ELSEVIER

www.compseconline.com

NETWORK Security

March 2005 **ISSN 1353-4858**

Featured this month

CA exposure provokes disclosure debate

Cath Everett

The discovery of multiple serious vulnerabilities in Computer Associates' enterprise license management software has re-ignited the debate over the ethics of disclosure.

The holes, which were made public by security companies, eEye Digital Security and iDefense, at the start of March, are found in versions 1.53 to 1.61.8 of CA's License Client and Server applications that run on most widely available operating systems, ranging from Windows to Unix.

This software enables customers to register, manage and track their licenses over the network and is installed by default in most of the vendor's products. While the server element is generally disabled, the same is not true of the client portion, so as Firas Raouf, chief operating officer of eEye, points out: "It's a big deal from an enterprise standpoint." Turn to page 2...

Goodbye passwords?

Computer systems face continually evolving threats but one bugbear that just won't go away is the vulnerabilities that arise through using passwords for authentication.

Passwords have haunted infosecurity professionals since before 1979 and yet they still appear without fail in the SANs list of critical vulnerabilities year after year. In fact Bill Gates is so aghast at passwords that he relegated them to history in his speech at the RSA conference in February. But despite Gate's wishes passwords are unlikely to disappear in the foreseeable future. In many cases a risk assessment may genuinely suggest that the adverse impacts of moving to alternative methods would outweigh those likely to result from password misuse. But it is also fair to say that the continued reliance on passwords could be due to the inertia of some organizations to introduce other methods. Turn to page 8...

Ten steps to business continuity

Bank of America said it lost customer data tapes in February on transit to a backup storage site. The fact that reportedly 1.2 million US Government employee's details were on the tapes has landed the bank in deep water. Although it said that the investigation has found no evidence that the tapes or their content have been accessed or misused, the bank could maybe lose its customer. The Bank of America Incident shows how business continuity steps can go very wrong. Business continuity is critical to an organization's ability to recover from a denial-of-service incident but the plan should be carefully throught through so it doesn't generate an incident! Turn to page 14...

Contents

NEWS

CA exposure provokes disclosure debate 1

US election-voting systems blamed for Bush win 3

Ivy League schools bar wanna-B students 3

Close shave for Japanese bank 4

FEATURES

URL threats

Dangerous urls: Unicode & IDN 5

Getting budget

Building security credibility 6

Passwords

Authenticating ourselves - will we ever escape the password? 8

Business continuity

Keeping your data available in 10 steps 14

Trojans

Trojans & spyware - an electronic achilles 17

Mobile data location

Mobile phone tracking threatens privacy 19

REGULARS

News in brief 3,4

Events 20

ISSN 1353-4858/05 © 2005 Elsevier Ltd. All rights reserved

This journal and the individual contributions contained in it are protected under copyright by Elsevier Ltd, and the following terms and conditions apply to their use:

Photocopying

Single photocopies of single articles may be made for personal use as allowed by national copyright laws. Permission of the publisher and payment of a fee is required for all other photocopying, including multiple or systematic copying, copying for advertising or promotional purposes, resale, and all forms of document delivery. Special rates are available for educational institutions that wish to make photocopies for non-profit educational classroom use.

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

Editor: Sarah Hilley

Supporting Editor: Ian Grant

Senior Editor: Sarah Gordon

International Editoral 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, California University, Berkeley Lab; Eugene Spafford, Purdue University; Winn Schwartau, Inter.Pact

Production/Design Controller:
Esther Ibbotson

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, e-mail: permissions@elsevier. com. You may also contact Global Rights directly through Elsevier's home page (http://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) 7508400, fax: (+1) (978) 7504744, and in the UK through the Copyright Licensing Agency Rapid Clearance Service (CLARCS), 90 Tottenham Court Road, London W1P 0LP, UK; phone: (+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 articles 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 e-mail addresses noted above.

Notice
No responsibility is assumed by the Publisher for any injury and/or damage 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.

02158
Printed by
Mayfield Press (Oxford) LImited

CA exposure provokes disclosure debate

...continued from page 1

In fact, Simon Perry, CA's vice president of security strategy, gives the vulnerability a seven out of ten rating in terms of seriousness and recommends that customers patch their applications as soon as possible. This is especially crucial because as many as six exploits are now available, appearing only days after the vulnerability was announced.

Such exploits enable malicious individuals to gain control of an affected system remotely, which means that they can install a back door or attack it using malware such as worms, although no such incidents have been reported to date.

The first of this exploit code was released by an organization called the Hat Squad, which describes itself on its website as providing digital security services such as penetration testing, technical training and consultancy.

But it is the release of this exploit code that generates the most fevered debate over the ethics of disclosure, although most commentators agree that there are many grey areas along the spectrum of partial to full information-sharing.

For example, Raouf takes the view that organizations such as his own are performing a service to the industry by undertaking partial disclosure. Because they alert vendors to any holes in their software before announcing them publicly to give suppliers time to come up with patches, they are the good guys.

"On the exploit side, however, it's a bit of a different story," Raouf says. "Full disclosure purists say you need to know about exploits because it helps security companies develop better protection and helps administrators to better detect whether their systems are safe or not."

But in his opinion, this is "nonsense" as there are currently enough tools and products available on the market to enable administrators to test for vulnerabilities without needing exploit code.

Perry agrees. "To put exploits up as a public service, I don't think is a legitimate business model. It increases the danger and I don't see any positive side. To stand up and say you're providing a public service, you're either kidding yourself or being hypocritical," he says.

But Jay Heiser, vice president and director of research at Gartner, takes the argument a step further.

"The mere fact that a vulnerability is known to exist, even if the details are not published, represents a significant piece of information. It provides a significant clue to the hacker community that if they put some reverse-engineering efforts into the code, they will probably be able to exploit it," he says.

Moreover, he adds, when a patch is published, it provides even more details about the hole. So in his view, "vulnerability disclosure by these so-called researchers has resulted in more harm than good".

Not so, says Gerhard Eschelbeck, chief technology officer and vice president of engineering at vulnerability management company, Qualys. "You have to make the assumption that the bad guys have the information anyway so releasing information levels the playing field between the good and bad guys. What's not appropriate, however, is to release exploit code before patches are available," he says.

As to what organizations can do to protect themselves more effectively, there are various options. The first thing is to establish exactly what software inventory is on the network and how well or not it is patched, before even attempting to undertake regular vulnerability assessment and remediation using one of the many tools on the market.

According to Perry, standardizing on a smaller number of vendors can also be useful because "if you've got a very splintered environment, it can be very difficult to understand what you've got where. If you've got 30 vendors, you've probably got 20 to 25 too many," he advises.

The next stage after vulnerability assessment is to ensure that patching activities are automated as much as possible and are up-to-date and verified.

While Eschelbeck acknowledges that patching everything constantly is impossible, he says that Mitre's new universal scoring system, which was released to vendors a few weeks ago at the RSA conference, should make prioritisation easier.

The aim of the Open Vulnerability Assessment Language initiative, as it was formerly known, was to provide a standardised way for the industry to define vulnerabilities and their seriousness and widespread industry adoption is expected to follow over the coming year.

As for applications that can help, intrusion prevention systems are useful, but a number of start-ups in the US are also developing virtual patching offerings. According to Eschelback, while such software is at least three years away from commercial release, it works by virtualising a patch as soon as it becomes aware of a hole.

"The box is aware of vulnerabilities so it can catch any potential exploits that are targeting the server. It prevents them hitting vulnerable systems by modifying the sequence of attacks so they don't have any impact. It doesn't completely eliminate the need for patching, but it's a good stop gap," he concludes.

US election-voting systems blamed for Bush win

Possible to hack from the inside, they say...

The wife of defeated US Democrat candidate, John Kerry, claimed that hackers could have swayed the outcome of last year's US presidential election. "It is very easy to hack into the mother machines," said Teresa Heinz Kerry, as reported in the Seattle Post-Intelligencer last week.

Teresa Heinz Kerry also pointed out that two brothers, who are strong Republican supporters own 80% of all the voting machines in the US.

One of the brothers, Bob Urosevich, is president of Diebold Election Systems and the other, Todd Urosevich, is vice president of customer support at ES&S.

Dr Gene Schultz, an IT security expert at University of California-Berkeley Lab said, "The president of Diebold has made no secret of his strong support of the Bush Administration."

Schultz added that insider manipulation of voting machines is more likely than remote hacking. "The people element weighs far more heavily in the potential for voting system fraud than do technical vulnerabilities. Remote access to them is severely or completely restricted. It would be far easier for someone with direct physical access to these systems to engage in wrongdoing."

Schultz questions why errors discovered in voting system tallies last November uniformly supported Bush, and why do states such as Florida refuse to pass legislation or adopt measures that would require adequate security in voting systems? "A case for conspiracy could be made," he said.

In addition critics have cited the lack of paper audit trails also as a concern. "National legislation requiring voting systems to meet certain security standards and also to provide paper audit trails is inevitable sooner or later," said Schultz.

"In the meantime the opportunity for fraud in elections in which voting systems are used abounds."

At the end of the election campaign, three Democratic members of the House of Representatives requested that the Government Accountability Office (GAO) review the voting systems.

Wayne Madsen contributed to this report.

Ivy League schools bar wanna-B students

Several top US business schools will reject would-be students who used a hacked admissions decision system to check their application status. The schools include Harvard Business School, MIT's Sloan School of Management, Dartmouth College, Duke University and Stanford University.

A hacker called "brookbond" cracked the online application and decision system at ApplyYourself, a hosting service used by some 400 colleges and universities to manage admissions, and posted instructions on how students could get information about their applications.

In brief

Cyberwar test coming

The US Government plans to test defences against direct or indirect attacks on the computer networks that control the nation's critical infrastructure such as power plants and oil pipelines, says Hun Kim, deputy director of the National Cyber Security Division at the Department of Homeland Security.

Security expert Rick Wilson says a "cyber winter" caused by a massive denial-of-service attack on critical routers and servers is unlikely. He believes attackers will try to stay invisible, but undermine confidence in the data sent between parties.

