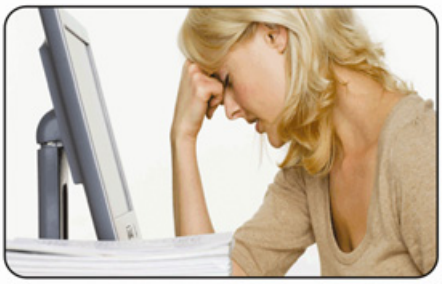
April 2011

Volume 20 • Number 4

Smart Card & Identity News

Smart Cards, SIM, Payment, Biometrics, NFC and RFID

www.smartcard.co.uk



Sony Breaks Chip & PIN?

Sony has shut down its PlayStation network after admitting an intrusion that risks the data of 77 million users including names, addresses, birthdates, passwords and credit card numbers, in fact just about everything a hacker might need to financially rob you. What is the point of Chip & PIN if you can get and misuse this sort of information on-line?

Surely, we are reaching some threshold on internet payments where consumers are going to revolt. It is totally unacceptable that the personal data and credit card details of 77 million people can be exposed.

Historically, this is not the biggest exposure that goes to Heartland Payment Systems who gave up over 130 million debit and credit card numbers in 2008/2009.

Continued on page 4….

Smart Card & Identity News
Is published monthly by
Smart Card News Ltd

Head Office: Smart Card Group, Anchor Springs, Duke Street, Littlehampton, BN17 6BP

Telephone: +44 (0) 1903 734677

Fax: +44 (0) 1903 734318

Website: www.smartcard.co.uk

Email: info@smartcard.co.uk

Editorial

Researcher – Patsy Everett

Technical Researcher – Dr David Everett

Production Team - John Owen, Lesley Dann, Suparna Sen

Contributors to this Issue – Dr David Everett, Sean Glynn, Tom Tainton, Suparna Sen, Gareth Ellis, David Gibson, Peter Tomlinson

Photographic Images - Nejron - Dreamstime.com

Printers – Hastings Printing Company Limited, UK

ISSN – 1755-1021

Disclaimer

Our Comments

Patsy Everett

Dear Subscribers,

The media this month is full of stories on smart phones and tablets all seemingly competing with Apple. Just at the end of the month however we have heard the problems that Sony has had with intruders on their network revealing the personal details of 77 million users as described in our lead article. And not to be overlooked Nokia is now facing those difficult decisions necessary for re-engineering the organisation, today they have announced 7000 people will be leaving the company.

The tablet revolution is interesting. I always felt that a small light touch screen device was the ideal portable computer. The other half of the household is even more gadget mad and has been experimenting for the last 10 years or more, the NEC Versa comes to mind as one of the early candidates for Microsoft's tablet software. We have gone through many incarnations including a more recent HP touch device with Windows 7 but none of them really captured the imagination. Then came the iPad, I can honestly express a totally unbiased view, perhaps even a little cynicism but hey this device is great. It is what you always wanted as a really useful PDA (I'll bet you've forgotten – Personal Digital Assistant, do you remember the Palm Pilot?). Anyway it seems like I'm to get the iPad one when he upgrades to the iPad 2. Apparently you have to have a camera – why?

Not only does it do email, calendar and web browsing but you can even read books under the Amazon Kindle banner. There really isn't a problem carrying 20 books around with you and unlike the Kindle they can be in colour. OK hands up I admit that in the full midday sun that screen is a bit hard to read but in the shade with a gin and tonic its shear bliss, just waiting for my own machine, sharing is a pain!

Now watching the others trying to catch up is interesting, Google's Android OS is of course gaining momentum but there is no obvious challenger to give Apple a problem just yet. With the iPad 2 people complain, the camera is not good enough, there is no Flash and much more, but let's not kid ourselves this device works with a vengeance. Everything is more than fit for purpose and I've long since been educated this is the way to think in business.

The Flash argument seems to cause the most excitement but it's really not a problem, if you want to watch Flash videos there are browsers like Skyfire and iSwifter that can handle that plus applications from many content providers that handle their content directly such as the BBC for example. What I hadn't fully appreciated was the problems that you can have with Flash animation on a touch screen where you have to decide what to do between hovering and touching, apparently this is going to be a problem with all touch screens when trying to work with Flash animation.

Back at the ranch we have been having lots of security discussions about these new smart phones and tablets, they are of course going

to have problems, I think we all agree that but actually we think the biggest understated problem is lost (and stolen) phones and laptops/tablets. Both Apple and RIM have their enterprise solutions for security and without arguing the finer points we really wonder why Nokia has missed this angle. Clearly they miscalculated the explosion of smart phones and should have reacted much quicker but where is the enterprise offering, presumably it's going to be Windows? I suspect a lot more people are going to jump ship than the 7000, and somehow or other Nokia's strategy just seems like too little too late.

Patsy.

Contents

Regular Features

Industry Articles

Events Diary

May 2011

2-4	Cards South America 2011, Sao Paulo, Brazil - http://www.cards2011.com.br/
16-19	IFSEC 2011, NEC Birmingham, UK - http://www.ifsec.co.uk/
17-18	Cards Middle East 2011, Abu Dhabi, UAE - http://www.terrapinn.com/exhibition/cards-middle-east/
17-18	Mobile Money World Middle East 2011, ADNEC - Abu Dhabi, UAE - http://www.terrapinn.com/2011/mmwme/
25-27	The 5th Annual Payment China 2011, Beijing, China - http://www.paymentchina.com/
26	Next Generation Mobile Devices 2011, London, England - http://www.avrenevents.com/

June 2011

13-15	Prepaid 2011, London - http://www.prepaid-conference.com/
20-21	Contactless Cards and Payments, London - http://www.smi-online.co.uk/events/overview.asp?is=8&ref=3515
28-29	SIMposium 2011, Berlin, Germany - http://www.simposiumglobal.com/

Source: www.smartcard.co.uk/calendar/

Sony Breaks Chip & PIN? …. Continued from page 1

In theory, you might argue that it shouldn't matter if somebody knows your credit card number, what really matters are that they shouldn't be able to use it. In other words you shouldn't be able to make a payment by just providing somebody's credit card number. And that's the simplicity of the argument the consumer must be involved in every transaction but with varying degrees of assurance and in the extreme case by the use of a Chip and PIN.

As a consumer I don't believe it is acceptable that I have to trust every merchant to handle my credit card information securely, and clearly they don't as the case in point with Sony. I would go even further and suggest that it is not economically viable to build a fool proof secure system to manage sensitive data through an intermediary, the only way is end point security and then of course you do have to trust that. However depending on the organisation involved, typically the bank that manages your account then the odds are more in your favour.

So if we have to have intermediaries such as merchants then it's back to some form of authentication just like Chip and PIN and it shouldn't be possible to go around it which is why the title of this article suggests that Chip & PIN has been broken by Sony's lax security attitude.

The question then becomes how do we pay on the internet? Clearly user name (or email address) and password don't hold up as a forward thinking strategy (PayPal are you listening). So dynamic passwords or One Time Passwords (OTPs) are a step forward but they can be painful to manage. Devices such as the RSA SecureID token seem great but then in March this year RSA was obliged to report that their system had been breached and that sensitive data may have been discovered.

