and controlled operating system.”

He does not believe that level of control is necessarily the best approach: “If you hide the way you are securing the hardware or software, the hackers will circumvent that and find out what you do and pull it to pieces,” he explains. “The open approach generally leads to improved security. I use a Blackberry but don’t download apps and use it only for basic email. I have a very simple Java phone for voice which again I don’t download apps on to – read into that what you will. I have an iPhone and I love it but there is a problem with the strategy to lock down apps. When people submit an app to the App Store it finally depends on someone sitting down and deciding whether it is suitable to be released. As they get more apps put into them they cannot cope with doing a detailed exam of every app. You have a human failing there and I am concerned whether the efficacy of the control mechanisms might start to fail as they come under more pressure.”

“Vital corporate data lost may be lost through voice communication alongside data – for example, if an employee is negotiating a contract”

Stanley has seen a number of enterprises creating their own apps to ensure security: “These are their own infrastructure access tools to get into the network but through very secure channels that have been configured by the business so that you are operating in a sandbox to access enterprise systems.”

He points out that smart devices are vulnerable to GSM air attacks: “For about £1,000 you can buy the kit to set up a fake mobile phone base station. The

phone will look for the strongest signal and if your fake station is the strongest signal the phones will camp on to your base station. You can then intercept all the voice and data traffic. The trouble with that kind of attack is it doesn't leave any trace and is very difficult to detect."

In this way, vital corporate data lost may be lost through voice communication alongside data – for example, if an employee is negotiating a contract.

He believes vendors are stepping up to the plate: "A couple of years ago there were only a couple of anti-malware vendors; now there is a large number of people selling solutions. There are some people providing very interesting ways of accessing corporate resources securely using VPN type technology, so there is definitely a growth in that."

Too big a risk

Thames River Capital, a UK investment firm, had written off smart device access to the enterprise network as loss of client data was just too big a risk. Then the CEO got his own iPad and immediately demanded everyone should have one.

"The worst thing for a company our size, where we don't have a huge IT resource, is having too many interfaces to do the same thing but for different estates"

Robert Cockerill, IT manager for Thames River Capital, explains: "Because we are FSA regulated and because of the Data Protection Act we have to be sure, and to be seen to be making sure, that we protect the data that we have, wherever that may be."

He wanted to be able to protect data on the device and control aspects of the presentation of the device to the user as well as remotely disable and wipe lost devices.

"The worst thing for a company our size, where we don't have a huge IT resource, is having too many interfaces to do the same thing but for different estates. It just becomes a headache to try and manage that," says Cockerill. "It needed to be a quick and easy win to find the right fit for what we wanted to do and to get it installed and work-

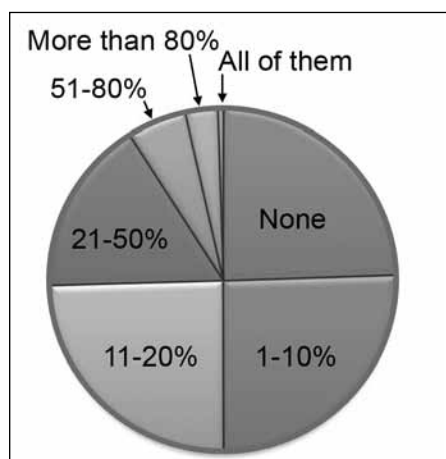


Figure 2: Responses to the question: Of all the PCs in your organisation, what percentage would you say are mobile (ie, laptops, notebooks, netbooks or tablets)? Source: Quocirca survey of UK and Germany SMEs, 2010.

ing quickly as well. It couldn't be one of these all-singing appliances that requires five months of programming to do."

Cockerill's research into potential vendors did not take long. "There aren't many vendors that actually have a solution to this and they are quite easy to find. We dropped it down to two, MobileIron and Good, within just a few hours of research."

The firm deployed MobileIron Virtual Smartphone Platform for real-time intelligence and control over mobile content, activity and apps. MobileIron supports mobile operating systems including Blackberry, iPhone and iPad and creates boundaries between personal and business data on employee-owned devices. For example, lost phone lock and wipe functionality is activated by the user, but configured by IT to ensure enterprise data privacy.

Cockerill has created two policies, one for the company and one that he describes as "more 50/50, a bit less corporate and a bit more consumer" where employees may lose a bit of corporate functionality and gain a bit more on the app store side. Employees might switch mode when going on holiday, for example.

Accelerated consumerisation

Ken Corriveau, chief information officer at Omnicom Media Group, believes tablet devices have accelerated consumerisation in

the workplace. "We wanted to enable our users to work when they wanted and how they wanted, balancing the data integrity and security that we needed in our environment," he says. "There has been a lot of talk of 'do we move to a direction that instead of providing corporate devices we provide a stipend and we let the consumers bring in their own devices?'"

Five years ago only corporate devices had limited network access, for email or a limited number of files. Now Omnicom runs a secure intranet environment based on Sharepoint and employees can access that to get to their files.

Corriveau has implemented the latest version of ForeScout CounterACT to get visibility and control of smartphones and iPads. CounterACT can force mobile device guest registration via HTTP redirection and manage access to network resources and wireless access points. The solution monitors who, what and where resources are on the network, including users, device types, applications, processes, ports, external devices and compliance status.

"I don't think there is any one technology or platform that is the be all and end all of security – it is about layers"

"We have the ability to monitor network traffic," says Corriveau. "If there is an anomaly to our everyday patterns it can isolate it and notify the security admin to look into the issue." The second component is to ensure network access policies are adhered to.

Corriveau is increasingly concerned about the unknown threats to smart device network access. "It is still such a new platform and we are hearing of a growing trend for viruses and worms coming into mobile devices. More people are targeting this platform because they know it is the gateway to corporate environments now."

He adds: "I believe in the layered approach to security so I have a variety of products in our environment that provide different levels of security and I don't think there is any one technology or platform that is the be all and end all of security – it is about layers."

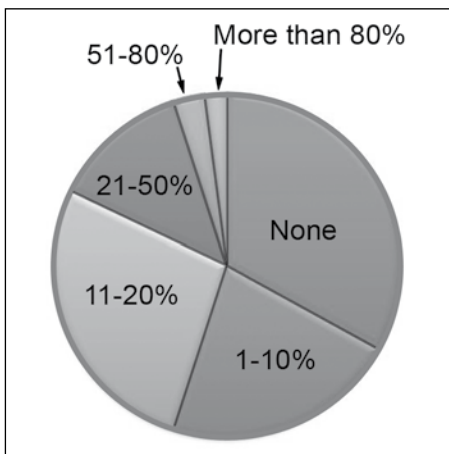


Figure 3: Responses to the question: What percentage of your employees work remotely at some time during the week and are given remote access to IT? Source: Quocirca survey of UK and Germany SMEs, 2010.

He is looking to broaden access functionality from smart devices to enterprise resources. “Employees didn’t have access to the network previously so they now have more capability. Is it the same capability that they have on their laptops? Absolutely not. Will they get there? Maybe. We are looking at exploring virtualised desktops or leveraging Citrix more.”

Cautious approach

Kevin Braysher is head of IT at Lane Clark & Peacock (LCP) – actuaries with offices in London and Winchester, UK, and four other European countries. He is taking a cautious approach, enabling limited access for 45-50 smart devices, mainly iPhones with some HTC on Android, alongside the firm’s established Blackberry estate, for corporate email access. The additional smart devices only interface with the enterprise network when they are connected to a PC for syncing and Braysher concedes to being ‘nervous’ about that. There are plans to integrate the access of corporate Blackberries and additional smart devices to the network but Braysher describes this as being at an early exploratory stage. He has also been exploring the development of corporate apps but has hit budgetary constraints.

