



Smart Card & Identity News

Is published monthly by
Smart Card News Ltd

Head Office: Smart Card Group,
Suite 3, 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

Managing Director – Patsy Everett

Technical Advisor – Dr David Everett

Production Team - John Owen,
Rebecca Kimberley, Lesley Dann.

Contributors to this Issue –
Tom Tainton, Adam Bosnian, Bruce
Schneier, Jane Crossley, Georges
Lieberman

Printers – Hastings Printing Company
Limited, UK

ISSN – 1755-1021

Disclaimer

Smart Card News Ltd shall not be liable for inaccuracies in its published text. We would like to make it clear that views expressed in the articles are those of the individual authors and in no way reflect our views on a particular issue.

All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means – including photocopying – without prior written permission from Smart Card News Ltd.

Our Comments

Dear Subscribers



Patsy Everett

This month we have been hearing the trial of the accused brutal murderers of two French students Laurent Bonomo and Gabriel Ferez in London last year. It was all about the attackers wanting to know their PIN numbers so that they could get cash from the ATM machines. It makes you stop in your tracks when you realise that chip and PIN is a security advantage but also a risk to your person even to the point of death.

Amongst all the financial turmoil some of the bigger and more expensive government projects are in for the chop. This month we have seen a cancelling of the national database for monitoring all internet and mobile phone activity and of course everybody is wondering about the national ID card project.

Having had some of that dead time we all know about when travelling and faced with a flat battery on the mobile phone when one should be catching up on video podcasts and all my Twitter traffic, I had to come up with something else. An old fashion idea but pen and paper allow you to sketch out ideas or test hypotheses.

The ID card had to be my starting point, do we really need it? How would it improve our way of life? If it was readily available what would make people buy it? Now this was the first hurdle, the ID card is not for free and will have to be bought either individually or as an extra to the passport. Why would I buy it?

Well classical theory tells me for one of three reasons,

- 1) To provide something I can already get but to do it better
- 2) To provide something that I can't currently get
- 3) Just to look good, gadget freak etc.

Well I'm sort of an admirer of gadgets but my cupboard is bare and I prefer to watch other people's gizmos, at least until I get bored. So let's look at the other paths. Well people tell you the ID card is a security object and here I'm going to quote David Everett (who does have a cupboard of gadgets), who argues consistently, that the only reason to use a smart card (or similar) is to provide security. If the business application doesn't need that much security then there are far better and more economical ways of providing a solution.

So now we know that the ID card either has to provide better security for existing functionality or provide new functionality that requires adequate security. As an example of the latter condition an electronic purse may remain elusive but one does not doubt that the smart card can enable potential new functionality in an adequately secure way.

Identity really implies two things, the presentation of identity characteristics and the verification that the individual is correctly bound to these characteristics. In particular if my name is on the card then I as the authorised holder of the card need to be inextricably linked to the card and it should not be possible for the miscreant to snatch my card and purport to be me.





Now how do we do that? Our headline news this month is about more problems with the implementation of financial payment systems and in particular the handling of PINs. At a point of sale or ATM it is the PIN that links us to the payment card. If you know the PIN and have possession of the card then you can empty somebody's account. This brings me to where I first started, possession of a chip and PIN card is actually more desirable to a crook than the cash in your pocket and as we have seen can lead to a startling loss of life.

The problem with a PIN is that it is transferable but so are most of the common biometrics such as fingerprint that can link your physical presence to the card. Of course you might argue that some techniques such as Iris scans are a little more difficult to emulate, albeit not foolproof. At London airports at the moment you can register to enter the country through the special IRIS gates at immigration. Interestingly you don't need to show your passport. Now remind me why do I need the ID card?

Patsy Everett

Contents

Regular Features

Lead Story - Phantom Withdrawals Halifax Nightmare	1
Events Diary	3
World News In Brief	6,10,14,18

Industry Articles

Interview with Georges Liberman, CEO of Xiring	8
Five Steps to prevent employees from accessing sensitive data	12
Card Not Present Fraud	13
Why Outsource?	16
Southampton University investigates the biometric potential of OAE . .	19

Events Diary

May 2009

3-5	Digital Identity Assurance 2009, Dubai, U.A.E - http://digital-idassurance.com
5-6	MMT (Mobile Money Transfer) Africa - www.mobile-money-transfer.com/africa/
6-8	Payment China 2009, China – www.globaleaders.com/en/2009/payment/
11-13	NFC World, Europe 2009, London - www.terrapinn.com/2009/nfcw
11-14	IFSEC 2009, Birmingham, UK - www.ifsec.co.uk
13-14	Retail & Transport Cards, Copthorne Tara Hotel, London - www.smi-online.co.uk

June 2009

15 - 19	Prepaid 09 Conference & Expo, The Brewery, London – http://www.prepaid-conference.com/contact-details
18 – 19	Cards & Payment Europe 2009, Prague – www.cpeurope.com
22 – 24	Contactless Card 2009, London – www.smi-online.co.uk/events/overview
29 – 1	Prepaid Europe, Vienna – www.iirusa.com

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





.... Continued from page 1

Personal Identification Number's (PIN's) are now the high value target of cyber criminals. Criminals implant internal rogue software to accumulate million's of PIN's an hour and often PIN and account information are sold over the internet to the highest bidder.

One of the methods being used according to the report to collect PIN's is to exploit the financial networks Hardware Security Module (HSM) switches. Worryingly the fraudster requires physical access to one of these switches to be able to collect PIN's.

Usually there is not a direct link between the ATM and the card-holders bank's verification system. The transaction data is bundled up in a encrypted data block and hops along HSM switches on way to the bank. To ensure no single party knows an overall encryption key a different key is used between switches and so the encrypted data block is decrypted and re-encrypted at each switch. Also the data block can be re-formatted at the switch to suit different financial devices and network schemas.