The banks have been promoting the Chip Authentication program (CAP) that uses authentication/signature widgets (i.e. calculator size devices) that can authenticate a transaction using your EMV payment card. The Security team at Cambridge University have pointed out some vulnerabilities that are possible with the implementation of such an approach but their main point is that consumers find this widget inconvenient to use (for which I agree) and that they would prefer some reader attached to the PC. And then the researchers point out you have reached hackers paradise, the land where everything can be modified without you knowing until it is too late.

Others dismiss this PC approach as suicide and explain that what you really need to use is your phone, some suitable software application, now I don't know what newspaper they are reading but they seem totally unaware that the modern smart phone is no more secure than a PC. In fact I would go further, I think that the current state of Mobile Phone operating systems is probably less secure than the PC.

The reality is that at the end of the day you need some trusted hardware object that contains a secret that can be proven without revealing the secret, a bit of clever cryptography can do this. What you can then do is to be assured at least that this object was involved in the transaction. So in short, you need a secure element in the phone, NFC I hear you say, well unfortunately most phones seem to be relying on the SIM for the secure chip. However help is at hand, secure MicroSD cards are now becoming available (info@microexpert.com) which can indeed provide a shared security object but I suspect we are going to hear more horror stories before it starts to catch on.

By Dr. David Everett, Smartcard & Identity News

Cases of UK fraud on the rise as Experian reports 11% increase

By Tom Tainton, Smartcard & Identity News

Fraudulent applications for credit and financial services saw an 11% surge in 2010 compared to 2009, according to a report by Experian, a global information services company. 7 in every 10,000 loan applications were deemed to be fraudulent, an increase from 5 in 2009, with fraudsters responsible for 60% of cases. As the effects of the recession tighten its grip on the UK population, experts suggest the overall 11% growth in insurance fraud could continue to rise.

Identity fraudsters have targeted bank current accounts as a means to gain access to the lucrative realms of credit card fraud. Experian's report revealed that credit card fraud levels jumped to 19 in every 10,000 applications in 2010 – with criminals accounting for more than 80% of fraudulent attempts.

Peter Turner, Managing Director of Experian Interactive, said: "Our research shows that fraudsters are becoming increasingly sophisticated and more menacing than ever before. It is important to have proper safeguards in place to protect your identity such as ensuring that you keep your pins and passwords private."

The preferred method of attack for both types of fraud is 'current address fraud', a technique whereby an individual has their mail intercepted or redirected. However, it isn't just criminal activity on the rise. Experian's analysis showed that first-party fraud, when an individual knowingly creates a false picture of their personal circumstances to secure extra credit, now accounts for 56% of detected fraud attempts, up from 39% last year. The biggest culprits for first party fraud were considered to be single people on limited incomes, as well as young professionals with a university education.

The typical targets of first party fraud were insurers and mortgage brokers. In fact, a whopping 97% of bogus mortgage applications and 80% of false car insurance claims were committed by first party insurers. Fraudulent mortgage attempts which experienced a 14% rise in 2009 involved individuals lying about their employment prospects and personal finances. The report also revealed that motor insurers have been hit by applicants failing to disclose penalty points or previous convictions.

Customers are having their personal details exposed across the pond, too. America's largest mobile phone carrier, Verizon, sheepishly informed their customers that it had been a part of a data breach when an anonymous hacker had infiltrated the online marketing firm, Epilson, which oversees Verizon's email database.

Epilson, who send more than 40 billion emails per year for over 2,500 clients, warned that customers who responded to the hoax emails and logged onto false bank sites could risk having their login details stolen by fraudsters. Around fifty other companies, including banks such as Chase and retailers such as Best Buy, also had their email addresses exposed in one of the largest attacks in U.S history. Other large firms such as Marks & Spencer were also affected.

In an effort to develop a universal standard for identifying online users, the US government announced plans for a National Strategy for Trusted Identities in Cyberspace (NSTIC). The aim is to enable individuals to use a single secure verification mechanism to access a wide variety of different services. For example, an 'online ID' that allows somebody to access email, online shopping and social networking sites. To dispel any suggestions of creating a Big Brother environment, the White House insist the system will be driven by the private sector, reporting that the verification tool could be a smart card or even a smart phone application.

Back in the UK, there's not a similar scheme in the pipeline. With little or no nationwide precautions in place, fraudsters are free to run riot and focus their attentions on the UK's most 'at-risk' individuals.

According to Experian, Britain's most vulnerable are, unsurprisingly, the wealthy and influential. The visible wealth and ability to access substantial credit lines makes them three times more likely to be targeted for fraud than the national average.

London remains the fraud capital of the United Kingdom, with Birmingham and Slough the only areas in the top 10 'first party hotspots' outside the M25. For every 10,000 adults in Greater London during 2010, there were seven fraudulent attempts – twice the number of attempts in the North-West – the next busiest region.

The Experian Fraud Report suggested that identity fraudsters are increasingly targeting residents of commuter towns such as Reading, Basingstoke and High Wycombe. As fraudsters fine-tune their strategies or turn their hands to new tactics, their targets become increasingly widespread, focusing on those with generous disposable income as well as individuals who flat-share or rent their properties.

Workers stealing your data - the 2011 headache – can it be stopped?

By Sean Glynn, Credant Technologies

Sean Glynn

Information is one of the primary competitive weapons and business enablers for organisations of all kinds. The ability to provide the correct information to educate workers has driven a proliferation of information sharing, but with it has come significant risk. The actions of users who intentionally or accidentally cause damage to an organisation are now one of the most complex and difficult to manage problems facing IT security teams. So, how can you thwart the people you trust? This article examines some of the important aspects of insider threats and offers guidance to reduce the risk.

While much has been written on the subject of the insider threat, it still remains one of the most contentious and difficult to manage areas of information security policy. It goes against the grain to believe an employee is capable of stealing information – yet it happens.

So exactly how big is the risk from insiders?

In short, it depends greatly on what we define as an insider attack and the role that insiders play in breaches. The 2010 Verizon Risk Team Data Breach Investigation Report states that almost half (48%) of studied breaches are caused by insiders (an increase of 26% on 2009). As our understanding of the role of insiders in data breaches develops, so does our understanding of the complexity of attacks facing organisations and the difficulty in maintaining the balance between free information flow and good security.

Understanding the insider attack

At the most basic level, there are two kinds of insider attack: malicious and non-malicious. 2010 statistics from The Open Security Foundation found that almost three times as many breaches are caused by accidental insider activity than malicious intent. In fact, non-malicious breaches will often occur through normal usage of information and especially through avenues such as email, loss of laptops or storage media, and exposure to non-authorised parties within the organisation.

As users carry increasingly large quantities of information on mobile devices such as laptops and smart phones, and on removable media such as thumb drives, the risk of breaches caused by accident will continue to rise. Statistics show that enterprise organisations lose large numbers of laptops every year, and in 60% of the cases the device is simply misplaced by the owner.

