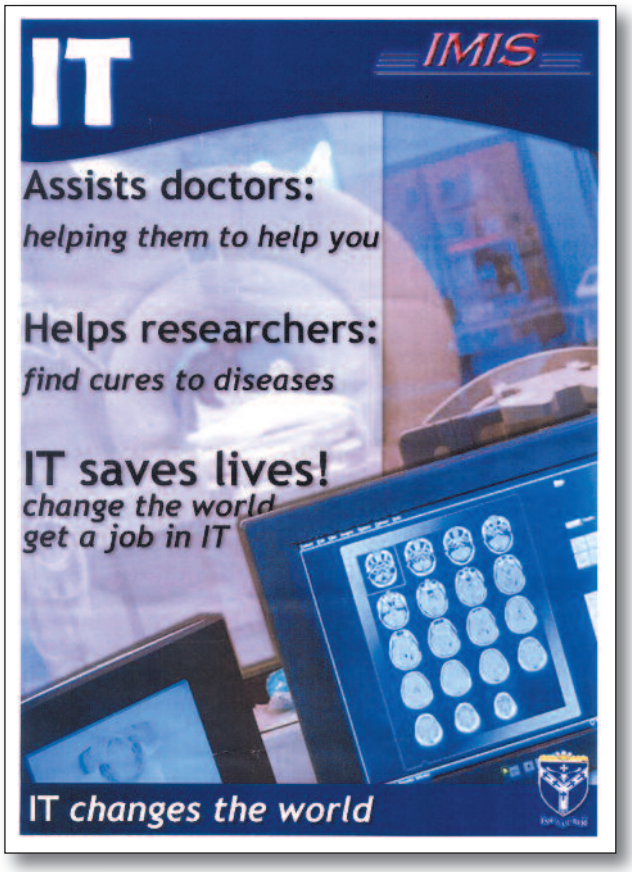
which the national winners will be selected.

All winning posters will be printed in the *IMIS Journal*, and used as part of our on-going work to raise the awareness of career opportunities in ICT among secondary school students in the UK and abroad.



Briefing pack for participating schools

The briefing pack, available on request from IMIS, with instructions for teachers and students participating in the competition, includes the following rules and deadlines:

- schools intending to submit entries to the Poster Competition should notify IMIS by May 30, by completing the attached form
- entries must be delivered to IMIS no later than November 30. IMIS cannot be held responsible for entries lost in the post. Entries for the technology stream may be submitted by e-mail
- winners will be announced by January 31, 2011, and prizes dispatched to the school head for presentation. Each of the winning posters will be printed in the *IMIS Journal* and may be used as part of IMIS campaigns promoting careers in IT. Suitable release forms must be submitted with each entry. Failure to submit the release form will disqualify the entry from the competition
- each poster should be composed entirely of original art ~ the incorporation of any previously published material will disqualify the entry due to copyright restrictions
- each individual entry should be clearly identified on the back, with the student's name and age, and the name of school and the stream (art or technology) in which it is to be entered
- IMIS is unable to return artwork, so copies should be retained if required

If any IMIS members currently involved with their local school would like to participate in this project, please contact the IMIS Executive for the full briefing pack.

Information Security is a field full of difficult problems, but the most intractable is probably authentication. Weak methods are used because they are cheap and easy to understand, strong methods are rarely used . . . and new developments have major flaws.

The most commonly used authentication method is, undoubtedly, the password, but it is notoriously weak and misused. The fundamental weakness is that any string of characters we can reliably remember is probably easily guessed ~ by a dictionary attack, or brute force. Security consultants say that users make matters worse, they choose easy-to-guess passwords, use them on multiple systems, and reveal them to strangers.

This is confirmed when organisations mess up, such as last December when social network web site RockYou exposed 32 million plaintext passwords via a SQL injection flaw. The web site made the colossal errors of storing plaintext passwords, and not checking their web applications for vulnerabilities, but analysis of the passwords showed the most popular to be '123456'. Similarly, studies from London through Sweden to

IMIS

IMIS 5 Kingfisher House New Mill Road Orpington Kent BR5 3QG
Tel + 44 70 0002 3456 **Fax** + 44 70 0002 3023 **e-mail** central@imis.org.uk **web site** www.imis.org.uk

Authentication ~ a trivial pursuit?

The challenges to on-line security are many and varied, but perhaps the greatest is authentication. Allan Dyer looks at the background and finds some potentially-damaging new methods of authentication coming into common useage

Auckland have shown that users will reveal passwords in exchange for a chocolate bar.

Users not always naive

Is this the whole story? The big flaw with the 'chocolate for passwords' studies is that the passwords were not verified ~ some people might be unwise enough to give away their real password, but how many are willing to lie about their password for chocolate? Users are not always as naive as we, their administrators, tend to think.

Everyone is faced by remembering far too many passwords: ATM PIN, home ISP, office network login, webmail account(s), social networking site(s), on-line banking, product warranty registration(s), the list is endless. In response, users will make rational decisions, according to the value they attach to the systems. Is the system security important to them? Would it be a hassle if they forgot the password?

Some users might decide to use a different, strong password on the two or three systems they deem 'important', and a single, easy-to-remember (easy-to-guess) password on all the rest. Compromise of the unimportant password, because it has been guessed or exchanged for chocolate, doesn't matter to the user, but it might matter to you, the administrator.

So, for more sensitive systems, we choose stronger authentication, but the criminals also up their game ~ for ATM cards, for example, we progress from PIN to chip and PIN, but still suffer fraud.