As well as the productivity benefits, Braysher says the need to portray LCP as an innovative enterprise is driving work on smart device access to the corporate network, in the face of any security

concerns. The company has been using iPads for paperless meetings and this has had a very positive impact on clients.

“The business wants to be exploiting the technology and it confirms our position on the marketplace as being innovative,” he says. “For the partners to be using these devices and familiar with them creates a very good impression.”

LCP is working with Azzurri, which provides network connectivity to LCP and now advises on integrating smartphones. “Telecoms providers operate in some weird space with their charging structure and their support offerings and you do need to speak to someone who can make sense of that,” says Braysher.

Smart device security options

There are a number of options for enterprises grappling with securing smart device access to the enterprise network. Gartner has predicted a strong trend for device-independent security – a collection of security technologies, application technologies and sourcing options that enable the provisioning of applications that are secure, but less tightly tied to specific devices and platforms, and that, in many cases, do not require security tools to be installed on the client.

This category includes: thin-client architectures; applications as a service; platform-independent forms of network access control (NAC); portable personality; virtualisation; and hosted security services, such as ‘in the cloud’ virus scanning.

Gartner reports: “Device-independent tools cannot provide the rigour of fully installed security, but a blend of several of these tools can enable CIOs to deliver applications that can run on a wider range of devices while reducing security risks.”

Bob Tarzey, analyst at Quocirca, points out that one of the issues is the number of different providers, from Apple to Blackberry via Android, which means that even if business were addressing the issue they have a bigger problem to manage than with the heterogeneous Microsoft environment.

“Windows is still far easier to go after as it is so pervasive and that is where the



Figure 4: Bob Tarzey, Quocirca.

juiciest data is,” he says. “But I think we will see an attack and when that happens that will be the wake-up call that hasn’t really happened yet.”

“Network managers are faced with a new world of operating systems and apps that must be addressed if previously well-executed network security is not to fail”

Tarzey outlines two approaches: “Put a management platform in place that can ensure security is maintained on all devices and make sure that confidential data is not copied on to devices or, if it is, it is encrypted, or that they can’t email except via the corporate email channel, which is monitored – all that stuff to make sure the device in itself is inherently secure. Or you have to force all access back via a central point which means the device becomes a dumb access point that gives the employees some of the benefits of being mobile. In reality, where organisations end up will be somewhere between the two and it will depend on job function. You are not going to stop the MD from using his Blackberry whenever he wants to, so you have got to make sure it is secure. But you can say call centre staff cannot access their email on their iPhones as there is no real need to.”

He describes the industry response as “messy. It is hard to buy something to solve the problem. A single vendor who can offer you a management capability across all devices and anti-malware just doesn’t

exist at the moment, but lots of vendors are starting to put the pieces in place.”

The drive to enable smart device access to the enterprise network appears inexorable and the benefits of a low incidence of malware may be short-lived as criminals spot the value of breaching communications between smart devices and the enterprise. Network managers are faced with a new world of operating systems and apps that must be addressed if previously well-executed network security is not to fail.

About the author

Tracey Caldwell is a freelance business technology writer who writes regularly on network and security issues. She is editor of Biometric Technology Today, also published by Elsevier.

References

1. ‘Gartner says worldwide mobile device sales to end users reached 1.6 billion units in 2010; smartphone sales grew 72% in 2010’. Gartner, 9 Feb 2011.

Accessed April 2011. <<http://www.gartner.com/it/page.jsp?id=1543014>>.

Resources

- ‘Competitive Landscape: Mobile Devices, Worldwide, 4Q10 and 2010.’ Gartner. <<http://www.gartner.com/resId=1542114> March 2011>.
- ‘IDC Predictions 2011: Welcome to the new mainstream’. December 2010. <<http://www.idc.com/research/viewdocsynopsis.jsp?containerId=225878>>

Why mobile two-factor authentication makes sense

Andy Kernshall, SecurEnvoy

Although technology never stops evolving, sometimes it takes its time. Often for good reasons: new operating systems need to be assessed for compatibility before being rolled out across an organisation, and numerous technologies have been vigorously touted as the Next Big Thing. Virtualisation has been held back by connectivity limitations. And the cloud has suffered from the same drawbacks – the omnipresent connectivity that was promised and has yet to materialise.

Two-factor authentication (2FA) has been heralded as the saviour of computer security for a good few years, but business users haven’t quite taken to the technology as quickly as expected. This is for one very powerful reason – inconvenience. 2FA forces users to significantly change their habits – for example, having to remember to carry a physical passcode token at all times or go through the time-consuming process of obtaining the passcode through other means.

Ultimately, regularly used computer security systems need to recognise the importance of usability and of allowing users to get on with the job at hand without having an excessive number of hoops to jump through. This is where tokenless two-factor authentication comes in. This form of 2FA adds an additional layer of security to the process by requiring a separate passcode in

addition to a PIN or other secret information to be entered when the user is resetting his or her password.

Mobile phones in our daily lives

With hackers becoming increasingly determined and more effective, it pays to add the extra level of security provided by 2FA (for more detail on why mobile 2FA is an effective measure, see ‘The threat of brute force attacks’ below). With tokenless two-factor authentication, users have a new and convenient way to authenticate for remote access or reset their password and validate their identity, regardless of where they are in the world, by sending a one-time, two-factor authentication passcode to the user’s personal mobile phone via SMS. In addition, SMS messages can be sent seven days before (as well as the

same day) that a user’s password expires. Studies in the Internet banking sector have proven that SMS delivery of single-use passcodes is very popular with end users for the simple reason that it is unobtrusive and convenient, especially when compared to the use of physical tokens.¹

“Goode found that 40% of organisations plan to deploy services that will enable employees to use their mobile phones as remote access authentication devices by the end of 2011”

Given the proliferation of mobile phones, for both business and personal use, and the natural habit of users of keeping their mobile devices with them at almost every moment of the day, some telling statistics recently revealed by Goode Intelligence should really come as no surprise. Goode found that 40% of organisations plan to deploy services that will enable employees to use their mobile phones as remote access authentication devices by the end of 2011.² It seems that the idea of mobile tokenless



Andy Kernshall

two-factor authentication is coming to the fore.

The trend for employees working from home is another compelling case for fast uptake of tokenless 2FA. At the end of 2010, we once again saw another satellite picture of Europe covered in a blanket of snow. It's no wonder that mobile and home working is here to stay, and inclement weather conditions make it all the more desirable as a way for companies to maintain productivity even when the transport infrastructure fails to cope. It's becoming a cliché to make this connection, but the fact remains that working from home is both popular and, sometimes, the only option for continuing business. Remote access has enabled companies to be unaffected by the snowfall, with the result that secure remote access has been pushed further up the agenda.

So 2FA may be the answer to multiple problems, but why use 2FA at all? Isn't a username and password enough? To answer this question, let's look at password strength in greater detail.

The threat of brute force attacks

Broadly speaking, the longer a password is, the stronger it is. Passwords can be associated with a mathematical cryptographic value that is dependent on a number of variables. Using additional variables such as upper case, lower case, numbers and symbols can generate even stronger passwords.

Long passwords are good, but consider the following examples:

- User 1 password = redcheese6
- User 2 password = zglihalq

User 1's password is made up of two words and one number. Assuming 20,000 easy to remember common words in the English language, this password's strength is $20,000 \times 20,000 \times 10$ numbers = 4 billion possible combinations, or in terms of cryptographic strength, a 32-bit key.

User 2's password is eight randomly generated letters, therefore strength is $26^8 = 208$ billion combinations, or the cryptographic strength of a 38-bit key.

The User 2 password is stronger and surpasses the strength of User 1.