Tora, tora, tora*

Hackers successfully mounted denial-of-service attacks on websites for the offices of Japan's Prime Minister and the Cabinet. There was no permanent damage, officials said.*Signal to attack Pearl Harbour.

Brits launch virus alerts for SoHo users

The UK government is to provide free security alerts to home and small business computer users via a new website, ITsafe, run by the National Infrastructure Security Co-ordination Centre (NISCC). The Home Office said it will also offer advice on protecting personal data, but not patches or prophylactic software. It expects to issue six to 10 alerts each year.

Firefox hits 25m in 100 days

More than 25 million users downloaded the open source Web browser Firefox in 100-odd days from release, said the developer, Mozilla. Firefox now has a market share of about 5% compared to Internet Explorer's 93%. Industry analysts reckon users are switching because of their concerns with IE's lack of security.

MSN's IM spreads Bropia and Kelvir worms

Antivirus companies say new versions of the Bropia and Kelvir worms are spreading via the instant message service of Microsoft's MSN Messenger application. They also fear a new family of worms, dubbed "Sumom" or "Serflog," which is spreading over MSN.

IM worms have been gaining popularity among virus writers because of IM's ability to disseminate malicious code quickly, says an anti-virus expert. The Stang and Aimdes viruses spread over AOL's Instant Messenger network.

In brief

Fine for Frenchman's exploit

A Paris court found Harvard University researcher Guillaume Tena guilty of publishing a vulnerability and a proof of concept virus for Tegam's Viguard anti-virus product on his website. He received a Euro 5,000 suspended fine.

French-born Tena highlighted holes in the French anti-virus product and justified his actions in an online diary. Tegam is now pursuing a Euro 900,000 civil case against Tena.

T-Mobile admit hackability

It is possible to access and download a person's voicemail messages or change their voicemail settings with a simple hack, T-Mobile have acknowledged.

The hack can be done simply if the hacker knows the phone number of the account. It is simple to avoid - simply put a password on the voicemail account. At the moment this is not a requirement for customers.

No patch is good news?

After last month's mammoth security bulletin, Microsoft announced that there would be no security update or patches this month.

This is the first time since December 2003 that a month has passed without an update supplied to users of Windows.

Nuclear security suppliers say no

Two producers of digital systems used in nuclear power plants have denounced a US Government proposal to enforce security standards to plant safety systems.

The proposal, by the US Nuclear Regulatory Commission, rewrites existing criteria which date from 1996. The two firms, Capri Technology and Framatone claim that the new proposal is too premature and broad to be truly comprehensive for the nature of their work.

Massive point drop for Choicepoint

Shares in Choicepoint dropped by 20% after it was revealed that identity thieves had stolen information from the data vendor.

A class action lawsuit against the company and its lead executives has now been filed in California on behalf of those shareowners affected by the drop in price.

Security build up for BlackBerry

The Canadian military and US security agencies are working together on a year long trial to make BlackBerry devices more secure, with a view for using them in top secret communications.

The devices have been incredibly popular in the business community, enabling the user to be contactable at all times and earning the nickname 'CrackBerry' due to their addictive nature. However, hacking of the devices has recently become more common and the main focus of the trial is to improve security of transmissions.

ID theft gang caught

Twenty-eight people have been charged with perpetrating an online fraud scam that is responsible for the theft of £2 million. Scottish police raided over 40 addresses after months of investigations. It is thought that the gang used simple tricks such as stealing thrown away documents and watching people type in PIN numbers as well as phishing.

Bank loses tapes for 1.2m workers

US senators and federal workers could have their identities stolen following the alleged theft from the Bank of America of computer data tapes with the personal information of 1.2 million government staff. The lost data include social security numbers and account information for a government credit card programme.

Patrick Leahy, one of the senators whose data was on the tapes, has led calls for a Senate inquiry into the need for more regulation of companies that buy and sell personal data.

Gumshoes track shoe shopper ID thieves

The US Secret Service is hunting hackers who stole the credit card and sales data of customers at 103 of 175 DSW Shoe Warehouse stores owned by Columbus, Ohio-based, Retail Ventures. The firm said the data was stolen over the past three months, but didn't know how many customers were affected.

Singapore to spend $23m on cyberdefence

The Singapore Government is to spend S$38 million (US$23.2 million) on a three-year scheme to make the island state safe from cyber attacks. One in two Singaporeans uses the Internet, and the World Economic Forum rates the island as the world's top IT nation.

Singapore's deputy prime minister, Tony Tan, said the Infocomm Security Masterplan will develop the manpower to manage rising online threats and set up an early warning system for cyber attacks.

The plan is to go live in 18 months, providing 24x7 tracking and analysis of threats such as computer worms and viruses, phishing scams and hacking attempts.

Close shave for Japanese bank

Brian McKenna

Israeli police have foiled an attempt to defraud Sumitomo’s City offices of £13.9m. They arrested a man who tried to benefit from information got from keylogging software. Yeron Bolondi, 32, is charged with money laundering and deception.

Meanwhile, the UK payments body APACS has released online fraud figures for the first time. These show that losses due to phishing and key-logging trojans in 2004 amounted to £12m — less than the Israeli's alleged attempted fund transfer.

The *Financial Times* broke the Sumitomo story on 17 March, reporting that rumours of an £220m attempted theft have been circulating in police and corporate circles since late last year.

Takashi Morita, head of communications at Sumitomo in Tokyo, said the company had not suffered any financial loss as a consequence of the robbery attempt.

He said: "The case is still in the middle of investigation so we cannot comment further.

The UK’s National Hi-Tech Crime Unit, which works closely with the Israeli police, has been credited by the BBC with the original discovery of a wider plot.

The IT security supplier community was fast to comment.

Symantec’s Richard Archdeacon said: “We have seen a meteoric rise in cyber fraud that specifically targets confidential data. It’s information warfare”.

Computer Associates’ Simon Perry said: "The use of keystroke logging software in this case, sends a strong message to all companies that anti-spyware technology is now a first line defence against cyber-crime”. CA said, in a statement, that this was 'the first recorded instance in the UK of key-logging being used for large-scale online theft'.

Dangerous urls: Unicode & IDN

Bruce Potter

The advent of Unicode representations of URLS means security experts have their work cut out for them.

The idea of a Universal Resource Locator (URL) is relatively straightforward. A single data string represents the location of any piece of information on the Internet. Starting with the protocol, followed by the hostname, and finally the path to the information, a URL is in theory an unambiguous reference to data, and one that has worked fairly well for years.

Unfortunately, several developments in the way programs and humans read and understand URLs have complicated matters. A URL string seems simple to decompose and understand, but new features and capabilities in standards, Web browsers, and Web content have made URLs a weapon for attackers.

Multiple hex encoding

In the definition of a URL there are reserved characters such as the dollar sign ($) and the at sign (@). But because these characters may be used in an unreserved part of a URL, they need to be passed to and from the web server using a special mechanism. The mechanism for sending reserved characters is to use a percent sign and the hex value for the ASCII representation. So a dollar sign becomes %24. For the sake of simplicity, all characters in a URL that follow the hostname can be encoded like this.

How it works

Applications and security devices parse URL strings and decode the hex encoding before acting on the URL request. Unfortunately, the hex encoding can be applied multiple times. For instance, %24 can be replaced with the hex values for %, 2, and 4. Upon the first pass, the application would decode each value for the three characters. If the application is not able to recognise that the URL is still hex-encoded, then it would pass the URL along to the next part of the application.

Multiple encoding has unfortunate security consequences. If an application or security device tries to validate input (i.e. ensure that only legitimate characters are passed to the application) and it cannot handle multiple hex encodings, attacks may get through.

For instance, applications often check for the ../ combination of characters when they try to prevent attacks from access files outside the Web server's file system (e.g. ../../../../etc/passwd). In a multiple hex-encoded URL, the first inspection and decoding of the URL may indicate that there are no instances of ../. However the second decoding will reveal the malicious URL. This is the secret of the MS01-026 vulnerability in Microsoft's IIS Web server.

Unicode

Unicode is a way of encoding characters beyond what is possible with the highly limited ASCII character set. It was designed to be extensible and handle as many character sets as could be dreamed up. Unfortunately, this extensibility creates problems for applications that have to sanitise URLs for safety.

A character can have multiple representations in Unicode. For instance, a slash can be encoded as %c0%af, %c1%9c, %c1%pc, and other sequences. This makes it even harder to validate Unicode input characters compared to simple hex encoding. In hex encoding attacks, an application simply has to unwrap a URL string enough times so that nothing is hex-encoded anymore. With Unicode, the unwrapping is complicated by the fact that any single character can have multiple representations within a URL. So in order to declare a URL "safe", the application may have to go through some very complicated logic to determine what the URL really represents. This is a difficult task, and again one that IIS initially did not handle well. The Microsoft vulnerability MS00-078 discusses Unicode handling problems within IIS.

IDN

In an effort to make the Internet more usable for non-English speakers, the concept of International Domain Names (IDN) was developed. The basic idea is that a domain name can be represented in the character set of native language, not just the extended Latin alphabet we use today.

While convenient for those using a particular character set, IDN is a security vulnerability for the internet at large. In a paper in 2002 Evgeniy Gabrilovich[1] described how a hostname can be constructed out of multiple character sets to look like a familiar latinate hostname. This ability to use multiple character sets to create many domain names that look the same, dubbed a "homograph" by Gabrilovich, can be used to trick a victim into going to an unintended website. The example Gabrilovich gives involves using a Cyrillic character that looks like a Latin o to register a domain that looks like microsoft.com. An inattentive user would not notice the difference between the two hostnames.

Although IDNs have become popular, the browser and certificate authorities have not addressed the problems posed by homographs. In 2005, Eric Johanson released an advisory that updated the work of Gabrilovich. Johanson took Gabrilovich's paper a step further when he was able to purchase SSL certificates for homograph domains. This undermines the Web user's one true rule of thumb, which is when you are on a secure site, you can look for the lock in the browser and validate the URL in the location window. Unfortunately in this case, a homograph domain with a valid SSL certificate will fool a user as they cannot know that the domain in the location window is comprised of multiple character sets.