While non-malicious insider breaches are a growing concern, most security organisations are focused primarily on preventing the actions of malicious insiders. A malicious insider can, and often will, cause damage over a long period of time, and may also be a significant contributory factor in external breaches too. In CERT's "Common Sense Guide to Prevention and Detection of Insider Threats," the authors identify four types of malicious insider attack:

1) Attacks aimed at sabotaging IT resources (often out of a desire for revenge)
2) Attacks that steal (or modify) information for financial benefit
3) Attacks that steal (or modify) information for business gain
4) A miscellaneous group of attacks associated with unauthorised access but not necessarily for personal gain

Attacks aimed at sabotage and those for financial gain make up the bulk of the cases the authors examined, however given the difficulty of tracking when sensitive information is stolen and handed over to a competitor, it is entirely possible that thefts for business advantage are under-represented in any study.

Avoiding the insider attack

The challenge of managing risks and reducing the likelihood of an insider attack is that it requires a close correlation between technical information, security controls and human resources and management. This need for the intersection of the human element with monitoring and other controls is precisely what makes insider attacks, especially malicious ones, so difficult to detect and prevent.

In the previously mentioned CERT whitepaper on preventing insider attacks, the authors suggest 16 practical measures, which can be adopted to help reduce risks from malicious insiders:

- Consider threats from insiders and business partners in enterprise-wide risk assessments
- Clearly document and consistently enforce policies and controls
- Institute periodic security awareness training for all employees
- Monitor and respond to suspicious or disruptive behaviour, beginning with the hiring process
- Anticipate and manage negative workplace issues
- Track and secure the physical environment
- Implement strict password and account management policies and practices.
- Enforce separation of duties and least privilege
- Consider insider threats in the software development life cycle
- Use extra caution with system administrators and technical or privileged users
- Implement system change controls
- Log, monitor, and audit employee online actions
- Use layered defence against remote attacks
- Deactivate computer access following termination
- Implement secure backup and recovery processes
- Develop an insider incident response plan

While these are focused on dealing with intentional attacks, some will also reduce the risk of accidental incidents.

In support of these initiatives encryption software can play a key role. Encryption presents the capability to render sensitive information unreadable to unauthorised users, and most importantly, once encrypted, the 'protection' stays with the data wherever it resides. A further benefit is that it helps enforce tight controls over who can access the information. Finally, because encryption is highly data-centric, it reduces the value of the information itself (and the liability associated with it) to a third party. An encrypted file on a laptop may contain highly proprietary information, or sensitive personal data covered by one of the many industry and legislative mandates, but if it is properly encrypted, the information remains protected even if the laptop is lost or stolen.

In the event of an incident, encrypted information is often exempt from some of the more punitive requirements for notification and will therefore significantly reduce the cost of an accidental breach. In their 2009 study, "Cost of a lost laptop", the Ponemon Institute reported that the presence of encryption on a lost laptop reduced its cost to the organisation by over $20,000.

Addressing the threats from insiders is always an emotive subject. While your organisation will always want to hire trustworthy employees, it is an irrefutable fact that accidental breaches occur with startling regularity, and that a single, well motivated malicious insider can cause immense damage. The nature of the interaction between IT and business units is also changing, fuelled in no small part by the availability of maturing Cloud offerings. As a result, the complexity and nature of the insider threat is too.

While no single technology can ever provide complete security, encryption will continue to play a central and pivotal role in both reducing the risk of a breach and limiting the damage to your business.

World News In Brief

Nokia Strengthens Smartphone Portfolio

Nokia announced the Nokia E6 and the Nokia X7, two new smartphones aimed at business people and entertainment enthusiasts. The two devices are the first Nokia smartphones to contain the updated Symbian software nick-named 'Symbian Anna.

The Nokia E6 is a sleek business smartphone with a full QWERTY keypad and a high resolution touch display. The Nokia E6 offers exceptional battery life and the best out-of-the-box Microsoft messaging experience on a business smartphone, including access to Microsoft Exchange, Microsoft Communicator Mobile and Microsoft SharePoint.

The Nokia X7 is an entertainment-focused smartphone with a large 4" display ideal for gaming, and an 8 Megapixel camera for capturing pictures and HD-quality video.

The Nokia E6 and Nokia X7 are also the first smartphones to contain the complete update of the Symbian software user experience.

No Prosecution for BT and Phorm

The Crown Prosecution Service (CPS) has decided not to consent to a request from an individual to begin a prosecution of BT Group Plc and Phorm Inc in relation to alleged unlawful interception of internet browsing data.

Prosecutions for unlawful interception require the CPS's consent. After a thorough review of the available evidence, the CPS has decided there is currently insufficient evidence to begin a prosecution under section 1 of the Regulation of Investigatory Powers Act (RIPA) 2000 and it would not be in the public interest to proceed any further.

The PageSense software (later known as Web Wise), created by Phorm and used by BT, stored a cookie on a user's computer and covertly gathered selected information on their internet browsing habits. The software used this data to automatically target web-based advertisements at the user.

An unannounced trial of this technology, involving about 18,000 BT customers, took place during 2006, when BT in partnership with Phorm, admitted of carrying out secret trials on 18,000 user accounts with technology from 121Media, which later became the targeted advertising company Phorm.

The secret trials appeared to breach the Regulation of Investigatory Powers Act (RIPA) 2000, which makes it an offence to intercept internet traffic without consent or a warrant.

Andrew Hadik, reviewing lawyer for CPS London's Complex Casework Unit, said: "We have thoroughly reviewed all of the material supplied by the individual who wished for us to consent to a prosecution, as well as the evidence provided by City of London Police, BT and Phorm. On the basis of the evidence gathered and with advice from legal and technical experts, we have determined the extent and seriousness of the alleged criminality. At present, the available evidence is insufficient to provide a realistic prospect of conviction. In the vast majority of cases, we would only decide whether to prosecute after the investigation had been completed and after all the available evidence had been reviewed. In rare cases, however, it may become clear prior to the collection and consideration of all the likely evidence that a prosecution would not be in the public interest".

3.5 Million Texans at Risk from Identity Fraud

The Texas Comptroller's office has begin sending letters to notify a large number of Texans whose personal information was inadvertently disclosed on an agency server that was accessible to the public.

The records of about three and a half million people were erroneously placed on the server with personally identifying information.

The records contained the names and mailing addresses of individuals. The records also included Social Security numbers, and to varying degrees also contained other information such as dates of birth or driver's licence numbers - all the numbers were embedded in a chain of numbers and not in separate fields.

The information was in data transferred by the Teacher Retirement System of Texas (TRS), the Texas Workforce Commission (TWC) and the Employees Retirement System of Texas (ERS).

The data files transferred by those agencies were not encrypted as required by Texas administrative rules established for agencies. In addition to that, personnel in the Comptroller's office incorrectly allowed exposure of the data. Several internal procedures were not followed, leading to the information being placed on a server accessible to the public, and then being left on the server since early last year without being purged as required by internal procedures. The mistake was discovered on the afternoon of March 31, at the time the agency began to seal off public access to the files. The agency has also contacted the Attorney General's office to conduct an investigation on the data exposure and is working with them.