However, this kind of password strength is inherently difficult for the user to remember, often requiring it to be written down – it is not uncommon to see things like a post-it note stuck to the computer screen with the password written on it.

So, we now understand password strength, but how do we protect passwords from brute force attacks? Unfortunately there's no one silver bullet to solve this problem.

Physical attacks

Nearly half of all password attacks are physical, using social engineering skills to obtain them. Simply reading a sticky note on a colleague's computer is a simple attack, so is the 'shoulder surfing' technique – literally watching over a person's shoulder (ATMs usually carry warnings when you are entering your PIN code, but personal computers do not). More sophisticated attacks use software to capture keystrokes at logon and then send the captured information to a criminal's computer for future nefarious use. Keylogging software can be installed on a computer from a virus infection, a trojan program or a spyware program that was automatically downloaded from a website (these can all occur without the user's knowledge). These attacks are especially serious as the user is unaware until the damage has been done. Anti-virus and anti-malware software can be used to guard against attacks, but no software can guarantee 100% success.

"A moderately powerful computer running L0phtcrack can sustain password cracks of around 3 million cracks per second"

Network snooping is another prevalent attack. Programs such as Cain and Able and Dsniff capture passwords as they traverse the network. These programs capture web, FTP and telnet logons (telnet is used with network communication equipment or Unix systems). They do this very effectively and with little user set-up or intervention.

Passwords traverse the network in one of two ways. In the first method, a password is sent in plaintext and therefore anyone using a protocol decoder will be able to see any plaintext password. The second way affords some protection by hashing the password. A hashing algorithm is a one-way function, transforming the plaintext password into a hash of fixed length. Common hash programs are MD5 and SHA-1, which have a fixed output of 128-and 160-bit hashes.

However, it is easy for hackers to defeat a hashing algorithm by generating a dictionary file of different password options and running them through the same hash algorithm. If the output from this algorithm is the same as the hash, the password has been broken.

This technique is known as a brute force attack. Commercial programs are available today such as L0phtCrack. A moderately powerful computer running L0phtcrack can sustain password cracks of around 3 million cracks per second. If this program were used with our example users above, all passwords would be cracked in the following timeframes:

- User 1 > less than 23 minutes
- User 2 > less than 20 hours

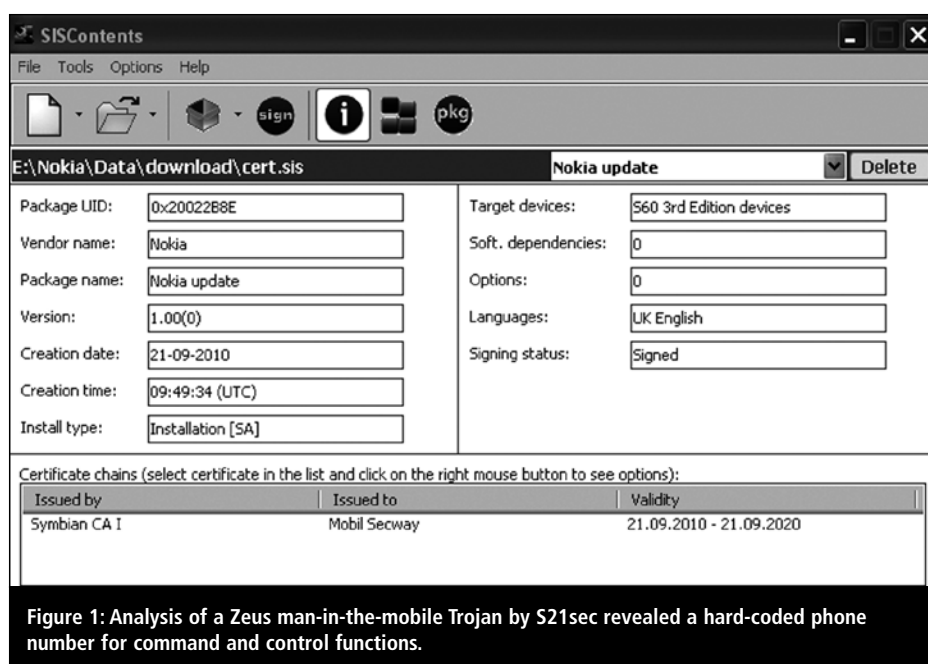
Finally, passwords are troublesome to manage as users typically decide their own passwords. Below is an extract from an audit of 342 user accounts conducted for a major client:

- 29 users had the password 'password'
- One user had the password 'password1'
- Four users only used numbers – two of which looked like a date of birth
- Three users only used five-character passwords

The key to defeating all these attacks is to employ a one-time password (OTP) that can only be used on a single occasion. Any attempt to record and replay a password renders it useless as the initial password has already been locked. This is strong two-factor authentication, and it renders the attacks outlined above either totally ineffective or highly improbable.

Password policies

To increase the strength of a password, organisations are advised to regularly reset user passwords. Some companies



reset after 30, 60 or 90 days, but even quarterly resets can result in users forgetting their passwords. Users may try to alternate their favourite passwords so it's also important to use a history list that tracks previous passwords. Traditional password-reset security questions rely on static answers, such as a mother's maiden name or employee number, but this method would fail a security audit because the information doesn't change, it would fail history list checks and can be easily obtained by a hacker.

"Mobile or remote users no longer have to return to the office and local users no longer need to be verified by IT or HR staff"

A CIO or IT supervisor who has implemented a password policy as part of a total security mandate will inevitably face problems resetting passwords – especially for remote users who rarely visit the office. They are out on the move, and when it comes to resetting their passwords, they will need to be physically in the office as they need to login to their laptop in order to start their VPN connection. This creates a catch-22 situation as they cannot reset their password until they are connected to the office. In the past, the only viable option was to allow their passwords to remain static,

but again, this is not recommended and would lead to a security audit failure.

With 2FA, there's an additional layer of security to the process as a result of requiring a separate passcode in addition to a PIN or other secret information to be entered when the users are resetting their passwords. Mobile or remote users no longer have to return to the office and local users no longer need to be verified by IT or HR staff. In turn, this prevents the type of scenarios where workers are sometimes unable to access their computers for up to two days due to password reset problems, particularly if they don't plan their trips around scheduled password resets.

Mobile security in 2011

No computer security solution can ever be totally watertight, but you can add layers of difficulty. To use an analogy, an especially determined criminal would find a way to gain access to the average family home, but there are ways you can deter a criminal and lessen the chance of being burgled. Although the threat of attacks is real, many computer security companies are increasingly using scare tactics to convince users and companies that certain types of attacks will circumvent advanced security measures. However, the examples they cite, such as phishing attacks (essentially a confidence trick), require an unrealistic level of action on the part of the user.

Taking SMS-based authentication as an example, it's patronising to assume that people will fall for a phishing attempt just because it arrives on their mobile phone. Building hysteria around 'smishing' – the latest scaremongering security story fuelled by companies touting hardware tokens – is at best naive, and at worst damaging to the wider efforts of the IT security community.

Analysts, think tanks and journalists all consider 2011 to be a breakthrough year for mobile computing.³ This expectation brings with it a new wave of speculation and fearmongering about mobile device security – for example, that Zeus is allegedly going to infect mobile devices and take over SMS use.⁴ Numerous stories are also claiming that cyber-criminals will soon be sending out rogue text messages with apps to download at the user end, while taking control of SMS gateways inside corporations.

While it's theoretically possible for an attacker to inject a rogue login panel to a banking website and steal some details, the security flaw there is due to the website and not the mobile authentication.