Response to Johanson's paper has been mixed. In February the Mozilla Foundation turned off IDN support by default in their main browsers. Other browser manufacturers are still determining their course of action. Several certificate authorities have started to hand-review all IDN certificate requests in an effort to thwart phishing scams.

Parting shot

A URL must be understandable by computers and humans alike. They are supposed to refer uniquely and unambiguously to a single object on the Internet. Unfortunately, problems with browsers, operating systems, and standards can confuse computers and people as to what a URL points to. Attackers can leverage this confusion to launch phishing scams, get access to data they should not have, and even compromise systems. Unfortunately, something as simple as a URL needs to be treated like any other data type on the Internet—dangerous until proven otherwise.

References

[1]http://www.cs.technion.ac.il/~gabr/papers/homograph.html

Building security credibility

Mike Kemp, NGS

Securing your network is good for your organization, but networking to safeguard your security is even more important.

Mike Kemp

As an information security professional or system administrator you probably have had an interest in computing that dates back until you could barely walk. You may have certificates and qualifications peppered throughout your CV.

At the very least you will have a grasp of important concepts and technologies. You will likely know how to configure a router, firewall or intrusion detection system (IDS), and you probably remain concerned about zero day exploits. You're regarded as an expert in your niche and are regularly called in to long meetings to discuss security issues. During these meetings you may start the discussion and watch as eyes begin to glaze, nods become regular, and smiles or frowns (depending on the situation) begin to form.

You get security; you understand its intricacies and foibles, but sometimes you find it hard to convince and engage members of the business management teams. Somehow, they just don't get it, and that's your problem, because they control the security budget, can seem an almost insurmountable task.

This article outlines briefly some of the methods you can use to communicate effectively with those budget holders who do not fully understand the implications of a security breach. And they will aid the development of a strategy to build a sustainable budget dedicated to improving network security.

Unlike network professionals, many senior managers have a limited interest in security. When things break (or are deliberately broken by malicious attackers) then they take an interest, and heads may or may not roll.

Talking up

Many business professionals have neither the time nor the desire to learn anything about security issues, other than that they are protected. Keeping the network and associated assets secure is mainly of concern to harried systems administrators or security professionals, but knowing how to communicate efficiently and effectively with the professionals from other parts of the business is essential to secure not only their interest, but also financial backing for security initiatives.

Although they may be aware (and they should be) of the importance of security and secure practices, turning that awareness into cold, hard, budgeted cash is vital to the long term integrity and security of an enterprise.

Having security-specific knowledge is an admirable asset in any network professional. Even so, it is vital to move beyond its confines. Organizations of all types are seeking to break down traditional hierarchical boundaries that exist between job roles. Whatever your personal views of the validity of this development, more individuals are becoming multi-skilled, usually with a specialization in some area.

An expert knowledge of security and network issues is vital if an organization's infrastructure is to be kept secure; however, having an in-depth knowledge of its business processes, practices and goals can greatly improve the validity and delivery of security solutions. It is crucially important to understand the

> “Know business processes, practices and goals”

architecture, construction, and threats to a network environment.

Know the business

It is equally important to recognize and understand the enterprise that it supports. If you know the business goals and the obstacles to achieving them, particularly profitability goals, making the leap from network security specialist to someone who speaks the same language as management should be that much easier. If when making a case for spending money on security you can show an understanding of your employer's industry and the firm's business goals, it will enhance your credibility and the odds for getting what you want.

The primary goal of most businesses is to make a profit. Even if you don't work for a profit-seeking organization, many not-for- profit groups are equally concerned to control their bottom line. As a network professional you will want to show a clear interest in assisting your enterprise to remain within budget, or to enhance profit.

This is where knowledge of a simple equation is greatly beneficial. Every activity of an organization (including network security) exists to make a profit or to avoid a loss. Although reducing enterprise risk is laudable from a security perspective, the great disadvantage is that sometimes it can greatly increase business cost.

Risk management

Risk management plays a vital role in any enterprise, and network security can help to reduce risk to a level that is commensurate with a cost the enterprise can accept. Network security does not exist in a vacuum. It is essential to identify the risks that the enterprise's network is exposed to, and to develop a way to address them that meets the specific requirements of your enterprise.

Knowing the enterprise's requirements means you can make a case for suitable security policies and purchases with far greater effect. Blinding non-IT managers with technological science cuts little ice with them. It may seem common sense to justify the purchase of a new piece of kit in terms of its exciting new features and functionality. But if instead you can show how these features help to reduce risk, protect vital data, reduce costs, and release resources for more enterprise specific issues, the holders of the purse strings will more likely to accept your proposals.

The integration of network security with enterprise goals and processes can be a delicate balancing act. It is easier to achieve with the help of others in the enterprise. If you can get your business colleagues on your side prior to budget decisions, they may often go in your favour. That is not to say that your daily habits should include obsequiousness. Far from it. But you should engage users of all levels, especially those who make policy and allocate resources. You will find many simply do not care about security issues, as they are often incredibly dull to outsiders. For example, it has been hard to escape mention of the threats buffer overflows pose, but few non-programmers know what it means.

> “Show a clear interest in assisting your enterprise remain within budget”

Education, education, education

But part of the duties of any network or security professional who cares about their budget should be to educate users concerning such terms, even if it is only informally. The details of the overflow of sectors of memory and jump points may sound dull, but if you can explain the consequences in terms relevant to your business colleagues, you can often pique their interest and win them over on any budgetary concerns that you have.

Developing effective communication channels between all sectors of an enterprise will challenge even the most extrovert of network professionals. But there are some steps that can ease the process. Firstly, it is important to engage all members of an organization in the security process. This does not just mean issuing diktats and policies, but rather taking the time to explain the risks the enterprise faces and how, by working collaboratively, they can be addressed. Provided such explanations fits the requirements of an enterprise and is understood by the majority, the status of security's role in fulfilling the enterprise goals will be considerably elevated.

Bureaucratic ju-jitsu

Another recommended approach is to form a security committee. Although this may sound like bureaucracy for bureaucracy's sake, it can reap big dividends both in relation to increasing security's profile in an enterprise and in the allocation of budgets. Such a committee should include all sectors of the organization particularly network staff, security specialists and executive management from all departments. It is challenging to set up and run such an entity and to keep business colleagues engaged in it. But it can position security as a core requirement of an enterprise's environment.

When considering communications strategies that will develop a sustainable security budget, it is vital to address issues such as return on investment. There are two basic ways to sell security to line managers and executives. The first relies upon the potential for loss, and the second on return on investment. Defining a return on investment in relation to security is contentious, however it is a consideration that most business colleagues will have.

It is painfully simple to sell security in terms of avoiding potential loss; however this is not without a downside. Creating an atmosphere of FUD (fear, uncertainty and doubt) around security can reap dividends in the short term, but in the long term the credibility of those spreading it can suffer. Even though enterprises face levels of risk that rise daily, basing all your arguments on this foundation is not an effective strategy in the long term. It is far more advantageous to explain the threats clearly and simply, and use your expertise as a security professional and your (new) knowledge of the business to qualify and quantify the risks that your organization faces.

Using a flexible classification system that sets out the levels of risk that the enterprise is willing to tolerate will help greatly to build the case for sustainable security spending. Although there are relatively few times when you can prove the hard financial case for security spending, there are exceptions. These include managements systems, which can cut help desk costs.

Even so, wherever possible you should try to make a ROI part of any discussion on security budgets. Provided that you can back up your argument with an unquestionable expertise and credibility, you should have no problems winning your case.

One way to greatly increase your credibility (and indeed your chances of securing funding for new security initiatives) is to go out of your way to build relationships with your business colleagues and decision makers. If you can explain the real risks to the enterprise and vulnerable resources clearly and precisely at the right time, it is often possible to increase the overall security posture of an organization. By developing mutual professional respect and understanding of both enterprise needs and goals, as well as the specifics of security, your credibility can only increase.

Of course these strategies rely on the ability to communicate effectively. This is not to say that one has to develop the easy patter of a snake-oil salesman, indeed far from it. Effective communication comes from understanding the needs and demands of your audience, as well as imparting expert knowledge in a way that is easily understood and appreciated by the decision makers within your organisation.

One critical point to remember is that it will often be necessary to compromise on a range of security related initiatives. Many elements go into developing the successful implementation of a new security initiative, including those contributed by decision makers, end users and indeed technology.

In working towards a compromise, network professionals can ensure that the security levels agreed reflect accurately the company's appetite for risk and reward. This will certainly increase your overall levels of credibility within the organization itself. Although your organization's decision makers may not understand or take an interest in the security threats they face, spelling out the consequences of breaches in business terms will make them far more receptive to new security initiatives.

By positioning risk effectively and relevantly, as well as developing the ability to speak in terms understood by business managers, the beneficial effects on security budgets can be dramatic, even where overall spending is restricted. Demonstrating tangible risks that can be understood and qualified helps your business colleagues become increasingly security aware, and assists your organization to become more effective in combating threats and reducing business risk which, after all, is what being a network or security professional is really all about.

Authenticating ourselves: will we ever escape the password?

Steven Furnell

Steven Furnell

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

Passwords have long been a source of discontent as a means of identification. But they are still being used and the problems associated with them still continue unresolved.

If you take a look at much of the published literature on the matter, it would be fair to say that passwords are not held in the highest regard when it comes to secure and reliable user authentication. Although the concept of a secret shared between the user and the system is fairly straightforward, the protection is often compromised by both the users and owners of systems. Indeed, the fact that passwords can provide less than ideal protection is far from a recent realisation. For example, a 1979 study examined the poor password choices being made by users and discovered that, from a sample of 3,829 passwords, 86% could be guessed by a PC in less than one week.[1] Although many other security issues have arisen to face our systems in the intervening years, it is notable that problems relating to passwords remain conspicuously unsolved. They have, for instance, consistently featured in SANS Institute's list of the most critical security vulnerabilities, including the most recent list from October 2004.[2] Nonetheless, they remain by far the most widely used authentication method. For example, according to the Information Security Breaches Survey 2004 from the UK Department of Trade & Industry, 93% of respondents who indicated how they were authenticating their users were doing so with passwords.[3] So, when we consider the predominance of passwords against all of the products and research that have sought to propose alternatives, we seem to be on a continual journey back to the same place.