Visa Gifts New 'Combi-Card' to Dubai

Dubai riders will soon get to use a new type of Visa card known as 'Combi-card' for paying fares on buses, trains and water taxis. People just need to swipe the 'Combi-Card' in stores or touch against sensors fitted on buses or trains and to parking meters to enjoy their rides. This is the first time such a 'Combi-card' is to be made available in the Middle East.

Elizabeth Buse, the group executive for Visa in the Middle East, Asia-Pacific and Central Europe believes, "We see transit as a huge opportunity. Consumers make transit transactions so frequently; it keeps Visa top of mind and top of wallet. It will increase our transactions, not just in the transit arena but in general, as this becomes people's primary payment device".

The new type of Visa card will be available in the coming months to those who qualify for credit cards through Emirates NBD. The Combi-card is a part of Visa's broader strategy to capitalise on different growth markets in the UAE and in the Middle East.

Interview with Stephen Watts, Sales Director of SecurEnvoy

By Tom Tainton, Smartcard & Identity News

Tom Tainton

Who are SecurEnvoy?
SecurEnvoy is pioneering the authentication space to meet the growing security needs of modern businesses.

Today's organisations need watertight security, particularly now that 'cloud computing' has empowered users to access data any time, from anywhere. However, they also need cost savings, optimum productivity and a renewed focus on environmental action. So SecurEnvoy's ethos is simple: Give control back to businesses and users without compromising on security or access.

By strengthening mobile security without breaking business budgets, SecurEnvoy helps its customers manage risk, maximise reward and retain control of sensitive data.

Can you tell us about SecurAccess and why it is so unique?
Unlike traditional authentication solutions, SecurEnvoy's suite of products can be installed and integrated into existing IT systems quickly. And crucially, they avoid the need for much of the additional cost or remote deployment of the traditional approach to security software, creating an unprecedented zero-footprint solution while ensuring long-term cost benefits.

What are the benefits of token-less solutions over two-factor authentication?
SecurAccess from SecurEnvoy turns any mobile phone that can receive SMS into a ready-made authentication device. This pioneering zero-footprint solution cuts costs by using hardware that is already in circulation. Unlike traditional tokens that take months to deploy and replace, SecurAccess can roll out more than 18,000 new remote staff per hour without the pain, cost or environmental impact created by legacy hardware distribution.

Experts have suggested 2011 is the year when token less technology will take off. Why now?
There are 5 billion handsets the same number of credit cards in the world – every one of those handsets could be an authenticator for SecurEnvoy! RSA have had a severe security breach in the last few weeks as most of the industry knows. However our solution doesn't rely on the same standards that RSA do. Our competition all use disparate databases and store token seed records in these servers, we don't and that's what makes our solution unique, secure and allows us to guarantee that such a breach the competitors have had would not happen to us!

How do you see the market developing in the future?
If you've been reading our blog or newsletter over the last few months, you'll know that traditional physical tokens have significant drawbacks, being expensive to deploy, difficult to maintain and liable to be lost by the user (not to mention the inconvenience to each remote worker needing to remember and carry their own token with them at all times). SecurICE gives companies a secure option when emergency situations arise, such as when unusually bad weather disrupts transport routes, forcing users to work from home. SecurEnvoy's solution allows companies to easily and securely authorise users on to remotely accessible resources.

What are the challenges associated with token less technology?
Some of the challenges include real-time delays, deleting the SMS, and accessing SMS from remote places. We can overcome every one of these issues. Our cases studies prove this. Andrew Brenson, acting Chief Information Officer for Save the Children UK, quickly realised the benefits that SecurAccess offered, saying: "I was concerned the reception available to our staff in some locations would mean they were unable to access the authentication codes. If you're in the middle of Africa and you try and log in you need to have a robust system of receiving the one-time pass code for safe access."

Andrew continued: "When I considered that the majority of staff had mobile phones already, and could receive the one-time authentication code, it made sense to adopt the SecurAccess system."
Most authentication systems work with pass codes that require a real time active GSM connection with no delays, which creates a problem for people working in remote locations and other places with limited mobile reception. But SecurAccess allows aid workers in the field to use pre-loaded pass codes. The next required code is sent during the previous authentication. So, the pass code stays on the phone until it is needed, doesn't expire and works even without mobile reception.

What next for SecurEnvoy?
SecurEnvoy is looking to develop mobile device apps in 2011 that will give users more choice of how they receive their token less two-factor authentication pass code. Users will still be able to receive SMS pass codes as usual, but some users will want to access a dedicated app that acts as a soft token and offers other functionality related to two factor authentication. Although SMS messaging is a secure cost-effective way of delivering pass codes, using a dedicated app would be appropriate for some users and convenient for others.

Malicious SQL Injected in Millions of Websites

By Suparna Sen, Smartcard & Identity News

Suparna Sen

Earlier this month, a massive worldwide cyber attack shook the security industry and organisations alike. Hundreds and thousands of websites were injected with malicious SQL[1] codes using fake software called the Windows Stability Centre. Windows Stability Centre re-directed and linked compromised websites to a fake software sales operation that warned people against viruses (that were actually non-existent) in their computers. Windows Stability Centre posed as a Microsoft Corp security product and urged people to pay for software to fix problems with their computer.

The cyber attack was first detected on March 29 by the US-based Websense, a web, data and email content security firm. Initially, the number of compromised websites was 28,000, but gradually the number rose to over 4 million by 3rd of April (as reported by Google). Ars Technica predicted the malicious attack has hit almost 700,000 websites so far. (April 1, 2011)

Named as the 'Lizamoon attack' since the first domain that the victims were re-directed to was lizamoon.com, the SQL attack directed netizens towards various fake domains (there were about 27 rogue domains founded to-date by security researchers).

Websense's senior manager for security research, Patrik Runald said: "the scale of the attack was worrying". Websense found online criminals used Microsoft SQL Server 2003 and 2005 to launch attacks on websites.

Now, why did the hackers specifically chose Microsoft SQL Server 2003 and 2005?

Both the Server 2003 and 2005 system use royalty-free MSDE or Microsoft Database Engine, which is particularly designed for individuals or small workgroups. Hackers took the advantage of the royalty-free database engine to gain easy entry to different websites that actually belonged to individuals and small businesses such as astronomy groups, social clubs, hospitals, sports teams and funeral homes.

These flexible Servers can easily be re-configured by hackers, at any time, to gain access to the master database, which contains all the settings for SQL Server and all SQL login IDs and data of the connected servers.

There was even news of hackers hitting web links connected with Apple's iTunes service. Websense's Patrick Runald wrote on the firm's blog, "This did not mean people were being redirected to the bogus software sites. The good thing is that iTunes encodes the script tags, which means that the script doesn't execute on the user's computer".

Graham Cluley, senior security analyst at Sophos, said: "Home PC users were probably the most likely victims of the attack. Attacks like this one do underline the poor security that exists on many websites on the internet, including sites belonging to well-known organisations and brands". Many organisations are making it far too easy for the hackers to inject malicious codes into computers and websites by not taking adequate, up-to-date security measures.