Ultimate challenge is on-line banking

Perhaps we can learn how to secure our systems by looking at what is being used for difficult authentication problems. Outside of the state security realm, the ultimate challenge in authentication is on-line banking, for three reasons. First, the target is just too attractive for criminals to ignore ~ an automated attack could net the funds of millions of ordinary people, or, if it is infeasible to automate, a few, very high net worth accounts can be chosen. Second, the authentication takes place remotely and, third, the endpoint is not controlled by a security expert.

Of course, every part of the system is protected. The banks protect their servers, the network communications are encrypted, and users are advised to install and update their anti-virus software and personal firewalls. The best current systems use code-generating tokens with a password for two-factor authentication. Despite all the security in place, the overall security is still weak because it is not defence in depth.

The obvious weak spots are the communications and the user's computer. The strength of SSL encryption is irrelevant if the web form the user is submitting is going to a fake web site, either with a certificate he or she didn't actually check, or tried to check, but were fooled by a browser trick of displaying an image of the real validation. On the user's computer, malicious software can capture the authentication information as it is entered. Such attacks are not just theoretical possibilities ~ there are publicised cases, like a New York school loosing $3 million, while some researchers report dozens of incidents involving between $10,000 and $500,000 each.

How to improve authentication

So, how might banks improve their authentication? A recent Gartner report recommended that banks should use server-based fraud detection techniques to monitor transactions for suspicious behaviour, such as abnormal speed or cadence of keystrokes that could indicate automation, and therefore malicious software rather than a genuine user. This would involve detailed research into the range of normal human behaviour, but

***Allan Dyer** CISSP MHKCS MIAP AIMIS MSc (Tech) BSc is chief consultant of Yui Kee Computing Ltd in Hong Kong; with a background in microbiology and control engineering, he specialises in computer viruses, spam and promoting better information security. He is a founding member and President of Anti-Virus Asia Researchers (AVAR), Vice-Chairman of the HK Computer Society Information Security Specialist Group, and founding member of the Asia-Pacific chapter of the High Technology Crime Investigation Association. He contributes to Government consultations and public debate on information security issues*

an attacker could defeat it by simply mimicking the behaviour of the victim.

Another novel trend for authentication has been noticed by Roger Thomson, AVG's Chief Research Officer. In short, his card was declined, he called his bank, and one of the security questions was about the age of his daughter-in-law, referred to by her maiden name. The only place Thomson knows of a public link between them is Facebook, so it appears that (some) credit card issuers are utilising personal data from social networks for the purposes of authentication.

Ignoring the privacy issues this raises, your control over your finances might depend on your ability to recall trivia from your family and friends social network sites, and any criminal can access the same sites. Even worse, if any of your friends or relatives has chosen to use a weak password ~ well, social networking is just for fun, it doesn't really matter ~ the data your bank is using for authentication could be poisoned. We are in the strange position of having access to a wealth of information about anyone, but little or no assurance of its accuracy.

The willingness to recommend and adopt these obviously-flawed techniques, recognising 'normal' human behaviour, and re-purposing personal data of dubious accuracy, shows the desperate need for better authentication. Perhaps it is time to re-examine PKI (Public Key Infrastructure), and see if better user education can make it more popular.


Andy Stanford-Clark

Green IT is high on every organisation's agenda. With new Carbon Reduction Commitment legislation coming into force from April and continued fallout from the failure of the recent United Nations Climate Change Conference in Copenhagen to reach anything more than a tepid accord, it is clear that climate change, carbon reduction and the role of Green IT is becoming an increasingly important topic of discussion.

The Gartner research group, whose predictions for the year ahead are always eagerly awaited by IT directors as a steer for areas of which they should be aware, included 'IT for Green' among its top 10 strategic areas for 2010, saying: "IT can enable many green initiatives. The use of IT, particularly among white-collar staff, can greatly enhance an enterprise's green credentials. Common green initiatives include the use of e-documents, reducing travel and tele-working. IT can also provide the analytic tools that others in the enterprise may use to reduce energy consumption in the transportation of goods or other carbon management activities."

This year, IT directors in Europe are having to help their organisations get to grips with specific additional environmental legislation. The Carbon Reduction Commitment programme is mandatory for businesses in the UK and is designed to help reduce the UK's overall carbon emissions by 80 per cent by 2050. Companies that have a single half-hourly electricity meter installed need to register for the scheme between April and September 2010. The likelihood is that similar legislation will eventually be introduced around the world as countries try and rein in their carbon emissions.

David Bicknell *has been a writer and editor for 20 years. He is a former news and US editor of* Computer Weekly *and covers a range of issues from ICT to business and technology. He is director of the C8 Corporate Media Bureau at C8 Consulting and is also co-author with Tony Collins of a book,* Crash, *about IT project management*
Web sites:
www.davidbicknell.com
www.c8consulting.co.uk

Control printing

One small way of achieving that is to take greater control of printing within organisations. A 2004 survey commissioned by Lexmark showed that board-level managers are alarmingly ignorant about the cost of print. Overall, 61 per cent of finance directors had no idea at all of the cost of document production in their business. Printing is considered to be a necessity rather than a luxury. As a result, many finance directors neither plan to cut print costs, nor do they see document production costs as critical to financial budgeting.

However, taking control of the print estate can help organisations to drive down costs, improve organisational efficiency, help the environment and the green agenda and improve cultural and operational issues.

The problem often lies in the fact that, in many organisations, the print estate is not centrally managed. This lack of control and management produces an environment where cost and waste can grow exponentially with little or no control. For example, in the UK a company with 500 employees spends £42,000 on wasted prints a year. For a waste reduction programme to be successful, there is a need for someone to take ownership of the problem, to install a decent print management solution to monitor device usage, and to fully optimise the print estate.

One solution I came across, Watchdoc, (http://www.doxense.com/) tracks and reports on print