> **“93% of authentication processes use passwords”**

This article examines some of the well-recognized problems with passwords and considers why, in spite of these issues, they continue to remain the most common authentication method in our daily lives. It is worth noting at this point that although the title of the article refers to passwords, many of the issues discussed are also relevant to our use of Personal Identification Numbers (PINs), and some of the examples will also make reference to these.

A plethora of passwords – too many secrets?

The fact that passwords and PINs are so widely used has the almost inevitable consequence that many people now make use of multiple systems that require them. A typical business professional, for example, could very likely identify most of the following as devices and objects for which such authentication is required (or at least should be!): office PC, home PC, laptop, PDA, mobile phone, ATM card, credit card. Indeed, being required to authenticate ourselves in most of these cases is not unusual, and the number of passwords linked to such physical artefacts has remained relatively the same over the years. However, it has been accompanied by an explosion of additional logins for websites and other online services. From a personal perspective, I have around twelve password or PIN-protected accounts on various systems and devices that I use on a regular basis (e.g. at least once a week). In addition, my conservative estimate is that I have at least three times this number associated with websites on which I chose (or was obliged) to register, but do not use regularly (and given that I cannot even remember the sites, I would not rate my chances of remembering the passwords!). Of course, this situation is in no way unique. A few years ago a survey was conducted by my research group to investigate the general attitudes and awareness of users towards various authentication technologies.[4] One of the questions asked the respondents to indicate how many systems they used that required passwords for access. The results that we observed (based upon 175 responses) are shown in Figure 1, and it is notable that even then 12% were accessing 10 or more systems. I am confident that this proportion would be significantly larger if we were to repeat the exercise today, and users were specifically asked to take websites into account alongside their access to physical devices.

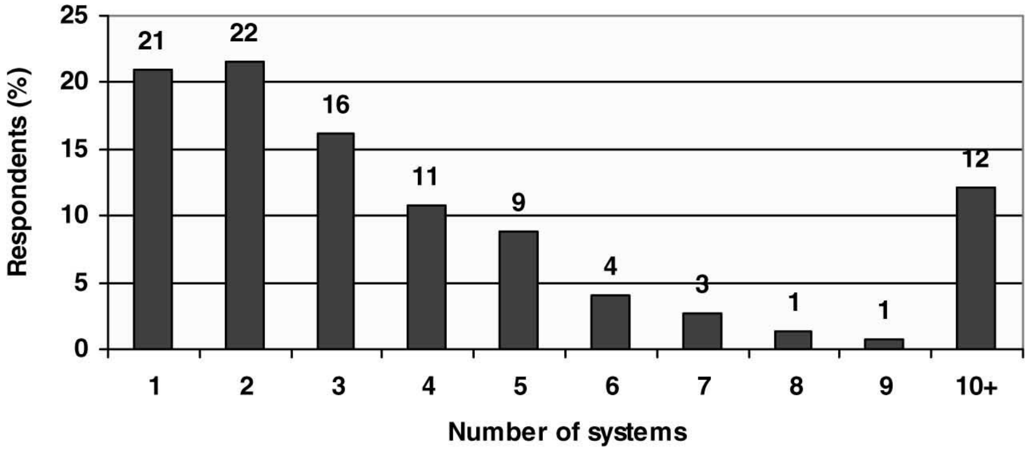
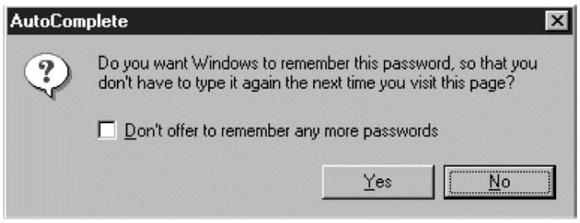


Figure 1: Number of systems requiring password access

Unfortunately, the more passwords we are required to use, the greater the chances that we will not use them properly – and as many readers will already be aware, there a number of well-recognized means by which users can compromise the protection that passwords seek to provide:

- Making poor password choices (e.g. passwords that are too short, based upon dictionary words, related to personal information, etc.), which leave them vulnerable to password cracking tools and social engineering.
- Sharing them with friends and colleagues, such that the supposedly secret knowledge becomes, at best, a shared secret and no longer remains under the control of the legitimate owner (i.e. colleagues may share it with other people, without the original owner's knowledge).
- Writing the information down (the stories of post-it notes stuck on monitors or underneath keyboards are no exaggeration in many cases).
- Sticking with the same password for long periods, thus increasing the window of opportunity for an impostor in the event of the password being discovered (or having previously been shared).
- Using the same password on multiple systems, with the consequence that a breach on one system potentially renders the others vulnerable.

Although system-level controls can often be used to guard against a number of these (e.g. prevention of short passwords, use of password ageing to enforce regular changes), others are pretty much down to the user. Unfortunately, this is where many of the weaknesses are compounded. Not only do users have problems following the good practice, but they also have a tendency to deliberately misuse the techniques when the opportunity arises. For example, another finding from the aforementioned survey was that 21% of respondents had used another person's password without their knowledge or consent.



Do you want Windows to remember this password, so that you don't have to type it again the next time you visit this page?

□ Don't offer to remember any more passwords

Figure 2: An invitation to weaken protection?

Of course, in an organizational context, concerted efforts can be made to promote password policies and good practice as part of a security culture. However, achieving good practice may be much easier said than done – and not just because the advice often falls upon deaf ears. For example, if you follow all of the recommended practices, passwords quickly become unmanageable (e.g. if you choose strong passwords, have a different one for each system, and change them all regularly, then the likelihood is that you will have to write them down to avoid forgetting things). As a result, most people are likely to recognise at least one of the elements of bad practice in their own behaviour. However, rather than being off-putting, we seem to find it reassuring (i.e. a 'safety in numbers' mentality), and the realisation that everyone else is just as bad as us effectively contributes to the maintenance of the status quo.

Keeping track of the secrets

From a usability perspective, our fundamental difficulty with passwords is that we have a problem remembering them, and this is clearly amplified if we have many of them to deal with. As a result, various solutions seek to overcome this overload by making things easier to remember, or by avoiding the need for us to remember things at all. Looking at the latter case first, it is possible to identify a case in which, rather than enforcing good password practice, our system may actually play a part in undermining the method. Consider, for example, the Windows dialogue box in Figure 2. Although the aim here is clearly to make life easier for the user, it also serves to compromise the level of protection that the password would otherwise provide. The security of the user's account on the associated site then becomes tied to the login authentication method being used on their PC.

In the extreme, the repeated offers to remember all of your passwords could result in all of your access effectively being dependent upon a single login. In actual fact, this is the exact principle behind one technique that has emerged as a potential solution to the problem of identity management and authentication within the enterprise – namely Single Sign-On (SSO). SSO can be formally defined as "any user authentication system permitting users to access multiple data sources through a single point of entry."[5] This clearly helps to combat the problem of password overload, and therefore makes it easier to encourage good practice amongst users, because they only have a single authentication method to worry about. However, it also relies very much upon organizations to use it sensibly, because if it is simply used to replace all logins with a single password then it is effectively weakening security - because a breach would then allow access to all systems that an individual is authorized to use. The expectation would therefore be for SSO to be achieved via a stronger method of authentication in the first instance (e.g. a two-factor approach involving tokens or biometrics rather than just secret knowledge). However, the 2004 DTI security breaches survey determined that businesses were often using SSO without this, and had therefore experienced an increased incidence of breaches as a consequence.[6]

Additionally, while an appropriate method of SSO can work well at the enterprise level, an individual may still be left with the problem of having many other passwords to remember outside the organizational context, when there is no common administrative authority (e.g. websites from a range of distinct providers). Although password management utilities have emerged to assist with the problem (e.g. PasswordSafe, a Windows-based utility that provides users with a means of storing all of their passwords for other systems securely within an encrypted database[7]), they are to some extent masking the problem rather than solving it.

Things can also be done to aid our recollection of passwords in other ways. For example, a colleague of mine recently admitted that he had written the PIN code for his ATM card on the back of the card itself. However, rather than writing the PIN as it would need to be entered at the ATM machine, he had written a modulo representation of it. As such, only someone with knowledge of this secondary secret (e.g. myself and the other people in the room when he shared the information!) would be able to make use of the card. We can do a similar thing with passwords as well (e.g. storing a prompt to help us remember the actual password), which is often the approach favoured by online sites for assisting users who have forgotten their passwords. However, the selection of such prompts clearly needs to be done with care, to ensure that they would not give a sufficient clue to someone else, or indeed be so obscure that we forget the link they are supposed to provide the actual password.

Although such workarounds can certainly be valuable, the underlying reason for needing them is that potentially arbitrary strings of characters such as passwords and PINs are difficult to remember in the first place. As such, another solution may be to use secrets that legitimate users can recall more easily. However, although authentication methods based upon other forms of secret knowledge have been proposed (including techniques involving the use of cognitive and associative questions[8], and graphical representations[9]), passwords appear to remain the preferred choice amongst end users[10], with other alternatives being considered more difficult and time consuming. The high degree of user acceptance is in some ways curious given that, in theory, passwords are a completely intrusive method of authentication and make fairly significant demands upon us as users. In practice, however, they have effectively become transparent and their use is frequent and familiar enough for users to regard them as natural. Coupled with the fact that many users do not use the technique properly in the first place, we have a situation in which, rather than change, most people appear satisfied to stick with a method that they realise is weak.