At present, the re-directs to rogue websites have ceased, and the websites selling rogue security software has been shut down.

Speaking on "Top Cyber Attacks in 2011", Michael Gregg, Ethical Hacker provided some interesting and useful tips on how to secure your PC from malware's and viruses.

- Keep anti-virus software up-to-date and run regular scans
- Check what links you get either on websites or via emails and never open any suspicious email
- Fake SMS or text SMS often pretends to be from your bank and are tricks to get your PIN number, etc. Always check with your bank before providing any details to anyone.

- While using smartphones, avoid third party application stores or paid applications offered for free. The offers can be a trap to rob your personal details and money. Instead, always visit a genuine Apple store or buy smartphone accessories from valid suppliers. Fake websites may tell you to click on a link to download a piece of software that appears to be anti-virus, but actually is malware infected.

Here's the link to his video: http://www.youtube.com/watch?v=BQw5cna1ZXs

Note: On the 11th of this month, hackers injected SQL on the US-based software security firm Barracuda Networks' corporate website. The attack led to the compromise of leads, channel partners and some Barracuda Networks employees 'names and email addresses.

However, Barracuda Networks successfully detected the attack by running an automated script on the company website. It found SQL was injected in a simple PHP script that serves up customer reference case studies.

[1] *SQL is a malicious code that is dropped into a computer to exploit the machine's security weakness. In the above incident, the injection meant a particular domain appeared as a re-direction link on the web pages visited.*

World News In Brief

Deutsche Bahn and NXP Strengthens Touch&Travel

Deutsche Bahn and NXP Semiconductors N.V. will continue to work together on "Touch&Travel" mobile ticketing scheme in Germany. The "Touch&Travel" system was started as a pilot project in Germany in 2008, and now both the companies are trying to introduce the system in the market. The contactless, NFC-based scheme will enable riders get e-tickets based on NFC-enabled mobile phones to travel in all public transport across the country.

Using "Touch&Travel", passengers can conveniently purchase tickets by bringing their mobile phone close to the "Touch&Travel" Touchpoints. Data is securely transmitted through the existing mobile phone network and payment for travel is done. The fare is calculated automatically and billing is done on an everyday basis.

China Cards Profits to Soar as UnionPay Monopoly Set to End

Lafferty Group, a global financial industry research company has announced that strong and credible rumours are circulating in China that China UnionPay, the state-owned payments company, will lose its nationwide cards network monopoly in two years. The news follows a recent complaint by Visa, the larger of the two global cards networks, to the World Trade Organisation (WTO).

Such a move is likely to lead to substantial increase in merchant fees for card transactions in China, leading in turn to substantial increases in income for cards issuers. Currently, average merchant fees in China are 0.57 percent, compared with 2.37 percent in the US and 1.29 percent in Western Europe.

"People's Bank of China (the central bank, which owns CUP) told UnionPay that the present position was a cut-and-dried case of unfair competition that could not be defended and said it has two years to prepare for competition from Visa and MasterCard", a Chinese cards executive told Lafferty Cards Insights. Visa and MasterCard had not returned calls by the time this story went public.

China's credit cards industry recorded a small pre-tax profit in 2010 for the first time in its history, according to Lafferty Group's World Cards Intelligence research service. The industry's $251m overall profit represents a demarcation line for China's cards business as issuers finally begin to see a return on the enormous investment pumped into the market over the last 10 years. Lafferty Group forecasts that pre-tax profits will continue to expand, reaching $2.4 billion by the end of 2015.

Chase Card Services - First Major U.S. Bank to Issue Chip-and-Signature Technology

Chase Card Services, a division of JPMorgan Chase & Co. has become the first major U.S. bank to issue chip-and-signature, a credit card with EMV chip technology that provides consumers with better ease-of-use and stronger security while travelling abroad.

Chase will first unveil chip-and-signature on the JPMorgan Palladium credit card in June, a card serving customers who frequently travel abroad, and later to other Chase credit cards within the year.

NFC: virtual world vs. banking world

By Gareth Ellis, Solution Consultant, ACI Worldwide

Gareth Ellis

It is clear that Near Field Communication (NFC) technology is making a huge impact in the financial services and payments world. Whether or not this leads to new products and services being launched – and adopted by consumers – we will have to see. But one thing is clear: there is a large majority of organisations – including many banks – who feel that there isn't yet a strong enough business case to get involved. In fact, a recent poll at the GSMA Mobile World Congress found that 76 per cent of the industry believes NFC payments technology is still at least 24 months away. But if financial institutions don't get in on the act soon, will they be overtaken by more nimble payments providers from the 'virtual' world, for example PayPal, Google and Apple? A number of relationships are currently being formed between players from the virtual world and the banking world, but which side will ultimately profit from NFC payments?

On the virtual side, Bling Nation – now powered by PayPal – allows consumers to use NFC stickers to charge items in the physical world to their online accounts. Meanwhile PayPal's iPhone app allows people to make payments in online stores and the company has just announced it is extending its remit to the offline bricks and mortar world, with the appointment of Don Kingsborough as vice president for retail and pre-paid products.

Google is in on the act too; all phones using the new 2.3 version of Google's Android operating system will be NFC capable. They are also looking to build a mobile wallet ('Cream') which will sit on all Android phones and could use NFC to perform contactless mobile payments. Add to that the fact that Google has recently acquired Zetawire, an e-wallet provider, and it makes you wonder how far Google is likely to go down the payments route. Meanwhile it looks like Apple's iPhone 5 and iPad 2 will not incorporate NFC in their latest releases, but rumours are that they are still investigating a closed loop proposition that would allow users to charge payments in the physical world to their iTunes account rather than a traditional credit card. This type of business model would allow these Internet businesses to cut out the card schemes and tap into a lucrative payments market traditionally cornered by the banks. All this sounds fantastic, but there are some challenges that they will face.

First of all, why would merchants want to get involved? A lack of NFC readers at the point of sale is a major barrier seen by many in the industry as the main culprit behind slow adoption. Furthermore, merchants are not keen on cluttering up their shops with more than one POS device, so how can these competing solutions all make use of the same device? Then there is the problem of getting enough people to have NFC-enabled handsets to make this a reality. Finally, who in the industry can provide the global standards and specifications that can provide the framework for multiple stakeholders to take part and succeed?

On the banking side, it is clear that there exists a massive payment infrastructure for cards, providing very functional acquiring, switching, authorising, clearing and settlement. From a technical perspective, it would be relatively simple operation for banks to view phones as "virtual" cards, add these "virtual" cards to their existing card management system and bolt on a capability to download payment apps to their customers' smartphones. Obviously, there are many challenges in such a project, but the technical challenges this provides are probably not as great the challenges around defining the business case.