"The computer security industry should refrain from circulating unlikely scenarios that could frighten users and potentially hold businesses back"

It's also naive to assume people are going to download an app sent to them from a malicious yet anonymous cyber-criminal. And while it's perfectly possible for a telephony denial-of-service attack to occur, well designed two-factor SMS authentication solutions should preload passcodes, therefore defeating this attack and resolving any intermittent signal or SMS delivery delays.

Two-factor authentication is still the benchmark in security, and doing it by SMS is not only the most convenient but the most realistic and achievable approach. The computer security industry should refrain from circulating unlikely scenarios that could frighten users and potentially hold businesses back. Instead, we should concentrate on making a clear case for effective authentication that will benefit businesses of all shapes and sizes.

So, we have a good idea that 2011 will be an important year for mobile phones and for two-factor authentication. Indeed, 2FA is a lean and effective option for organisational computer security that is easy to use and simple to implement. So, are you one of the 40% that will be adding mobile 2FA to your security measures this year?

About the author

Andy Kemsball is technical director at SecurEnvoy, the inventors of mobile two-factor authentication. He began

his 16-year career in computer security at RSA Security before founding SecurEnvoy with Stephen Watts in 2003. Since then, SecurEnvoy's products – SecurAccess, SecurPassword, SecurICE and SecurMail – have been adopted worldwide.

References

1. Han, Joo Suk et al. 'The Impact Of Two-Factor Authentication Technology On The Adoption Of Internet Banking'.
2. Goode, Alan. 'The Mobile Phone as
3. 'Informa Telecoms & Media identifies Top 10 trends for 2011'. Informa Telecoms and Media, 2010. Accessed Mar 2011. <<http://www.informatm.com/itmgcontent/icom/s/press-releases/20017828913.html>>.
4. 'Zeus Mitmo: Man-in-the-mobile'. S21secBlog (2010). Accessed Mar 2011. <<http://securityblog.s21sec.com/2010/09/zeus-mitmo-man-in-mobile-i.html>>.

Cracking GSM

Steve Gold, freelance journalist

Next year – 2012 – will be the 30th anniversary of the birth of the GSM standard. Back in 1982, the European Conference of Postal and Telecommunications Administrations (CEPT) created the Groupe Special Mobile (GSM) standard to allow mobiles to be used across Europe. In 1989, the development process was transferred to ETSI, the European Telecommunications Standards Institute, and phase I of the GSM specifications was published in a year later.

In 1991, the world's first GSM service at 900MHz went live on Radiolinja's network in Finland, to be quickly followed by Vodafone's GSM 900 network in the UK and the Deutsche Telecom network in Germany.

Unlike the world's first Total Access Communication System (TACS) analogue networks launched in 1986 in the UK, the second-generation GSM standard services were – and still are – fully digital, allowing data IDs to be shared between networks in real time. This was – and continues to be – a key selling point of GSM over TACS, since 2G digital services allowed roaming between networks: by the end of 1993, just 30 months after the launch of the Finnish network, there were more than a million subscribers on 70 operator networks in 48 countries.

Unlike TACS analogue services – which were phased out in the early part of this century – GSM uses encryption to protect the integrity of the data transmissions, which can either be voice calls (in a packet data format) or a data

stream carrying anything from email and picture messages, to a VOIP transmission or a web surfing session.

The modulation used in GSM is Gaussian Minimum-Shift Keying (GMSK) – a continuous-phase frequency shift keying that modulates the signal onto the carrier, suitably smoothed with a Gaussian low-pass filter prior to being fed to a frequency modulator. This frequency modulator helps ensure that co-channel interference issues do not affect the data transmission's integrity between the mobile and the GSM base station.

Although GSM – aka PCS in the US and the Far East – operates on many frequencies, including 800, 900, 1800 and 1900MHz, the standard mandates the use of timeslots for individual phones to use. Under the basic GSM standard, this allows eight full-rate or 16 half-rate speech channels per radio frequency. These eight radio timeslots – aka burst periods – are grouped into a Time Division Multiple Access (TDMA) framework, with half-rate channels using alternate frames in the same timeslot.

an Authentication Device: Analysis and Forecasts 2010-2014'. Goode Intelligence, 2010.

3. 'Informa Telecoms & Media identifies Top 10 trends for 2011'. Informa Telecoms and Media, 2010. Accessed Mar 2011. <<http://www.informatm.com/itmgcontent/icom/s/press-releases/20017828913.html>>.
4. 'Zeus Mitmo: Man-in-the-mobile'. S21secBlog (2010). Accessed Mar 2011. <<http://securityblog.s21sec.com/2010/09/zeus-mitmo-man-in-mobile-i.html>>.



Steve Gold

The channel data rate for all eight channels is 270.8Kbit/s, and the frame duration is 4.62ms.

Authentication

The system also includes one potential weakness, at least from a security perspective. The only means by which a mobile can authenticate itself to the network is over the air (radio channel) interface. This is achieved through a combination of the International Mobile Subscriber Identity (IMSI) – the unique electronic serial number of the SIM card inserted into the phone – and the International Mobile Equipment Identity (IMEI), which is a unique serial number of the mobile. Both these serial numbers are encrypted using A5/1 encryption and presented to the cellular network at the start of each outgoing call. And, just to make life difficult for eavesdroppers, the IMSI is normally only transmitted to the network when the handset is first switched on. At this point, the network randomly assigns a Temporary Mobile Subscriber



Identification (TMSI) number to the mobile, allowing it to be identified by the network at all stages while it is within its current power cycle.

The network also randomly and periodically assigns a new TMSI to the mobile, meaning that only the network ‘knows’ the IMSI to which the current TMSI is assigned.

This makes the task of ‘tumbling’ – the cracker term for mobile serial number sniffing from radio data channels – all the more difficult, as it is only when the handset is switched on or when the network periodically assigns a new TMSI, that the IMSI code is transmitted by the mobile back to the network.

Early hacks explained

Early hacks of GSM networks centred around a system known, appropriately enough, as an IMSI catcher – also known, in commercial terms, as a Virtual Base Transceiver Station (VBTS).

VBTSs were developed commercially for use when testing GSM networks and handsets. But they were later reverse engineered by crackers in the early 2000s to develop software-driven, laptop-based mini-base stations known as picocells. It’s important to note that VBTSs can function because the GSM standard requires the mobile to authenticate itself to the network but not the network to authenticate itself to the mobile.

An IMSI catcher works by appearing as a base station to all the mobiles within range and logging all their IMSI/IMEI and TMSI/IMEI pairs. It also takes advantage of a ‘feature’ of GSM handsets: when they encounter ‘choppy’ signal conditions – such as when in a moving vehicle or subject to signal fading (eg, over water) – the GSM standard allows for encryption to be switched off (a mode known as A5/0 encryption). IMSI catchers – in the form of modified VBTSs – are used in many countries by secret service and law enforcement agencies, but the hacker IMSIs are the ones of real concern.

“Hackers can software-generate a new IMSI/IMEI pair anywhere on the network, to make and receive voice and data calls as they wish”

After the unit has logged all the IMSI/IMEI and TMSI/IMEI pairs in the area, the system triggers a reauthentication process with the mobiles on a one-by-one basis, so capturing their complete IMSI, and then using that IMSI/IMEI pair to stage a man-in-in-the-middle attack with a legitimate, but distant, cellular base station. This allows complete voice and data call eavesdropping.

Perhaps worse, because the GSM users can make and receive calls as normal, they are unaware of the presence of the

IMSI catcher and the hackers can then software-generate a new IMSI/IMEI pair anywhere on the network, to make and receive voice and data calls as they wish. Furthermore, it is also possible to clone a SIM card with the eavesdropped IMSI and, by reflashing the firmware of another GSM handset – an illegal process in most countries – assign the paired IMEI to that handset. To the network, the correct IMSI/IMEI pair is offered and authenticated, and a TMSI assigned to the handset – and the hacker has a cloned handset that will work as long as the carrier thinks the legitimate user has credit.