Other options . . . and why we still stay with passwords

On the basis of all this, it would seem that passwords are far from an ideal solution for frequent IT users who access a number of systems or websites, but despite their shortcomings, they remain the dominant form of user authentication. Of course, this is not because they are the only option, and other methods of authentication can be based upon something the user has (e.g. a card or some other physical token), or something the user is (e.g. a biometric, such as fingerprint, face or voice recognition).

Biometrics represents a particularly interesting example, not least because the associated methods have been predicted as possible replacements for passwords

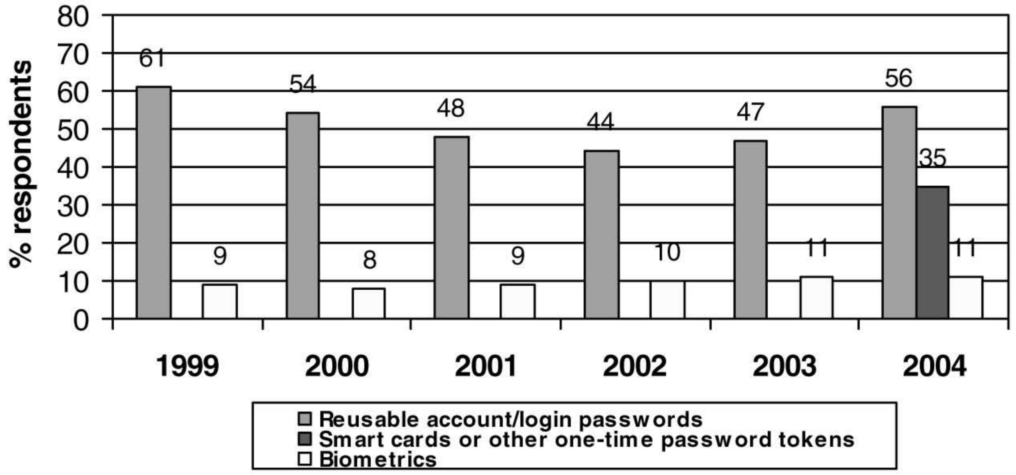


Figure 3: Use of authentication technologies (Source: CSI/FBI surveys)

for many years. Indeed, it is possible to find survey articles focusing upon biometric options that date back as far as the early 90s[11] [12], but some 15 years later it would still be difficult to regard their use as widespread. For example, looking at six years worth of results from the CSI/FBI Computer Crime and Security Survey[13] [14] it is apparent that biometrics have made relatively little impact when compared to other methods, and the proportion of respondents using them has remained fairly static (note: the studies prior to 2004 did not include the category for smart cards or other tokens). In viewing these results, it is worth noting that the profile of CSI respondents is generally skewed towards larger organizations (with only 20% generating revenues of under $10M per annum), and so it can be generally assumed that they also have the larger budgets available to spend upon security technologies. Given that, even in these cases, the extent of biometric adoption is relatively small, it can easily be appreciated that the extent of their usage in small and medium contexts is likely to be dramatically less.

Over time, one might expect that we will see the gradual replacement of passwords and PINs by biometric techniques. However, the current trend does not always suggest this. For example, in the UK, we are now widely witnessing the replacement of customer signatures with PIN entry as the means of verifying a purchase at point-of-sale terminals. The main rationale for this is that the latter will represent a more secure means of authentication, which is less susceptible to fraudulent use than the signatures. Now, admittedly, the extent to which signatures were verified by point-of-sale staff was variable at best: many plainly did not take the time to look whether what was signed on the paper matched what was on the card; some would even hand your card back to you before you had signed the till receipt at all; and I am sure that other readers will have shared the experience of witnessing someone present an unsigned card to the checkout operator . . . and then be asked to sign it, with the sale being accepted without any further form of verification! Another argument in favour of the move is that the use of the PIN at point-of-sale makes it consistent with the way in which the user is authenticated when using their card at an ATM. However, from the authentication perspective, the key point is that we have not moved to the automated equivalent of the signature-based technique, but towards a technique that is in many ways more vulnerable to unauthorized use (e.g. users can share their PIN, whereas they could not do the same with the signature). Nonetheless, the rationale for choosing the PIN over the available biometric options is clearly indicated by the following quote from the Cardwatch website:

> “Finger and iris scanning as well as voice recognition and dynamic signature have all been put forward as possibilities. Such technology, however, is not sufficiently reliable or cost-effective in a point-of-sale environment to meet the requirements of the UK card industry within the next ten years.” [15]

Point-of-sale is far from the only context in which such considerations will apply, and there are a variety of reasons why, in spite of their weaknesses, passwords or PINs are perceived to be the only viable option. One of the main factors is, of course, the cost. Passwords appear attractive because there is virtually no cost associated with their deployment. By contrast many token and biometric approaches require additional hardware to be added onto each system, which can lead to substantial deployment costs within a large organization. However, it is important to realise that none of the methods are cost-free, and the conventional wisdom may suggest passwords to be much cheaper than they actually are. For example, it has been estimated that approximately half of the technical support calls made to IT help desks are in relation to forgotten passwords[16], and with another study having calculated that every such call costs an organization approximately $25[17], it is clear that the issue can have significant financial implications. However, many organizations will not factor this into their initial decision making, and so the decision basically becomes a trade off between the ongoing (but potentially hidden) helpdesk costs for passwords, versus the upfront technology deployment and training costs that may be incurred by moving to other methods.

“There is no cost associated with password deployment”

Another possible complication of moving away from passwords is the users’ perception of the replacement method. Even though they may experience problems with them, most people tend to feel comfortable with passwords, whereas unfamiliar alternatives may engender resistance. This is particularly the case with biometrics, as users may object to the nature of the information being gathered. For example, fingerprint recognition often gets criticised because users dislike the idea of being fingerprinted each time they want to use their system.

A further constraint is the effectiveness of the replacement method – a problem that is again most readily associated with biometrics. Whereas passwords and token-based approaches result in black and white judgments (i.e. if a user knows the password they will get access, otherwise they will not), biometric methods are not as clear-cut, resulting in both false acceptance errors (where impostors may incorrectly be judged to be legitimate users), and false rejection errors (where legitimate users are falsely believed to be impostors). Although the technology has improved dramatically in recent years, it is still not considered accurate or reliable enough for deployment in all scenarios – as shown by the point-of-sale example.

A final factor that often points us in the direction of passwords is the type of IT system on which the authentication is required. Although it may be feasible to use tokens or biometrics within an organizational setting (with a relatively contained user community), it would be impractical to do for a website, where users can register at any time from any location. In this case, it would not be possible (or financially viable) to provide a physical token to each registered user before permitting them access, or to rely upon each user having the appropriate hardware facilities to support biometric authentication on their systems. Even other secret knowledge approaches are only suitable to a more limited range of contexts. For example, graphical methods are limited by the size and capabilities of different displays, whereas techniques requiring more lengthy typed inputs, such as responding to a series of cognitive questions, will only be reasonable on devices with good quality keyboards. As such, passwords and PINs gain from the fact that, from an operational perspective, they have almost universal applicability.

No single solution

Ultimately, no single method of authentication is ideally suited to all contexts and from the discussion presented here, it should be apparent that passwords are unlikely to disappear in the foreseeable future. This, in itself, is not bad news – they can still provide a good level of protection if they are used correctly, and in many cases a risk assessment may genuinely suggest that the adverse impacts of moving to alternative methods (e.g. cost, disruption, etc.) would outweigh those likely to result from password misuse. However, while there are clear obstacles to the use of alternatives in some contexts, it would also be fair to conclude that the continued use of passwords in some quarters is the result of complacency or inertia on the part of users or organizations, and hence a lack of demand and incentive to introduce other methods. Whatever the reason for their use, we must constantly work to ensure that passwords do not become a standard part of security-related bad practice. As such, promoting suitable guidelines to users (both within the workplace and as part of online services) is an important responsibility of any system or service operator that depends upon the technique for the protection of its assets, or those of its customers.

References

1 Morris, R. and Thompson, K. 1979. “Password Security: A Case History”, *Communications of the ACM*, vol. 22, vo. 11, pp594-577.

2 SANS Institute. 2004. “The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts Consensus”, Version 5.0, 8 October 2004. http://www.sans.org/top20.

3 DTI. 2004. *Information Security Breaches Survey 2004*. Department of Trade & Industry, April 2004. URN 04/617.

4 Furnell, S.M., Dowland, P.S., Illingworth, H.M. and Reynolds, P.L. 2000. “Authentication and Supervision: A survey of user attitudes”, *Computers & Security*, vol. 19, no. 6, pp529-539

5 FOLDOC. 2003. “single sign-on”, Free On-Line Dictionary Of Computing (FOLDOC), http://wombat.doc.ic.ac.uk/foldoc/foldoc.cgi (accessed 3 February 2005).

6 DTI. 2004. *Information Security Breaches Survey 2004*. Department of Trade & Industry, April 2004. URN 04/617.

7 “Password Safe”, http://passwordsafe.sourceforge.net/ (accessed 3 February 2005).

8 Haga, W.J. and Zviran, M. 1991. “Question-and-Answer Passwords: An Empirical Evaluation”, *Information systems*, vol. 16. no. 3. pp335-343.

9 Dhamija, R. and Perrig, A. 2000. “D´ej`a Vu: A User Study Using Images for Authentication”, Proceedings of the 9th USENIX Security Symposium.

10 Irakleous, I., Furnell, S.M., Dowland, P.S., and Papadaki, M. 2002. “An experimental comparison of secret-based user authentication technologies”, *Information Management & Computer Security*, vol. 10, no. 3, pp100-108.

11 Cope, B.J.B. 1990. "Biometric Systems of Access Control", *Electrotechnology*, April/May: 71-74.

12 Sherman, R.L. 1992. “Biometric Futures”, *Computers & Security*, vol. 11, no. 2, pp128-133.

13 Richardson, R. 2003. *2003 CSI/FBI Computer Crime and Security Survey*. Computer Security Institute. Spring 2003.

14 Gordon, L.A., Loeb, M.P., Lucyshyn, W. and Richardson, R. 2004. *Ninth Annual CSI/FBI Computer Crime and Security Survey*. Computer Security Institute.