The primary difference between the virtual and banking approaches seems to be that although the phone could be viewed as simply a new token with which to make payments, the introduction of a phone into the payment business brings in a large number of new stakeholders. Mobile network operators, handset providers, Trusted Service Managers (TSM)s and virtual wallet providers to name but a few. This makes the business case less attractive to banks, leading them to either adopt a defensive position on mobile, or more often, to adopt no position at all. But by not doing anything, the banks are playing into the hands of the virtual players, despite the challenges they face as outlined above. These new, flexible players, who do not have outdated legacy banking systems to maintain, but do have experience of switching, billing and settling and are therefore in a very strong position vis-à-vis the banks. They can move very quickly, have a younger, move technical-savvy customer base, who are more willing to try out new payment methods and they have the financial backing to attack the market

As the fight between the virtual providers and the banks commences, we are seeing a small number of forward thinking banks, partnering with mobile network operators, providing their customers with new contactless mobile payments methods: Barclaycard and Everything Everywhere being one example. But the vast majority are playing a waiting game, burying their head in the sand, not realising that the threat to their business is just over the horizon. But Banks must realise there is a massive opportunity here. Firstly, consumers have shown

that they want to use their phone in all areas of their day-to-day life, and that includes payment. Secondly, and importantly for banks, until the whole acquiring infrastructure has been upgraded, consumers will need both a phone and a card for payment, which should put the Banks in the ascendancy. Whether Banks will take up the challenge, is still not clear – we await the outcome with bated breath.

[1] http://www.finextra.com/news/fullstory.aspx?newsitemid=22299

World News In Brief

Google, Facebook Challenge French Data Law

Several well-known internet companies, including Google, Facebook and eBay have challenged the French government's plan to keep web users' personal data for a year. The legal challenge that will be heard by the France's highest judicial body, the State Council, is brought by The French Association of Internet Community Services (ASIC).

The law will be imposed on a wide range of e-commerce websites, video and music services and web mail providers to keep a host of data on customers, which includes all users' full names, postal addresses, telephone numbers and passwords. The data must be handed over to the authorities as and when demanded. Police, the fraud office, customs department, tax and social security bodies will have full right of access to the personal information of users.

The French Association of Internet Community Services believes "Several elements are problematic" in the law. Through the law, the French government is trying to put too much pressure on the internet companies. Moreover, the Association stated "passwords should not be collected and warned that retaining them could have security implications".

NXP Offers New UCODE I2C RFID Chip

NXP Semiconductors N.V introduced its new UCODE I2C chip, which features an integrated I2C interface and a large 3,328-bit user memory. The UCODE I2C Chip includes Gen2 UHF to embedded systems, providing bidirectional communication between a wireless reader and a microprocessor via an I2C bus. Customers can use the chip to configure various electronic devices such as smartphones, tablets, music players and game systems and can customise the devices remotely even when the device is not in motion.

UCODE I2C can quickly identify the serial number and the error logs internal to the device without opening it, resulting in saving time and energy. The UCODE I2C chip features 3,328 bits of EEPROM memory size, two independent front-ends, each of which can be enabled or disabled independently, as well as an RF or I2C interface which can also be disabled independently.

Vodafone to Sell SFR to Vivendi for GBP-7 Billion

The telecommunication giant Vodafone has planned to sell its 44% stake in the French mobile phone company SFR to Vivendi SA for GBP 7 Billion (7.95 billion-Euros). Vivendi SA is a Paris-based international multinational company with stakes in telecommunications, internet, music, television and film, publishing and video games. Vodafone is said to return 4 billion-pounds to its shareholders by buying back shares.

Vodafone's chief executive Vittorio Colao said in a statement, "The sale of our stake in SFR, at an attractive multiple, represents a significant further step in the execution of this strategy" - the Company's plan of selling assets in operations it no more controls. The UK-based Company's deal with Vivendi is said to be completed by June, this year.

Amazon to Roll Out Mobile Payment Service!

As per Bloomberg reports, Amazon is working towards starting its own mobile payments service. The service will be based on NFC or near-field communication and will enable customers to pay using their mobile phones or smartphones. There is news of Google, Microsoft and Nokia developing applications to suit Amazon's interest.

Amazon has already released its own Android Appstore, and has even introduced a music streaming/locker service that works with Android devices. According to Gartner, about 340 million mobile users use their phones to carry out mobile transactions to worth $245 billion in 2014.

Samsung and Visa to Offer Mobile Payments in 2012 London Olympics

Samsung and Visa have teamed up to provide mobile payment technology for the London 2012 Olympic and Paralympics. Both the companies are official sponsors of 2012 London Olympics.

The new NFC-based contactless mobile payment system will allow people pay using their Samsung Olympic and Paralympics Games mobile handset. Customers need to insert a Visa-enabled SIM card within their mobile phones, select the Visa mobile contactless application, click on pay and hold the cell phone in front of a contactless reader at the point of purchase to make payments. Visa has already started working with a number of banks and retailers across the world in a bid to make its contactless technology commercially successful. In London, more than 60,000 locations are accepting contactless payments.

Which? Launches Super Complaint against Excessive Card Fees

Which? a registered consumer charity, has submitted a super-complaint to the Office of Fair Trading (OFT) asking it to investigate excessive credit and debit card surcharges.

The consumer champion warns that these charges are unjustifiable and becoming increasingly widespread. While the cost to companies for taking payment by card is around 20 pence to process a debit card payment, and 1 - 2.5% of the transaction value for a credit card, researchers found dozens of examples of companies charging far higher fees.

Which? chief executive, Peter Vicary-Smith, says: "Consumers are really fed up with paying excessive card charges. So far, over 40,000 people have pledged their support for our campaign to bring these to an end. Low-cost airlines are some of the worst offenders, but excessive card surcharges are becoming ever more widespread, with everyone from cinemas and cabs to hotels and even some local authorities getting in on the act".

Visa and MasterCard support the campaign as the high fees being charged are damaging their reputation. The OFT has 90 days to investigate and decide whether to launch a full inquiry.

Watchdata Successfully Rolled Out 3 Million SIMpass

At the CARTES Asia 2011 conference, Watchdata announced that its SIMpass commercial deployment has exceeded the 3 million-unit mark.

SIMpass mobile payments system supports integrated transportation and campus payment applications onto a single mobile phone, and its low deployment costs and scalability makes it suitable for multi-industries applications. Presently, it has become the mainstream mobile payment technology in China.

Using SIMpass, China Telecom officially launched Yang Cheng Tong Card on 24 February 2011 to target the users in Guangzhou and Foshan. Guangdong residents are using the card to travel, dine and shop. In Dongguan, in addition to transport and supermarket payments, residents are enjoying the convenience of SIMpass mobile payment at farm produce markets.

Omni-ID and Extronics Sign RFID Global Partnership Agreement

Omni-ID and Extronics Ltd., a UK-based manufacturer of intrinsically safe and explosion-proof equipment, has signed a RFID Global Partnership Agreement. The deal is expected to accelerate adoption of passive UHF RFID tags for hazardous environments worldwide.

Extronics will certify Omni-ID's entire range of products for compliance to safety and performance standards for ATEX in Europe, Class 1 Div 1 in the U.S. and IECEx worldwide. The first product of the agreement will be unveiled in early April this year at the Hannover Messe 2011 trade show to be held in Germany.