IBM research

Before we look at some of the breakthroughs that hackers have made in subverting the GSM standard in recent years, it helps to step back to 2002 when IBM carried out in-depth research into security flaws in GSM SIM cards.

At the time, it was known that cloning a SIM card was technically possible, but used expensive kit way beyond the reach of most hackers, making the process highly uneconomic. IBM’s research discovered a loophole in the SIM cards of the time – now long superseded – that allowed hackers with physical access to the card to read all the available data and so software-generate a cloned SIM card, all using off-the-shelf hardware costing around \$200. The IBM technique required a smart card reader, a PC equipped with software that could analyse power consumption samples extracted from the card and, of course, physical access to the phone plus its SIM card.

“The kit used was nothing more than a high-power laptop and a couple of RF antennae from the local electronics store. In his demonstration, he was able to record his audience’s GSM calls”

While IBM developed the technology to stop this loophole from being exploited, and presented its research at the Institute of Electrical and Electronics Engineers conference of 2002, a chain of events had been started.¹ That IEEE conference was attended by researchers at

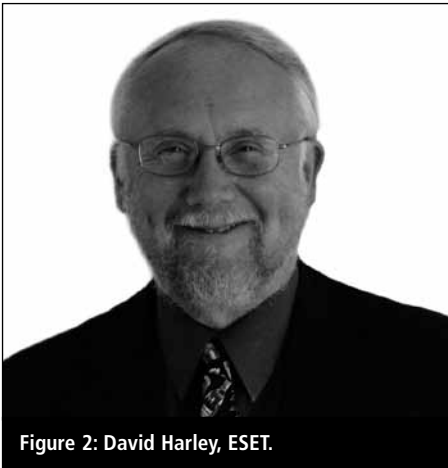


Figure 2: David Harley, ESET.

the Technion Institute in Haifa, Israel – Professor Eli Biham and doctoral students Elad Barkan and Natan Keller – who started their own research into cracking the GSM standard. A year later they presented their theoretical findings at the Crypto 2003 conference at the University of California and rocked the previously (reasonably) secure GSM world.

“If you thought things couldn’t get any worse, think again. In early March of 2011, hackers managed to download and recompile more than 50 apps for the Google Android smartphone platform.⁵ After infecting the apps with malware, they then uploaded them to Google’s Android Market, the open source equivalent of Apple’s iTunes store for iPhones, iPads and iPod touches”

It took a further seven years before a hacker called Chris Paget put the Israeli researchers’ theories into practice by developing a home-brew unit costing \$1,500 that captured – and interpreted in near real-time – all outgoing GSM data from mobiles in the area. Paget, who a year earlier had publicly cracked the RFID technology in US passports, allowing him to download the credentials of a passport in close proximity, staged a demonstration at the summer Defcon 2010 event in Las Vegas that spoofed a GSM base station.² The kit used was nothing more than a high-power laptop and a couple of RF antennae from the local electronics store. In his demonstration,

he was able to record his audience’s GSM calls and generate a recorded message to them that their phone security had been compromised. Paget’s demonstration again showed the security issue of the GSM mobile accessing the base station with the strongest signal.

Later in 2010, two other researchers – Karsten Nohl of Security Research Labs and Sylvain Munaut of OsmocommBB – explained at the December conference of Germany’s Chaos Computer Club how they had enhanced Paget’s and other researchers’ work to a new level.³ Using a multi-core laptop running open source software and four low-cost (\$15) GSM handsets, the pair were able to eavesdrop the GSM burst periods on all channels in the vicinity, and then feed all the available data into the laptop, where it was crunched in real time.

The crunching was made possible by work that Nohl had revealed a year earlier at the December 2009 Chaos Computer Club conference, in which he announced that he had painstakingly computed all possible A5/1 encryption hashes, generating a 2TB code table in the process.⁴ By crunching the streamed data from the four GSM handsets though his high-powered laptop in December 2010, and tapping the 2TB hash table, Nohl and Munaut were able to decrypt all the GSM calls on a nearby base station in real time.

Enter the Google Android

If you thought things couldn’t get any worse, think again. In early March of 2011, hackers managed to download and recompile more than 50 apps for the Google Android smartphone platform.⁵ After infecting the apps with malware, they then uploaded them to Google’s Android Market, the open source equivalent of Apple’s iTunes store for iPhones, iPads and iPod touches. Although the apps were only available for 48 hours, they were reportedly downloaded by around 200,000 Android handset users, who then infected their mobiles with the DroidDream malware.

In a posting to Android’s security blog on 5 March, Rich Cannings, Android’s

security lead, revealed that his firm was remotely removing the malicious applications from the affected devices. “This remote application removal feature is one of many security controls the Android team can use to help protect users from malicious applications,” he noted in his security blog. “The applications took advantage of known vulnerabilities which don’t affect Android versions 2.2.2 or higher. For affected devices, we believe that the only information the attacker(s) were able to gather was device-specific (IMEI/IMSI) unique codes which are used to identify mobile devices, and the version of Android running on your device.”

Although Canning did not realise the significance of what DroidDream does, most people are able to draw their own conclusions. This is the problem with the Google Android smartphone operating system. It is open source, meaning that, unlike the Apple iTunes platform, apps can be downloaded from anywhere on the Internet into an Android handset, which typically has no native security software. Using DroidDream-infected apps, hackers can then harvest users’ IMEI/IMSI pairs remotely.

“This is the problem with the Google Android smartphone operating system. It is open source, meaning that, unlike the Apple iTunes platform, apps can be downloaded from anywhere on the Internet into an Android handset”

No wonder that David Harley, a leading security researcher and security fellow with anti-malware vendor ESET, called Android “terrifying” in an interview with *InfoSecurity* in early March.⁶ But it could potentially get worse, as Harley claims that his peer researchers at Gartner are now saying that there will be 17.7 billion smartphone apps – not just on Android – downloaded by the end of 2011. It is, he explains, an almost impossible task to track them.

The Android incident represents a software-only attack vector, making the cost of entry effectively zero for those looking to harvest GSM IMEI/IMSI

pairs for use on the world's cellular networks. It's an entirely new ballgame for GSM hackers.

About the author

Steve Gold has been a business journalist and technology writer for 26 years. A qualified accountant and former auditor, he has specialised in IT security, business matters, the Internet and communications for most of that time. He is technical editor of Infosecurity and lectures regularly on criminal psychology and cybercrime.

References

1. 'IBM Research Develops Technology to Protect GSM Cell Phones' ID Cards From Hacker Attacks'. IBM, 7 May 2002. Accessed Apr 2011. <<http://www-03.ibm.com/press/us/en/pressrelease/22040.wss>>.
2. 'Hacker shows how he intercepts GSM cell phone calls'. YouTube, Jul 2010. Accessed Apr 2011. <<http://www.youtube.com/watch?v=q8JuYh7Km34>>.
3. Dec 2010 – Krempel, Stefan. '27C3: GSM cell phones even easier to tap'. The H Security, 29 Dec 2010. Accessed Apr 2011. <<http://www.h-online.com/security/news/item/27C3-GSM-cell-phones-even-easier-to-tap-1160200.html>>.
4. 'GSM 64-bit encryption standard cracked and posted to web'. InfoSecurity, 30 December 2009. Accessed Apr 2011. <<http://www.infosecurity-magazine.com/view/6157/gsm-64bit-encryption-standard-cracked-and-posted-to-web>>.
5. Mar 2011 – Hamada, Joji. 'New Android Threat Gives Phone a Root Canal'. Symantec, 2 Mar 2011. Accessed Apr 2011. <<http://www.symantec.com/connect/blogs/new-android-threat-gives-phone-root-canal>>.
6. "Android is terrifying" says ESET's David Harley'. InfoSecurity, 1 Mar 2011. Accessed Apr 2011. <<http://www.infosecurity-magazine.com/view/16286/android-is-terrifying-says-esets-david-harley>>.