15 Cardwatch. 2004. “Chip and PIN programme”, in ‘Card Fraud Overview’, APACS (Administration) Ltd April 2004, http://www.cardwatch.org.uk/html/overview.html#chip (accessed 3 February 2005).

16 “Passwords Continue to Cause Problems”, Computers & Security, vol. 21, no. 4, pp300-301.

17 “IT helpdesk suffering user password hell”, Silicon.com, 14 January 2003.

About the author

Dr Steven Furnell is the head of the Network Research Group at the University of Plymouth, UK, and an Associate Professor with Edith Cowan University, Western Australia. His research has included a number of projects focusing upon user authentication issues, particularly in relation to secret knowledge and behavioural biometric approaches. A number of current projects within the Network Research Group are continuing to pursue these themes, and related papers can be obtained from the website at www.plymouth.ac.uk/nrg.

Keeping your data available in 10 steps

Mark Heywood is a consultant with Insight Consulting's Business Continuity Practice

The provision of integrated and replicated enterprise-wide data across a wide range of business tools is perhaps the most valuable contribution that an IT department can make in an organization. Unfortunately, vast arrays of technical options stand in the way of this contribution. Effective partnership between IT and business based on a solid business continuity management foundation can make a difference.

Introduction

There has been a noticeable increase in recent years in the reasons why organizations take business continuity seriously. Traditional justifications such as power failure, fire and flood have been joined by legislative and corporate governance requirements as valid drivers for business continuity programmes. Modern business practises and advances in technology have meant that such programmes are facing more and more complex issues, which in turn lead to increased costs in establishing effective and appropriate plans.

Unlike traditional Disaster Recovery planning or contingency planning, Business Continuity Management places an increased focus upon prevention by means of risk reduction, as well as upon recovery. Business Continuity should be a fit-for-purpose, business owned and driven activity that engages a broad spectrum of business and management disciplines. IT and its role as data protector is one such discipline.

The complex Web of available technical infrastructures, modern trends in outsourcing, moves to mobile working and developments in Interactive Voice Response Systems and Voice over IP all make the job of protecting and delivering integrated data across an enterprise extremely difficult. So difficult, in fact, that an organization's disaster recovery needs may be met with a wholly inappropriate response. Oddly, within certain organizations, it is the manager who is able to respond to a situation - once things have gone wrong - who is prized above the manager that can facilitate prevention in the first place. The highly visible nature of crisis management, particularly within IT, is certainly

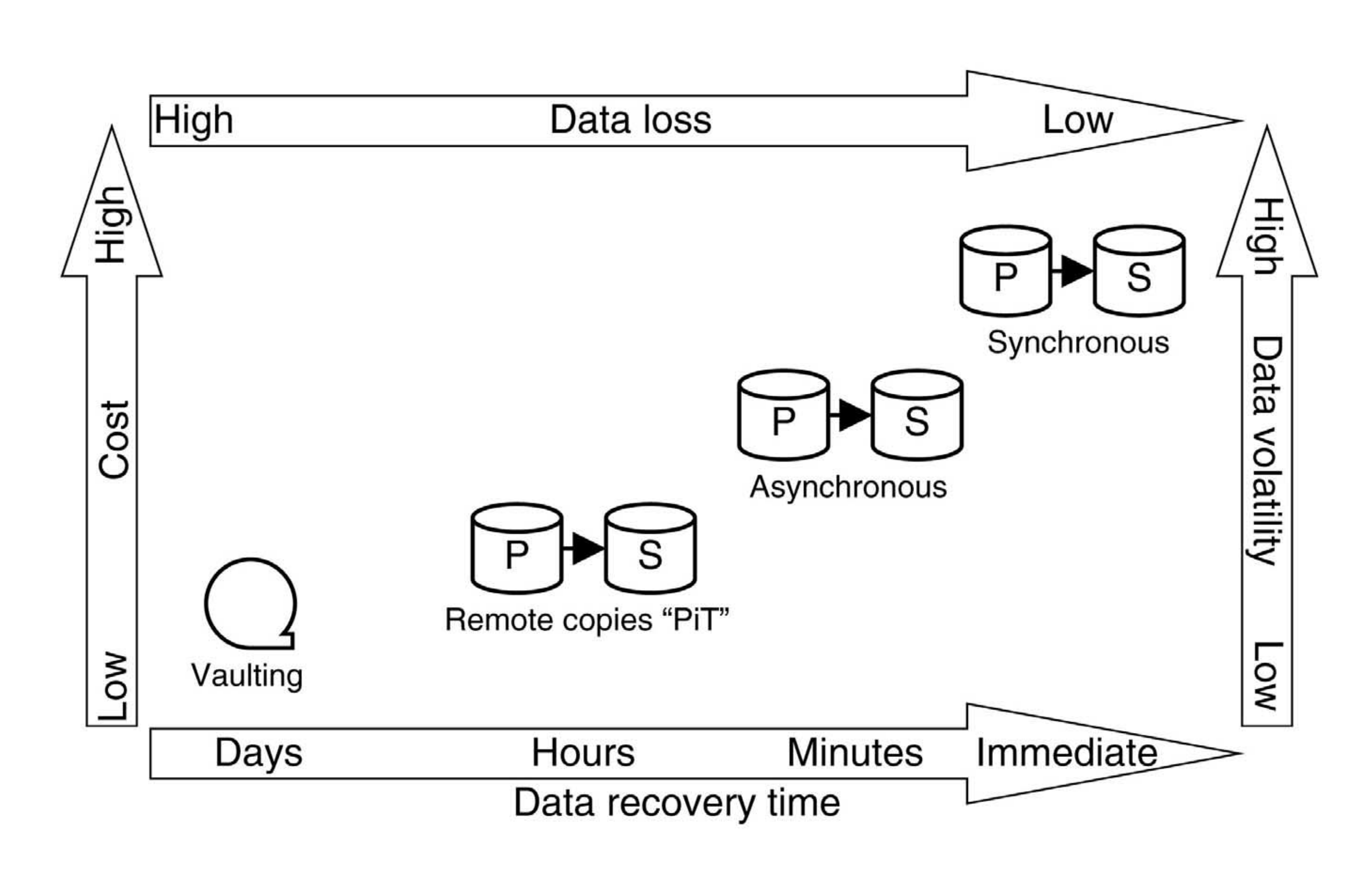


Figure 1: Data replication value chain

impressive and perhaps one of the reasons why prevention is so unpopular is that it involves making infrastructure and often process changes before something has been shown to be faulty or insufficient.

> **"Prevention is so unpopular"**

Business continuity of important applications and access to information is absolutely critical to an organization's ability to recover from a denial of service incident. Organizational data drives an increasing proportion of enterprise value and prolonged periods without it can have very serious implications. However, whilst certain types of data are irreplaceable and provide a heartbeat between an organization and its customers and suppliers, not all data is of equal value and indeed the value of certain data can change. The challenge that this presents has traditionally been seen purely in IT terms. However, the recent growth in the importance of business continuity has meant that this has actually become a challenge to be solved jointly between business and IT. As such, IT departments have started to be seen as tools which link the business continuity goals of prevention and resilience with organizational goals related to strategy.

Ten steps to work through

In order to ensure this challenge is met, there are ten key issues which businesses and their IT departments need to work through.

1. **Who defined/decided what data is critical - IT, business, or both?**
2. **How was the critical data identified?**
3. **How often are backups performed and what are the success rates of the backups?**
4. **When did you last rebuild an 'off the shelf' server using restores?**
5. **Where are the backups stored and would the backups be accessible following an incident?**
6. **Would the data be consistent following a restore?**
7. **How is data synchronised across the entire enterprise?**
8. **How much data would be lost and how could this be recreated?**
9. **For 'total loss' do adequate DR contracts exist to enable the infrastructure and data to be recovered?**
10. **Would the DR site be accessible following an incident?**

Organizational data is both self-contained and enterprise-wide in that it can range from being stored on a single application on a single server to a single application being distributed across multiple platforms spread across multiple sites. A single transaction can update data across entire enterprise architectures. A further challenge that this brings is the realisation that organizational data is no longer under the control of an internal organization. Whilst employees are still responsible for updating data and inputting new data, the same is now true for customers and suppliers. Internet and electronic data technology allows customers and suppliers to change organizational data at speeds that were unimaginable as little as five years ago. It is this challenge which drives the need to resolve the 10 key issues that have been mentioned. But first, there are two questions which much be addressed.

- How long can you afford to be offline?
- How much data can you afford to lose?

The answers to these two questions will determine the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) of an organization. These objectives will help to shape the IT Continuity approach that an organization takes to protect its data.

IT continuity

By integrating IT Continuity into an overall enterprise-wide Business Continuity Management framework, organizations can ensure that critical IT systems can be sustained during an incident. Threats can be identified and managed to an acceptable level of risk and single points of failure can be eliminated through the implementation of a resilient infrastructure. The development and testing of effective IT recovery plans can help to protect critical data from malicious or accidental damage. Spam, viruses and hacking are not new phenomena yet mobile working and the tools that support it place greater demands on IT departments in these areas. Mobile devices such as PDAs and Blackberry handsets are at risk from viruses and the wireless network infrastructures that underpin these devices offer new avenues for denial-of-service attacks on data.

A robust IT Continuity plan needs to have clearly defined requirements relating to recovery priorities with respect to both RTO and RPO. In order to do this, business units need to work with IT in order to understand how their business processes map to the available technical infrastructure. This is about much more than simple asset inventory (although this is still important). Technical recovery plans need to consider data centre logistics (location, physical security and environmental issues such as air conditioning, fire detection and suppression, power and water requirements) and infrastructure configurations, for both hardware and network architecture.

Telecommunications requirements are also important and a proper understanding of the inherent risks is vital. Telecommunications companies engage in wholesale arbitrage for switched telephone minutes and in the use of common ducts and peering points for data pipes – which means that what may appear to be dual supply might turn out to be two suppliers sharing the same infrastructure. Moves to Automatic Call Distributors, Interactive

Voice Response Systems and Voice over IP are placing voice very much at the heart of an organization and voice recovery also needs to be considered within an overall recovery plan.