Apple to Show World The Future of iOS & Mac OS X

To quote Mr. Philip Schiller, Apple's senior vice president of Worldwide Product Marketing: "At this year's five-day conference Apple will unveil the future of iOS and Mac OS, including exciting demonstrations of the new kinds of apps that developers can build using Apple's advanced frameworks and more than 100 technical sessions presented by Apple engineers". Apple's 2011 Worldwide Developers Conference (WWDC) will be held from June 6 to10 in San Francisco, USA.

Apple believes its live demonstration at the WWDC will help all Mac developers explore the latest advancements and capabilities of iOS Lion mobile operating systems.

How to Become Compliant With PCI DSS

By David Gibson, Director of Technical Services, Varonis Systems

David Gibson

PCI DSS was developed as part of a collaboration by MasterCard Worldwide, Visa International, American Express, Discover Financial Services and JCB. Their efforts have culminated in the standard that serves as directive and guideline to help organisations prevent the misuse of credit card data.

Who Needs To Comply

All merchants and service providers who store, process and transmit credit card information must undergo quarterly self-assessments as well as audits (vulnerability scans) by an Approved Scanning Vendor (ASV) and in accordance with PCI DSS Scanning Procedures.

Large merchants (i.e. more than 6 million transactions per year for all outlets including e-commerce) and service providers (i.e. more than 1 million transactions per year) must also undergo annual on-site audits performed by a PCI DSS Qualified Security Assessor (QSA). The audit is inclusive of all systems, applications and technical measures, as well as policies and procedures used in the storing, processing and transmission of cardholder and credit card information.

What Is Considered Sensitive Data

Per the standard, the following information is considered sensitive:

- Primary Account Number (PAN)
- Cardholder name
- Service code
- Expiration date
- Pin Verification Value (PVV)
- Security code (3 or 4 digit)

In accordance with the standard, merchants or service providers are not allowed to store the PVV or the security code that uniquely identifies the piece of plastic in the cardholder's possession at the time of the transaction. However, the PAN, cardholder name, service code and expiration date may be stored.

PCI Compliance Is More Than Just Securing Cardholder Information Within Databases

Many organisations naturally focus efforts for protecting cardholder information within databases, a challenge for which technical solutions abound. However, as breaches like Citigroup's and Pfizer's have shown, enterprises also face challenges controlling access to and dissemination of spreadsheets and documents that contain cardholder information. Exporting sensitive cardholder data out of databases is all too common, often done so that the information may be analysed as part of market research or be imported into other applications. In fact, 42 percent of enterprises hold customer data in spreadsheets as a matter of course according to Ventana Research, and these figures don't include the individual users who conduct such exports on their own for business analytics or other purposes.

In the case of PCI, it is important to protect not only databases, but also file shares and SharePoint sites that house these spreadsheets and documents. Organisations need to implement a comprehensive system for not only finding the PCI information that resides outside of databases, but also for authorization, access control and auditing of all unstructured & semi-structured data stores. When file shares contain any of the PCI-designated sensitive information, organisations need to audit, review, and tighten up access to these shared networked resources as part of their PCI compliance efforts.

[1] Citigroup Customer Data Leaked on LimeWire (2007): http://www.eweek.com/c/a/Security/Citigroup-Customer-Data-Leaked-on-LimeWire/

[2] Organisations Struggle To Manage Customer Data As Information Assets (2007): http://www.itbusinessedge.com/cm/community/features/guestopinions/blog/organizations-struggle-to-managecustomer-data-as-information-assets/?cs=22600

What Are The Costs/Risks Of Non-Compliance

Credit card fraud and misuse reaches into the billions of dollars annually. While the costs per incident may vary by merchant size, they include:

- Loss of income from fraudulent transaction
- Cost to reissue cards
- Costs of investigation and possible litigation
- Possible fines imposed by credit card companies
- Loss of reputation, customer confidence and business
- Possible loss of ability to accept credit cards for payment

PCI Compliance the Easy Way

There are five principles organisations need to address when seeking to comply with PCI DSS:

- Continual identification of relevant data
- A process to identify and revoke unwarranted access
- A process to configure and review logical access controls
- Proper separation of duties
- Evidence that these processes are being followed

Logical access control objectives are based on the principal of least privilege; access should be granted to only those resources that are required to perform a user's function. Many audit regulations now focus on proper access and use of unstructured data on file systems and SharePoint servers.

It stands to reason that wherever the organisation has permissions to write or read data, a data owner, or steward, should be designated to make decisions about who gets access, acceptable use, etc. Otherwise, decisions about that data are left up to members of IT, who have little organisational context about the data they are trying to manage and protect.

In order to identify an owner/steward, IT needs to know who is making use of data—analysing data usage over time provides actionable business intelligence on the probable data owner of any folder. Using these statistics, administrators can quickly see the most active users of a data container. Often, one of the active users is the data owner. If none of the active users is the business owner, he or she will likely work for the data owner, or at least know who the data owner is likely to be.

Data Owners/stewards need to be automatically involved in the authorisation workflows and reviews for their data. Automation should enable users to request access to data, route the requests to the data owner and other appropriate parties, execute the appropriate actions, and track each requests. Entitlement reviews, or attestations, should also be similarly automated and auditable.

While this may all seem an insurmountable task, software solutions are available to find PCI data, aggregate user and group information, permissions information, access information, and content information (which files actually contain PCI data) from directories and file servers. Sophisticated analytics can then be applied to reveal detailed data use, misuse, and determine rightful access based on business need. Using this intelligence, organisations can then:

- Continually scan for PCI data (the audit trail enables true incremental scanning for only changed or modified files)
- Protect data by removing overly permissive access controls
- Ensure on-going compliance with automated entitlement reviews, and authorization workflows
- Restrict unstructured data access to those with a business need for that data
- Automatically update access controls to account for changes in roles and file server contents
- Track and monitor file touches for each and every user
- Alert on behavioural deviations that may signal a possible data breach

Surely, the loyalty of your customers should be rewarded by securing their sensitive information. A breach doesn't just affect the person whose account has been emptied— it can affect your reputation if the violation can be traced to your door. Compliance is important, for every one in the chain, and it may be easier than you realize to not be the weak link.

eID and all that - all what? Information Assurance, that's what.

By Peter Tomlinson, Smartcard & Identity News

Peter Tomlinson

Late last year, two topics were in the spotlight both here and in the USA: secure eID, and the more general need for greater confidence in online services. Then there seemed to be a pause. Now there have been two significant advances, both involving publication of government strategies. On March 30th, the UK Cabinet Office published its composite strategy for ICT in government. On April 15th, the USA NSTIC team published confirmation that their national project for secure online ID is up and running and is open for multiple independent operators to provide eID credentials direct to the public.

Simultaneously, with the UK publication, the Parliamentary Public Administration Select Committee (PASC) held a public hearing: a witness session with Francis Maude (MP and Cabinet Office Minister) and Ian Watmore (Cabinet Office Chief Operating Officer). Here there was both clarity and doubt. More public sector services are indeed going to be provided online, with Cabinet Office vetting projects at the key milestone of funding approval. But confidence in the quality of those services continues to be questionable, much as was reported in the January and February editions of SCN, and the UK methodology is going to be specific to public services.