Resources

- 'The GSM Specifications'. Tutorialspoint. Accessed Apr 2011. <http://www.tutorialspoint.com/gsm/gsm_specification.htm>.

Information security in the cloud

Richard Blandford, Fordway

Although cloud computing promises limitless capacity, almost total flexibility and increased efficiency – as well as the benefit of moving IT spending from CapEx to OpEx – organisations are being slow to adopt it. One of the key inhibitors for the take-up of cloud services is information security. However, you can address these concerns through initially moving to a hybrid cloud model and assessing which services are appropriate to move to the public cloud.

The basis of cloud computing

The US National Institute of Standards and Technology (NIST) defines cloud computing as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (eg, networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction".

Underneath the hype, cloud computing includes some extremely useful concepts that organisations can quickly and easily implement to improve services. However, many organisations are extremely nervous about the implica-

tions of moving to the public cloud model, perceiving it to be inherently less secure than a private network infrastructure. There are several reasons for their concerns – the cloud is multi-tenanted, no-one knows exactly where their data is and there is the potential of a long supply chain, meaning that the ultimate provider of the service may not be the supplier that the organisation has contracted with.

Happily, the majority of these issues can be negated by initially implementing a private cloud infrastructure for critical services and reserving the public cloud for specific, low-risk services – effectively creating a hybrid cloud. At the same time, you can put in place the appropriate security standards and protocols,

which will develop as cloud services and service providers mature. This means organisations will still need to have and run their own infrastructure, or have a trusted third party run it for them.

Once organisations are familiar and comfortable with cloud concepts and practices, and as commercial cloud service providers enforce and provide better guarantees of information security standards, they can look to migrate less business-critical services to the public cloud, if appropriate.

Implementing security standards in the cloud

For an optimum hybrid cloud solution, business units should define the application or service they require with relevant Service Level Agreements (SLAs) plus access and information security requirements. Once defined, the business should then leave other decisions (such



Richard Blandford

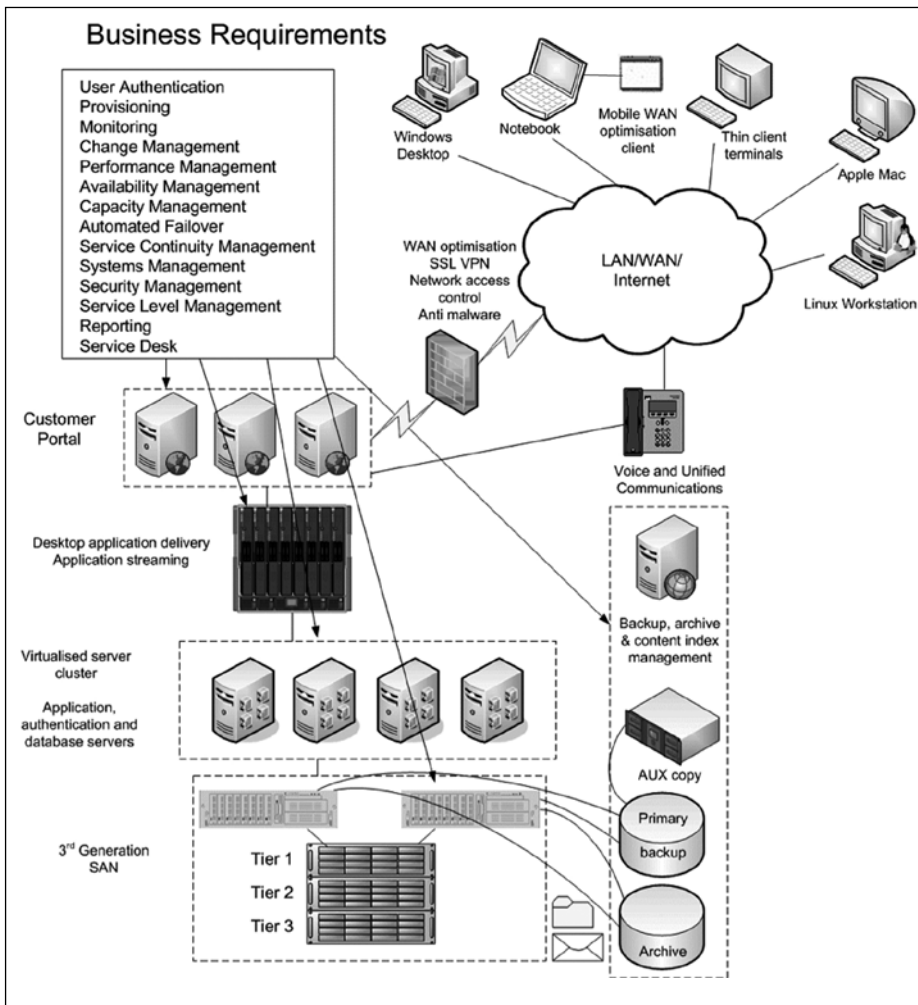


Figure 1: The infrastructure for a private cloud.

as platform, OS, virtualised vs non-virtualised, resilience and failover etc) to the IT professionals. The business units benefit as their service definition and initiation can be considerably quicker and easier than before, while the IT professionals benefit as they spend more time ensuring the service to their user community.

“Once the policy is in place, the security standards then provide the organisation with a set of tools and techniques to review, enforce, maintain and improve the policy”

Once service levels are defined, there are several standard best-practice frameworks with which the organisation may already be complying, or may be intending to implement, such as ITIL/ISO20000 for IT service delivery and BCI best practice for business continuity. These can be refined and optimised to

suit the exact requirements of the organisation.

There is a number of appropriate security standards available that organisations can use. These provide a model for establishing and operating an Information Security Management System (IMIS). Every aspect of private cloud can be audited against standards such as ISO27000, the government-mandated Code of Connection or PCI DSS best-practice information security standards in order to minimise or negate the chance of a security breach. Effective security processes can be embedded into the portal and the platform. Once the policy is in place, the security standards then provide the organisation with a set of tools and techniques to review, enforce, maintain and improve the policy.

The first stage in cloud security implementation is to develop a high-level organisational policy supported by appropriate lower-level policies. The

next step is scoping – ie, defining which parts of the organisation will be covered by the IMIS and the location, assets and technologies to be included.

“Putting the correct security standards and protocols in place is not the only aspect of security. Identity protection is also important and it is vital that users maintain security standards through, for example, not sharing passwords”

A risk assessment should then be undertaken to determine the organisation’s risk profile and identify how these risks will be managed, including the selection of appropriate controls with respect to those outlined in the standard. The justification for each decision should be recorded in a Statement of Applicability (SOA). Once the controls have been implemented, the organisation can apply for certification to the appropriate standard.

Levels of security

Putting the correct security standards and protocols in place is not the only aspect of security. Identity protection is also important and it is vital that users maintain security standards through, for example, not sharing passwords.

There are several levels of security:

1. User identification – am I who I say I am?
2. Device authentication – one of the advantages of private cloud is that, as the organisation will be supporting a known user community, device authentication can be controlled by network access control. Every element of the connection between a client device and delivery platform can be secured using 128-bit or higher encryption. If properly designed, two-factor and biometric authentication methods should be fully supported.
3. Data security – the organisation needs to ensure that no-one else can get hold of its data, that it is secure, backed up, resilient and there are multiple copies etc. It may decide that some

data will never leave the organisation's premises and has to be held internally under specific security classifications. One of the key advantages of using private cloud to deliver a virtualised desktop environment is that no data ever leaves the datacentre unless the organisation's security policy specifically allows mapping of local drives, USB memory sticks or other external storage. Also, with private clouds, the existing user directory infrastructure can be reused, saving time and configuration effort (most public cloud services require this to be recreated from scratch).