Ultimately, IT Continuity is of vital importance because it serves to protect infrastructures and data. A key element of this is data replication.

Data replication

Of paramount importance to organizations is the need for an accurate copy of key data at a remote site that does not impact business as usual system performance too adversely. In order to achieve this, business units must work with IT to determine specific data requirements. It is these requirements that ultimately decide the method of data replication that will be used and these methods have adapted to meet the challenges of data availability requirements. Point in time, asynchronous and synchronous forms of data replication (see Figure 1) all represent different levels of the data availability value chain, yet they all have inherent problems and disadvantages.

Within a local Storage Area Network (SAN) synchronous data replication is able to provide an up to date copy of key data at a remote location. Each write transaction is acknowledged by the remote site thus ensuring that the two sites hold consistent data and that in the event of a problem at the main (or primary) site, the backup (or secondary) site will simply take over the provision of data without any loss. However, if the distances between the sites are extensive, or if the bandwidth that connects the sites is not sufficient, the acknowledgement of each write transaction can cause key business systems to slow down thus impacting business performance. Of course bandwidth can be increased to reduce latency issues, but the costs can be prohibitive.

Moving down the data value chain, although asynchronous data replication is still fairly bandwidth intensive, it can reduce latency on a network. This is because the data being sent to the secondary site is held in a queue before being written to disk. There are two main disadvantages with asynchronous data replication. The first is that applications which require a greater amount of writes to disk become more out of date with their secondary copies depending on the length of time taken to write to disk. This means that in the event of a failure at the primary site data loss will inevitably occur at the secondary site. The second disadvantage is that whilst data is held in a queue waiting to be written to disk at the secondary site, there is no guarantee that the writes will be performed in the appropriate order, thus leading to inconsistency.

> **“data is no longer under the control of an internal organization”**

Point in time data replication provides a much simpler and cheaper method of protecting data. However, the simplicity and cost effectiveness of this approach is often rendered useless by its limitations. Data is written to tape, stored at a remote location and can be restored in the event of a failure at the primary site. However, the time taken to perform a restore can be hours instead of minutes meaning that data loss will be significant depending on how out of date the data is. Also, in terms of data retention it is worth considering that magnetic tape has an extremely limited life span. Storage conditions and re-use of tapes can lead to data loss due to the stress put on the tape as it passes around the tape wheels. In such circumstances, some tapes or DLT cartridges can be rendered useless after a few uses.

To add to the difficulty of choosing an appropriate approach an IT department also needs to consider the wide range of technology options which are available. Database and storage-based replication are offered by vendors as a way of protecting data. However, often these solutions are proprietary and will only serve to protect specific, and in this respect isolated, elements of organizational data. Contractual obligations must be thoroughly investigated before such an approach can be considered. The outcome of this is that IT departments will often need to add further layers of protection in order to cater for the rest of the data and these additional layers simply add to the confusion and cost of such an operation.

The challenge is then one in which available methods of data replication and technical options all have advantages over each other, but also have significant disadvantages in terms of cost, consistency, performance and even complete data loss. One thing that is consistent, however, is the fundamental importance of data to organizations and focus of senior management and Board Directors on the growth and predictability of future earnings. The impact of data unavailability over a prolonged period can have a significant impact on this focus. Additionally, brand reputation and customer loyalty take years to achieve yet can be destroyed in hours.

Summary

Enterprise value is driven significantly by data. By working through the 10 issues that have been mentioned, IT can ensure that an appropriate IT Continuity strategy is developed with specific data replication and protection elements. The starting point - in the form of Business Impact Analysis - to ascertain which processes, systems and, of course, data are key is one of the initial stages of a robust Business Continuity Management platform. It is from the foundation of such a platform that IT can make a valuable contribution to an organization.

Trojans & spyware: an electronic achilles

Paul Gosling

ICSTIS, the body that regulates premium rate phone numbers in the UK, recently received about 50,000 complaints from PC users who claimed that secret Trojan software had changed their Internet dial-up settings to connect automatically to premium rate phone numbers.

ICSTIS concedes this was only the tip of an iceberg. Anyone who fell victim to that infestation and who banks online could also be vulnerable to Trojans that take control of their machines to conduct rogue banking transactions.

"Our view is that Trojans are potentially a much more insidious and damaging threat than phishing," says Sandra Quinn, spokeswoman of the Association for Payment Clearing Services, which leads the industry fight against online fraud.

> "Spyware is an escalation of phishing"

"Absolutely," agrees George Thompson, director of security services at business service providers, KPMG. "They could be worse than phishing simply because users are not aware that these things are on their machines."

What lurks within?

But while most commentators still talk of Trojans and spyware as a potential threat, there is evidence of damage. A survey published last year by Earthlink and Webroot concluded that about 90% of PCs host spyware, with on average 26 pieces of spyware installed on each computer. In many cases the aim is some form of identity theft, for example by capturing personal information through logging keystrokes used during online banking.

Spyware authors collate information collected from 'client' machines and sell it on to organized crime gangs who then use it to make fraudulent transactions.

Nasty problem

In recent months audit firm Ernst & Young has tackled "half a dozen" assignments to advise financial institutions on how to respond to these attacks. "The buyer can validate the information, see what works and then collect several (sets of account details and passwords) to make a co-ordinated attack," explains Antony Smyth, a partner in information services advice and assurance at E&Y. "Suddenly it can turn into a nasty problem."

And there are signs that the fraudsters are busy. Thompson says "I know of one bank that suspects most of its losses [from online fraud] come from details obtained from Trojans rather than phishing."

"Spyware is a large threat to the industry," agrees Phil Robinson, managing consultant of the penetration testing team at Information Risk Management. "It's an escalation of phishing attacks, rather than a different type of attack. But it is difficult to quantify the level of losses. I would certainly say some of the banks have suffered unauthorized access, but you can't easily determine what success Trojans have had."

Greatest challenge

There are now signs that the retail banks are tackling the threat with urgency. Mark Hemingway, spokesman for HBOS, confirms that his bank has written to all its online customers warning of the risks from Trojans and spyware. "Yes, it's a weak link," he says. "Fraudsters will always target the weakest links. Banks and building societies are very secure, but customers who may not have the most up-to-date anti-virus software pose our greatest challenge."

In an effort to improve security, HBOS has arranged a discount on Trend Micro's anti-virus software for its online banking customers.

But there is little agreement about how effective anti-virus software is against spyware in particular. This is because a user may inadvertently download it when closing a pop-up, obtaining freeware, opening an email attachment, through instant messaging, or visiting a website that spoofs that of a legitimate company.

HBOS and APACS say that strong firewalls as well as anti-virus protection may be needed against spyware. And APACS accepts that some firewall settings that protect against spyware can cause problems for home users just to access the Net.

"Most home computers don't have the software to safeguard them [against spyware], even if they have anti-virus software installed," says Peter Yapp, deputy director for IT security at the Control Risks Group. "They will need specialist software, but for most individuals this is just another piece of software they are told they need."

Austin Dunn, a senior manager at business service provider Deloitte & Touche, agrees. "Although regular anti-virus updates are important, they do not necessarily alert or protect users against spyware. This may allow third parties to captured their personal details surreptitiously," he says.

Naïve users

"Although some ISPs now offer home users spyware detection in addition to anti-virus and personal firewall software, users remain vulnerable as they are often naive about the risks of not taking precautions against malware or of the symptoms associated with infection. Furthermore, the risks associated with malware infection are compounded with the increasing uptake of 'always on' broadband connections."

Infiltrators

Dunn wrote Countering financial crime risks in information security, which was commissioned by the Financial Services Authority and published by the FSA last November. In it he argued that one of the biggest threats to banks was from organized criminals who infiltrated "agents" to steal from within or to compromise security. This view, which the banks dispute, may yet be vindicated once details emerge from the £22m pre-Christmas heist of Belfast's Northern Bank.

> **"The Internet is not secure enough for online banking"**

Ian Grigg, director of e-payments advisers, Systemics, only partially accepts this assessment. "Insider fraud is still by far the biggest concern of the City banks," he says. "Whether IT security is included in that bailiwick is open to question - no virus has brought down a bank, whereas insider frauds have."

Grigg adds "I would challenge (the FSA) to elucidate and present its evidence (of organized crime placing agents inside banks). In contrast to that, there is evidence that identity theft crimes are becoming organized. And there is some evidence, although not conclusive, that traditional organised crime players are involved.

"There is also substantial evidence that much identity theft comes from insider breaches, whereby insiders are "turned" and sell (individuals' personal details). In this sense, the FSA could be pointing in the right direction, as there is definitely a high risk wherever identity is stored in mass databases."

Just once

Grigg argues that as UK lenders rely more heavily on customers' electronic identities to transact business, and the government offers more services based on digital proofs of identity, then their vulnerability to identity fraud must rise. "The scope for security defences is limited, as the identity thief only needs to succeed only once to steal an entire database," he says. "It's an asymmetric power struggle which the banks won't be well placed to win."

And, says Control Risks' Yapp, the move to chip and PIN could actually make that situation worse. "The pressure to learn PIN numbers means that people will use one PIN number for all their cards, online access and even their burglar alarm," says Yapp. "When someone guesses one of these they've unlocked the whole lot." Deloitte's Dunn also warns about the impact of chip and PIN: success in countering credit card fraud is likely to push fraudsters to concentrate on online fraud.

Many observers believe that if banks are to protect online transactions the only solution is to improve the payment authentication process. Yapp says banks will simply have to be more imaginative than to ask for a user's mother's maiden name.

Biometric data?

In what looks like a mighty shove towards digitally-stored biometric data, Yapp says the banks' challenge is to validate transactions using information that both parties have easy access to without anyone having to write it down somewhere, and preferably not information that a third party could guess or obtain by research.