Comparing the two advances leads to an immediate conclusion: the USA programme will be taken global by the suppliers of the methodology for securing online ID and the associated transactions. It therefore makes sense for our public sector to go the same open systems route. The old cliché of Britain as a mid-Atlantic island applies, but for securing the online environment we have to avoid being insular in our attitudes.

First to another window into the same general area of web services: confidentiality and relevance in the collection and use of personal data, as illustrated by the recent launch of a customer loyalty card scheme from a regional real ale brewery with a small chain of pubs. Management of the loyalty card scheme is via the brewery's web site. On the registration page to which that web site sends you, they collect your name and street address so that they can personalise the loyalty card and send it to you by Royal Mail - no problem. They also demand date of birth and phone number and email address. What relevance to them are those additional personal data items? How will they use them? There isn't any explicit explanation. The brewery's Ts & Cs simply say that the data collected will not be shared with anyone outside their company, yet registration data is in fact collected and processed by a third party service provider on the third party's own web site.

It does make sense for the scheme owner to know the geographical distribution of applicants - the street address gives them that. They may even like to know the age distribution of the members, so I would not mind having to indicate my age range. But phone number and email address have to be optional, with a clear explanation of the use to be made of them. And the registration page and associated database really ought to be on the brewery's own web site. They may, however, continue to use a third party to manage the data - if so, we need to know that in the privacy statement.

That loyalty card is only for people who can legally purchase alcohol, so the brewery has to require applicants to declare that they are over 18. But there is no way that a basic online registration environment can verify the truth of an 'over 18' statement (or of a date of birth), so at registration there has to be a clear warning that you must be over 18 and may be asked for verification of age when you try to use the card in participating pubs and cafe bars. User psychology indicates that the warning should be on the registration page, positioned immediately above a tick box for you to assert 'I am over 18'. And, of course, the card is not a proof of age.

This brewery scheme needs a re-design, plus deletion of at least the date of birth data already collected. The starting point for good design is the Data Protection Act (in particular the data protection principles in

Schedule 1) and the advice on the Information Commissioner's Office web site. Then work out what the scheme has to do in the light of both the legal compliance requirements and the psychology surrounding people using the internet. Apply the principles of quality management, of which the component known as Information Assurance directly applies. Do I sound as if I'm being idealistic, rather than practical? I hope not - this is just good governance, which the Directors of the brewery company already know about in the context of brewing and serving excellent beer - after all, they drink in their own pubs.

The brewery web site was brought to my notice only a few days after watching the video of that 30th March PASC witness session for which the starting point was the Cabinet Office strategy document for ICT in government. During the PASC session, reference was made to the enrolment of online users of public services. Government's problem is that we no longer have a national ID card programme, but many online public services really do need to know that you are who you say you are. Clearly consideration is being given to simply passing the problem to the likes of the banks, rather than taking the USA line of creating a fully open market – but the USA is a federation and we are (Francis Maude) "a very centralised country" (answer to Q479) .

In the PASC session, reference was also made to a very relevant interaction between Francis Maude and a civil servant:

Francis Maude (answer to Q557): The Chief Executive of one Government agency said to me a few months ago, "Of course, we need to educate the public to use our service properly." I said, "I think you have that the wrong way around actually. I think we need to educate ourselves to provide our service in a way that the public do not need to be educated about it." Amazon did not get where they were by saying, "We have to educate the public to use our service." They did it by having an offering that was irresistible, irresistibly easy to use and then constantly developing it. We have to change our own mindsets and behaviours.

Shortly after:

Ian Watmore (answer to Q558): Again, the Minister's point is a huge one, which we should develop, which is how we use the world of the internet to deliver public services to the public. There are two fundamental changes. One is that we can do things online that, in the past, required the public to interact with a clerk in an office. Now they can do it directly. Equally importantly, we do not need to do it ourselves in Government. If we make the information and rules available, whole marketplaces develop on the other side of the divide. A great example of that is from talking to Mumsnet, the network of single mothers. They do not want us to provide services; they want us to give them our data so that they can provide services. If we can do more of that, not only will it be easier for us on this side of the table to do the work but it will actually create much better public service outcomes. That comes from the internet's availability, which of course was not there 20 years ago.

So we are clear about services, but not so clear about enrolment. By contrast, the USA is clear about both topics: private sector provides public sector benefits as a spin-off from designing an overall ecosystem.

And Information Assurance? It describes a set of quality disciplines applicable to the ICT environment. They aim to guide you towards understanding the nature of the environment: computers are deterministic - the old 'garbage in, garbage out' rule applies. Often we move to ICT implementation from paper-based methods that allow for human interaction to adapt those methods on the fly, so we have to check and double check our deterministic online methods to ensure that they really are fit for purpose. Online, no longer can I write 'over 18' alongside the brewery's date of birth box, and then give the form to one of the brewery staff who can see that I am over 18 - and who might well then give me a loyalty card. Information Assurance, however, misses out taking into account user psychology - practitioners will do well to add that into their armoury.

[1] http://www.parliament.uk/business/committees/committees-a-z/commons-select/public-administration-select-committee/news/minister-on-it/ and click on 'Watch the meeting'
[2] http://www.cabinetoffice.gov.uk/resource-library/uk-government-ict-strategy-resources
[3] Excerpts are taken from the Uncorrected Transcript of Oral Evidence of the session (HC 715-v) http://www.publications.parliament.uk/pa/cm201011/cmselect/cmpubadm/uc715-v/uc71501.htm

Marketforce and the IEA's 4th Annual Conference

The Future of

Cards and Payments

4th & 5th July 2011, Radisson Blu Portman Hotel, London

Explore regulation, innovation and the latest marketing strategies at the UK's leading strategic conference

Register before 6th May to save £250 off the standard delegate rate
marketforce.eu.com/cards

What people were saying after last year's event

> **"Excellent and very relevant"**
> **Paul Love,** Consultant, **ACI Worldwide**
>
> **"Very informative"**
> **Kim Heaton,** Payments Manager, **Co-operative Bank**

Reasons to attend

- Hear from leading representatives from the card schemes and top issuers
- In depth look at regulation, with panel discussions exploring the Commission's regulatory agenda
- Focus on fraud: heads of fraud from leading retail banks discuss strategies to take on the criminals
- Choice of streams: go deeper into fraud or hear issuers discuss marketing and portfolio management
- An entire day focused on payments innovation, including a peer-to-peer discussion, presentations and case studies on contactless, mobile and alternative

Also take advantage of:

- The peer-to-peer discussions, refreshments breaks and lunch to meet and debate with the key players in the cards and payments sectors

In association with the iea

Speakers include

Marc O'Brien
UK Managing Director
Visa Europe

Kartik Mani
Director, Cards Portfolio
Lloyds Banking Group

Ed Chandler
General Manager - Business Development, UK & Ireland
MasterCard

Carl Olav Scheible
Managing Director
PayPal UK

Rita Wezenbeek
Head of Payments Unit
European Commission

marketforce
mobilising knowledge in business

+44 (0) 20 7760 8699 marketforce.eu.com/cards conferences@marketforce.eu.com