4. Information security – the value of data may not be in the individual items of information themselves but in making the links between them, thus using the data to gain insights. For example, the recently published spending data from various government departments states that transactions have been made but not the application or purpose of the items, so are inherently of much lower value than if the context of each decision had been made. How to manage and secure the links should also be addressed by the information security policy.

The dangers with the cloud

Moving to the cloud, whether hybrid or public, does not negate the need to take proper security precautions. If an organisation is asking a service provider to implement this for it, it still has to take responsibility for asking the provider to deliver the appropriate levels of information security and to measure and audit the supplier to ensure that the relevant security is applied.

Before moving any data to the public cloud, there is a number of questions that organisations should ask their service providers:

- Who is the ultimate holder of the data?
- Where is the data held? This may be particularly important if the data needs to comply with Safe Harbour principles on the protection of personal data.

- Do you operate good processes and can you prove it?
- What specific security standards and levels of security are you applying to my data?
- How can you guarantee that no-one else can get access to my data unless I specifically want them to?

Organisations should check all of the information for themselves and manage it as they would for every corporate risk.

“On the positive side, most good service providers would not want to skip on quality and would take all the appropriate steps to avoid data loss or breach, as their reputation is at stake”

On the positive side, most good service providers would not want to skip on quality and would take all the appropriate steps to avoid data loss or breach, as their reputation is at stake. We are currently in the early days of cloud adoption, so any problems in this area that are widely reported would be even more damaging now than they would be if cloud was already an accepted and widely used service.

How to get to the private cloud

The high-level actions most organisations will need to take to get to an initially private or hybrid cloud, and potentially public cloud in future, are as follows:

1. Understand what services your business requires from your IT function. Define your service catalogue based on this.
2. Review the required service levels needed for each of the defined services: include resilience and data security.
3. Define and agree the services you want to provide internally and those that can be hosted or provided by a third party.
4. Measure the current resources you need to deliver the internally provided services to the required service levels.

5. Review your current infrastructure and look for all opportunities to simplify, rationalise and standardise what you support and how you manage it.
6. Find suitable public cloud services providers for the services you believe can be hosted externally.
7. Virtualise every element where you have not already done so and where it is technically and commercially appropriate to do so. This includes desktops.
8. Implement a common user portal where all users access all services, whether provided internally or by a third party.
9. Refine and improve your operational processes to take advantage of the new environment.
10. Implement suitable internal charging mechanisms so all users/departments can understand the costs of the services they are using.
11. Review the cost of internal service provision against what commercial cloud providers can offer for the same level of service.
12. If commercial cloud providers can offer the same service more cost effectively with appropriate risk mitigation and guarantees, then look to migrate the service to their cloud platform.
13. Monitor every service provided, whether delivered in-house or externally, to ensure it meets agreed service levels.
14. If commercial cloud service providers cannot meet required service levels or costs in future, move service to another provider or bring the data back into your private cloud.

About the author

Richard Blandford founded Fordway in 1990 a provider of IT infrastructure change in the UK. An ex-technician, Blandford has over 20 years' experience in helping organisations of all sizes and across all industry sectors define, design, implement and optimise core ICT infrastructure, offering vendor-independent advice and guidance. He regularly speaks at conferences on infrastructure change and other industry issues.

Learning to love SIEM

Steve Jenkins, Q1 Labs

In the 1964 motion picture, *Dr Strangelove or: How I Learned to Stop Worrying and Love the Bomb*, a paranoid general played by Sterling Hayden is able to hack into a system and initiate a nuclear attack on the Soviet Union without the knowledge of his superiors.

The classic Cold War film, featuring cinema's earliest example of an IT security breach, would be viewed as impossible within a modern system of checks and balances. However, the often strategic importance of IT, especially to governmental agencies, has prompted a tightening of regulatory requirements around security. The fear, in both the public and private sectors, is about the potential for breaches that lead to significant financial damage and widespread embarrassment. And this is eroding confidence in switching to lower-cost Internet-based and cloud services.

Incidents such as Stuxnet, which was an attempt to tamper with both the computers and infrastructure controlling elements of Iran's nuclear programme, are touted as examples of state-sponsored cyber-warfare that is on the increase. Headline-making internal breaches leading to leaking of sensitive data – such as the Wikileaks 'Cablegate' affair – has been cited as an IT security failure, although the reality was that an authorised person stole confidential data. This could be seen as a failure of policy or even physical security protocols, but the end result is still more concern over data security. These kinds of examples provide European regulators with more ammunition to persuade the politicians to get tough on IT, much like their US counterparts.

Around the world, organisations are using technology and the pervasiveness of the Internet to open up systems to partners, customers and the wider general public. But this highly interconnected society that we are heading

towards is ever more difficult to secure, in what some experts term the 'post-perimeter world'.

Setting the benchmark

If modern IT security regulation had a role model it would probably be the Payment Card Industry Data Security Standard (PCI DSS). It is widely adhered to and affects in varying degrees any organisation handling credit card payments. How much it has helped to reduce card crime over the past five years is difficult to gauge. However, the UK Cards Association reported fraud on UK credit and debit cards in 2010 was at its lowest level since 2000 – a 17% reduction on 2009 figures, to £365.4m. There has also been a 15% reduction in card-not-present (CNP) fraud, which is essentially criminals using stolen card details fraudulently over the Internet, phone or by mail order. However, some of this reduction could be a result of more use of chip and PIN and equivalent online, two-factor authentication systems.

"The PCI authorities understood that if a breach occurred they needed to know the mechanism to make sure it didn't happen again and maybe also apportion blame"

Putting aside its fraud-fighting abilities, PCI DSS has set the benchmark and raised the profile of IT security compliance across the world. In another recent survey, InsightExpress ques-



Steve Jenkins

tioned 500 information technology decision-makers and found that 70% of respondents felt that their organisation was more secure than it would otherwise be if PCI compliance were not required.

The standard has evolved over the past five years and undergone revisions to deal with new areas such as hosting and cloud, as well as embracing areas such as anti-malware and other forms of end-point security. Auditing is one the areas that has undergone further clarification in the latest revision of the standard.

On the audit trail

PCI DSS was initially founded to help the big credit card companies fight fraud and theft. The central tenet was that any organisation that handled credit card data needed to have a credible level of security that could be checked by independent assessors. But as pragmatists, the PCI authorities understood that if a breach occurred they needed to know the mechanism to make sure it didn't happen again and maybe also apportion blame. So the new clarification states that audit logs must be retained for at least one year, with a minimum of three months available online.

This long-term audit requirement is starting to spread from PCI to other regulatory frameworks such as the Gramm-Leach-Bliley Act (GLBA), Sarbanes-Oxley (SOX) and the Health Insurance Portability and Accountability Act (HIPAA). These all have elements that require affected organisations to be

able to provide logs across a myriad of different systems. These well-known, and mostly US-based, compliance rules are joined by other regional or national guidelines that are equally onerous. For example, the Italian Data Protection Act has elements concerning how personal data must be stored and accessed as well as audit requirements. In the UK, the Information Commissioner's Office (ICO) can impose fines for data breaches due to negligence while the Communications and Electronic Security Group (CESG) is pressing for its Good Practice Guide 13 (GPG 13) to become mandatory for organisations involved in UK government business, including government departments, public organisations and indeed service providers and outsourcing companies. In France, Autorité de Regulation des Jeux en Ligne (ARJEL) is a regulator for online gaming that will only issue a licence for firms with proper IT security in place. Germany has additional rules around financial services while a new EU rule will force communication carriers to notify authorities if they are victim to a security breach.