Phil Robinson, from Information Risk Management, believes that banks must first concentrate on consumer education. "I haven't seen (them publish) a huge amount about Trojans and spyware, the nature of risk posed by some of the websites you may visit and what others can do to your computer," he says. "Banks should also be advising customers to increase browser security and perhaps use a different browser because a lot of these things target Internet Explorer. I haven't seen any banks do this."

Ernst & Young's Smyth suggests banks should focus on two-factor authentication. This might include a transaction being confirmed through text messaging to a mobile, or through a smartcard reader attached to a PC. In some countries, online banking can be done using only PCs that store an agreed identification code.

Who benefits, really?

Such moves are unpopular with the banks because of the cost; at present this outstrips losses from online fraud. But, says Smyth, the main deterrent is probably bankers' worry that stricter controls could discourage customers from banking via the Internet. They want to encourage this trend because the costs are negligible compared to teller-mediated transactions.

But customers' awareness of the rising threat could also stem the tide. The banks must hope not too many consumers share the views of Peter Yapp, who argues that we should restrict electronic banking to private networks. "The Internet is not secure enough for online banking," he says.

About the author

Paul Gosling is a freelance journalist who specializes in finance and information technology, and who is author of several books. He writes for The Independent, Public Finance and Accounting & Business

Mobile phone tracking threatens privacy

SA Mathieson

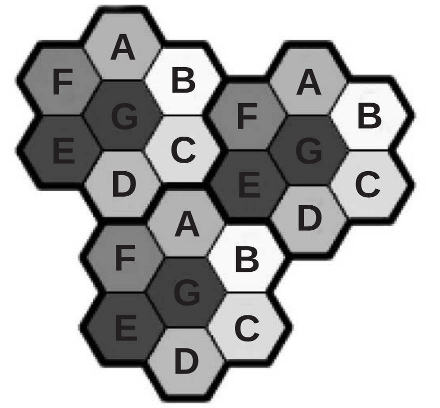
In 2001, it was a struggle to convince the UK division of mobile phone operator Orange to disclose location data held against my account, generated when I made or received phone calls, in an intelligible form. Through a subject access request made under the UK's implementation of the 1995 European data protection directive, Orange eventually provided a list of numbered cell-sites used for each call - fairly meaningless, as it refused to provide locations for these numbered sites.

Mobile phone location data has since become less shadowy. Cases such as the Soham murder trial highlighted mobiles' potential as locator devices, with one of the victims tracked to a spot near the murderer's house with location data from her phone's network. In 2003, services such as ChildLocate and Mapminder started selling the ability to track mobiles, with users' permission. These services pass on the location and the coverage range of the cell site through which a tracked phone is connecting.

And early in 2004, London Ambulance Service gained automatic access to this cell site data. Its operators can now see the approximate location of anyone calling the UK's 999 emergency number (or 112, the common EU number). The UK's other emergency services have since adopted, or are adopting, the system.

Similar moves are taking place elsewhere. A 2002 European directive on telecoms requires mobile location data to be passed on to the emergency services in this way, and should have been implemented in mid-2003. However, in April 2004 the European Commission said it was taking six of the old 15 EU states to the European court for failing to implement. Across the Atlantic, the United States' E911 legislation, requires mobile operators to have introduced extra technology such as triangulation to provide the emergency services with locations accurate to within a few dozen yards by the end of 2005.

Emergency service access to a caller's location, which in some cases could prove life-saving, is hardly controversial. But other uses can be. The current quality of location data is middling to



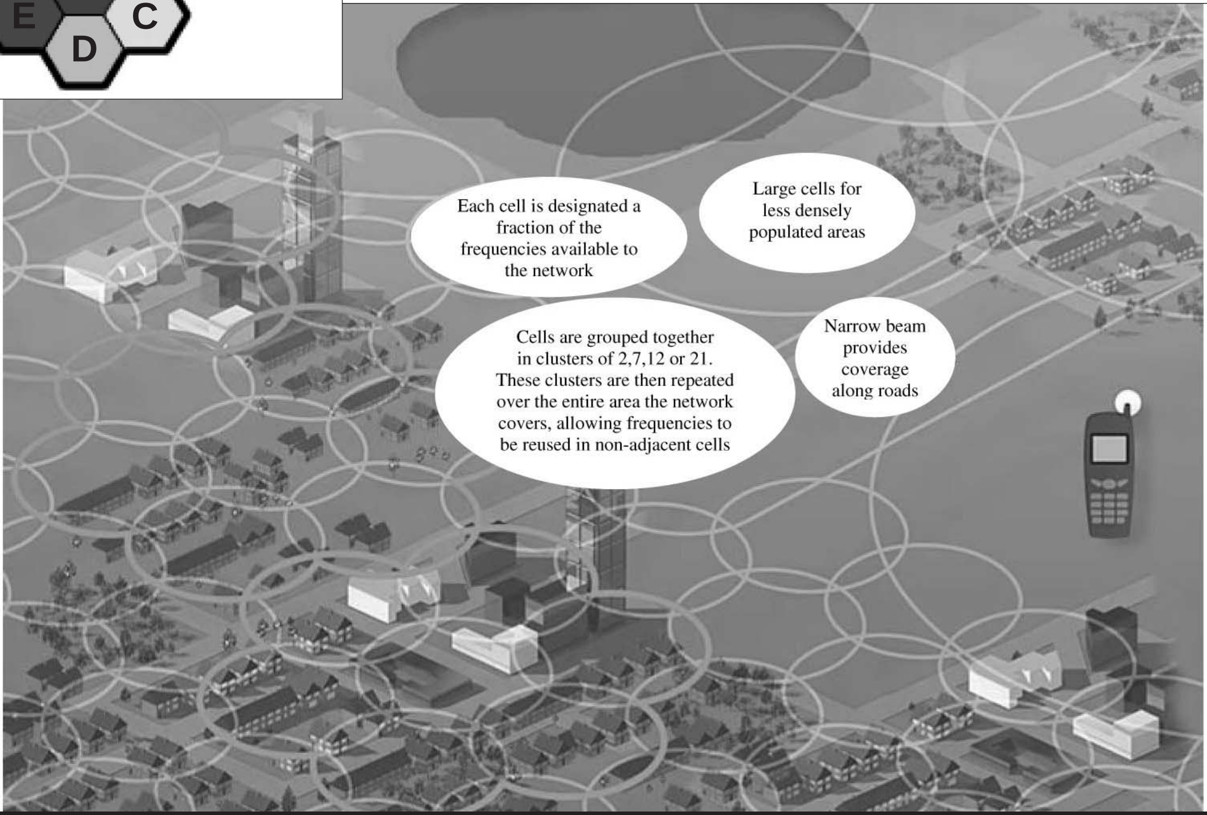

Each cell is designated a fraction of the frequencies available to the network
Large cells for less densely populated areas
Cells are grouped together in clusters of 2,7,12 or 21. These clusters are then repeated over the entire area the network covers, allowing frequencies to be reused in non-adjacent cells
Narrow beam provides coverage along roads

Figure 1: Base station cell clusters

poor - in the countryside, a cell-site can stretch for miles - but it is improving.

The power of base station transmitters must be carefully calculated to avoid interference. To avoid this, cells are grouped in "clusters" in which each base station uses a different frequency. The arrangement is represented in Figure 1 as letters of the alphabet. These frequencies are then re-used in neighbouring clusters.

The adoption of third generation phones will shrink the size of cells, as each one covers fewer customers. However, the big improvement in accuracy will come from phones that incorporate global positioning system (GPS) technology, providing locations to within a few yards. This is not yet a standard feature. The only Nokia model with GPS built-in is a Tetra radio, for professional use such as by emergency services, although GPS modules are available for a couple of consumer handsets. However, with mobiles, this year's cutting-edge function is often unavoidable when you upgrade in two years time.

> **"Mobile operators need to protect customer movement data"**

This means that mobile phone operators will obtain an increasingly accurate picture of their customers' movements - not just which town or suburb they have visited, but which building. As a consequence, the operators should review their infosecurity arrangements. Cell-site data is not good enough for a kidnapper to find a victim; GPS probably is.

And the operators should also confess to what they know. Surely only the dimmest criminals are still ignorant that mobile phones act as locator devices: any element of surprise for the police and spies, who have legitimate access to such location data, must be over. However, law-abiding citizens - those who do not depend professionally on the police not knowing where they are - may not. Mobile phone customers should be told on their bills about the accuracy of the location data held on them, how long it is kept for and who can get access.

This could act as a sales opportunity, a chance to market location-dependent services. But it would also mean that mobile phone users would know where they stand - only fair, given the networks know where their customers stand with increasing accuracy.

EVENTS CALENDAR

29-30 March 2005
ECCE E-CRIME & COMPUTER EVIDENCE
Location: Monaco, France
Website: www.ecce-conference.com

29 March - 1 April 2005
BLACKHAT EUROPE
Location: Amsterdam, The Netherlands
Website: www.blackhat.com

5-6 April 2005
E-CRIME CONGRESS
Location: London, UK
Website: www.e-crimecongress.org

26-28 April 2005
INFOSECURITY EUROPE
Location: London, UK
Website: www.infosec.co.uk

12-13 May 2005
RSA Japan
Location: Tokyo Prince Hotel, Tokyo, Japan
Website: www.rsasecurity.com/conference

5 - 6 May 2005
CLA 2005 World Computer and Internet Law Congress
Location: Washington DC, USA
Website: www.cla.org

13-15 June 2005
CSI NETSEC
Location: Scotsdale, Arizona USA
Website: www.gocsi.com

26 June - 1 July 2005
17th ANNUAL COMPUTER SECURITY CONFERENCE
Location: Singapore
Website: www.first.org

23-28 July 2005
BLACKHAT USA
Location: Las Vegas, USA
Website: www.gocsi.com

17-19 October 2005
RSA Europe
Location: Vienna, Austria
Website: www.rsasecurity.com/conference

14-16 November 2005
CSI 32nd ANNUAL COMPUTER SECURITY CONFERENCE & EXPO
Location: Washington, USA
Website: www.gocsi.com