"With so many rules and jurisdictions, the notion that any one security product or innovative appliance can make a company instantly compliant is ludicrous. All compliance frameworks are based on policy"

Compliance works?

With so many rules and jurisdictions, the notion that any one security product or innovative appliance can make a company instantly compliant is ludicrous. All compliance frameworks are based on policy. While tools such as firewalls, Network Access Control

(NAC), or intrusion detection or protection systems can provide a certain level of protection, organisations are turning to Security Information and Event Management (SIEM) to help understand the current processes and flows to allow them to adopt and monitor policies to meet compliance frameworks.

'Total information' is, in many ways, the most important element of meeting compliance. Organisations need to first understand what is going on across the hundreds of applications and many thousands of users, partners and customers, all with different roles within a distributed organisation. In the world of compliance, there are no small businesses, as regulations such as PCI DSS cover anything touched by the credit card and all affected organisations must be fully compliant. But building a compliance process is almost impossible without clear visibility. A strategic plan to achieve compliance should include enterprise-wide visibility, which can then be achieved to deploy security intelligence to address insider threats, cyber-espionage and many other potential breaches that are faced in the post-perimeter world.

Jumping through hoops

For anybody shuddering at the prospect of having to jump through the hoops of another regulatory audit or compliance process, it is worth noting that PCI seems to have a direct impact on the likelihood of a successful cyber-attack. In the highly respected 2010 Verizon Data Breach Investigations Report, which collates the case files of thousands of organisations that have had an IT breach, as well information from the US Secret Service, 79% of victims subject to the PCI DSS standard hadn't achieved compliance prior

to the breach. Another key finding of the report is that almost all victims have evidence of the breach somewhere in their logs.

It doesn't take much to figure out that something is amiss and changes are needed. The authors of the Verizon report said that organisations should make time to review more thoroughly any batch-processed data and to analyse logs. "Make sure there are enough people, adequate tools and sufficient processes in place to recognise and respond to anomalies," they said.


"As compliance moves from best practice to mandatory across Europe, putting your head in the sand is no longer an option"

Regulations are likely to tighten further as governments start moving more paper-based processes online and interact electronically with suppliers to transact and deliver services. A key consideration is around frameworks. As organisations build processes to meet PCI or SOX or anything else, tools such as SIEM can be used to meet the next regulatory challenge with less difficulty.

In the end, it's better not to fight against compliance, but to embrace it – most firms probably don't have a choice anyway. As compliance moves from best practice to mandatory across Europe, putting your head in the sand is no longer an option.


About the author

Steve Jenkins, VP, EMEA of Q1 Labs (www.q1labs.com), has over 20 years experience within the industry at leading technology companies, including Isilon Systems, F5 Networks, Nortel Networks, Bay Networks and Wellfleet. Q1 Labs is a global provider of next-generation security intelligence products.



A SUBSCRIPTION INCLUDES:

- 12 printed issues
- Free Delivery
- Online access for 5 users
- An archive of back issues


www.networksecuritynewsletter.com

Continued from page 2...

The Ponemon report is available here: <<http://aa-download.avg.com/filedir/other/Smartphone.pdf>>.

In Europe, Kaspersky Lab, via the Association of Independent Research Centres, polled 1,600 smartphone users in the UK, France, Italy and Spain to see if they were aware of smartphone threats. The answer, for the most part, was 'no'. In spite of a fifth of all smartphone users having experienced the loss or theft of a device, most still consider them to be safer than a PC. The vast majority of users (over 90%) store personal data on their smartphones – such as photos, emails or contact details. Around a third also carry login credentials, including passwords and PIN codes on the devices. All this comes against a backdrop of increasing threats against smartphone platforms. And we can expect a lot more of these, the Kaspersky report claims.

This view is supported by Panda Security. In its Q1 2011 malware report, the firm notes a steep rise in smartphone exploits. Rogue applications on the Android platform played a large part in this – an issue that has been only partially addressed. But Panda also notes that smartphone sales are now outstripping those of PCs, making these platforms much more attractive for malware writers.

Cyber-criminals appear to be trying out a number of techniques. And the same is true of researchers – the number of proof-of-concept exploits for smartphones has increased dramatically over the past few months, says Panda.

The report is fairly critical of the Android platform's lack of vetting for apps. It notes that recent malware, such as Trj/ADRD.A, was spread through 'alternative' app stores. Unlike Apple's iOS platform, there is no attempt to limit users to downloading via official channels. That said, more than 50 apps recently had to be removed from Google's own Android Market because they contained malware.

The Panda Security report is available here: <<http://pandalabs.pandasecurity.com/pandalabs-quarterly-report-q1-2011>>.

Utilities still under threat

In spite of the high profile given to Stuxnet, utility companies using Supervisory Control and Data Acquisition (SCADA) systems remain vulnerable to attack, according to work by security researchers and a report from the Ponemon Institute.

Italian researcher Luigi Auriemma found 34 flaws in SCADA systems from Siemens, Iconics, 7-Technologies and Datac, which he posted on his website and vulnerability site Bugtraq. All of these vulnerabilities can be exploited remotely if the systems are connected to the Internet. The potential exploits range from reading files, through crashing systems to remotely executing code. Auriemma's revelations led to US CERT's Industrial Control Systems team issuing four alerts.

One of the affected systems is Siemens' Tecnomatix FactoryLink, used in the food, pharmaceutical and metals industries, among others. Four years ago, Siemens began withdrawing FactoryLink and pushing customers towards its WinCC product. However, tens of thousands of FactoryLink systems were installed and many remain in operation.

Datac has denied that the vulnerability demonstrated in its RealWin systems is a genuine threat, because that product is used primarily for demonstration purposes. And 7-Technologies said it was issuing patches to fix the flaws in its product.

Meanwhile, other security specialists claimed to have found flaws in software often used with SCADA systems: Ruben Santamarta published code he says demonstrates a flaw in virtualisation software WebAccess, from Broadwin. And ICS-CERT found a SQL injection vulnerability in IntegraXor from Ecava.

Russian security firm Gleg has released Agora SCADA+, a single exploit pack that it says includes almost all known SCADA vulnerabilities, including 11 zero-day examples.

A Ponemon Institute report for Q1 Labs, 'State of IT Security: Study of Utilities & Energy Companies' found that 75% of these firms had suffered an IT security breach in the past year, and a lack of priority given to security means it's not going to get better any time soon.

EVENTS CALENDAR

3–12 May 2011
SANS Security West 2011

San Diego, California, US
Website: <http://bit.ly/ifP1F2>

9 May 2011
Secure Coding: major web attacks and how to defeat them

Rome, Italy
Website: <http://bit.ly/fzoBQF>

9 May 2011
SANS Secure Europe

Amsterdam, Netherlands
Website: www.sans.org/info/70708

9 May 2011
SANS Brisbane 2011

Brisbane, Australia
Website: www.sans.org/info/70819

10 May 2011
Cyber Security Strategies summit

Washington DC, US
Website: <http://cybersecuritystrategies-summit.com>

12 May 2011
Developing Secure Applications for the i-Phone

Rome, Italy
Website: <http://bit.ly/gtsxh7>

15 May 2011
SANS Cyber Guardian 2011

Baltimore, US
Website: <http://www.sans.org/info/70944>

16–19 May 2011
IFSEC

Birmingham, UK
Website: www.ifsec.co.uk

6–10 June 2011
OWASP AppSecEU2011

Dublin, Ireland
Website: www.owasp.org/index.php/AppSecEU2011