An attack has been documented by a computer student of Tel Aviv University as part of his masters thesis entitled "The unbearable lightness of PIN cracking". The author Omer Berkman describes exploiting the "Translate" functionality of the box. This is a standard operation of the HSM and part of the Financial PIN Processing API, a 30-year old standard including all the functions for PIN verification, changing and reformatting.

The HSM Hack

Prerequisites

- Access to the HSM Switch
- Non-EMV compliant operating ATM (magnetic stripe operation ATM)

The attacker makes transactions with any account number yet at this time he knows the value of the PIN. Once the encrypted PIN and account number data block reaches the HSM, he uses the translate function to change to a weaker data block format using a fixed account number. The attacker only needs 100 transactions and by using a cryptographic flaw in the new format the attacker can build a 10,000 entry look-up table. The attacker uses this table at the HSM to work out any subsequent PIN number.

Military grade encryption specialists, Credant Technologies have suggested a solution; this is to double the encryption by further encrypting the PIN between both end-points (ATM & Bank verification system). Vice President Michael Callahan said; "There is nothing to stop banks adding military grade encryption as an underlay to their existing HSM-based network encryption system and so ensuring their cardholders are safe from this new type of hacking exploit".

The Liability Shift

A lot of documentation on hacking payment systems has become available because of anger at the banks shifting the cost of fraud to the card-holder as a result of Chip&Pin.

Before Chip and PIN, magnetic stripe cards and signatures were used for authorisation, if a fraudulent transaction took place a cardholder could ask for the signature on the receipt be examined against a sample of their own.

Now banks refuse liability. "If you act without reasonable care, you may be responsible for them". Banks now can easily stamp card-holders with not taking enough care in keeping their PIN secret. Now only CCTV can refute the customer's involvement.

Academic institutes have been investigating Chip&PIN attacks. In the UK, Professor Ross Anderson of Cambridge University has been the most vocal, capturing the most media attention on this subject. Anderson and his team have been reverse engineering and documenting attacks on financial security systems for years. In the case of Chip&PIN they have even set-up a dedicated website to highlight the raw-deal card-holders are getting from Chip&PIN. (www.chipandspin.co.uk)





The Cambridge team's work includes;

(May 2005) - Chip and Spin;

The Fall-back Hack

Prerequisites

- Non-EMV compliant operating ATM (magnetic stripe operation ATM)
- Tampered PIN Pad

When a card is presented at an ATM or POS terminal whose chip has been damaged, or which never had a chip, then the device falls back to magnetic stripe operation.

Magnetic stripe card skimming is used to make a clone card, and a tampered PIN Pad records the PIN. The fraudsters then use the half-baked cloned card at an ATM which allows fall-back to magnetic stripe or in a foreign country where EMV is not supported.

The Offline POS Hack

Prerequisites

- Offline Point of Sale Terminal

The fraudster goes to a POS which is not directly connected to the bank's verification system. The fraudster creates a half-baked smartcard using previously stolen account details. The fraudster's card is programmed with any PIN he likes. The card's authenticity is not checked until the POS goes online, in which time the fraudster is long gone.

Modern DDA (Dynamic Data Authentication) cards, have a challenge-response mechanism in which the offline POS can test for card authenticity.

(February 2006) - Phish and Chips;

The Smartcard Relay Hack

Prerequisites

- Tampered PIN Pad/POS
- A fake card with Bluetooth or similar

The victim pays for a small value item at the tampered POS;

"The smartcard data stream would go maybe via GPRS to a PDA in the crooks pocket, then to his fake card, and the captured PIN read out via a headphone in his ear. You think you're paying for lunch, but in fact you're buying the crooks a diamond!"

(February 2009) - Optimised to Fail;

Exploiting Card Readers for Online Banking

Prerequisites

- A Hostage

Card Readers for Online Banking may be used to assist during a mugging. Previously, muggers marched a victim to an ATM to ensure he gave them the right PIN. Now, with portable card readers, criminals have a portable device that will tell them if their victim is lying about their PIN.

Many of the more practical attacks exist because many foreign countries are not compliant with EMV and financial systems can be fooled into operating in a non-EMV fall-back mode.

Perhaps the solution would be to apply more pressure to speed up EMV migration and stop legacy payment methods.

One thing is for sure criminals are using ever more sophisticated ways of committing fraud. Banks should be





more open to the more far-stretched hacks, especially as insiders are helping the fraudsters and older style cards without the necessary anti-counterfeiting measures are in circulation.

Alain Job, will challenge chip and pin security in the UK in a lawsuit with Halifax building society. This will be the first UK case to question the strength of the bank's security measures. Alain Job claims that £2,100 disappeared from his account whilst Halifax allegedly has evidence that Job's real card was used at a ATM.

The Hearing will be held at Nottingham County Court on 30th April, where many will be eagerly awaiting to hear the outcome of this case, and the conclusions resulting from the questioning of bank security.

John Owen, Smartcard & Identity News

World News In Brief

Giesecke & Devrient Acquires SmartTrust

Giesecke & Devrient (G&D) is acquiring SmartTrust AB. Together they will offer all-in-one solutions for securely integrating services provided by mobile telephony companies, banks, government agencies, and transport operators. The financial details of the transaction have not been disclosed.

“G&D has a strong reputation for comprehensive smart card expertise, and SmartTrust is well-known for high-performance server solutions in the telecommunications sector. Demand for secure mobile applications on SIM cards is on the rise and will certainly expand beyond cell phones in the future. There will also be a need for various storage media that can provide a secure platform and for the ability to run the technology on any device. For clients, the most important thing is for the applications to be securely stored and managed. And that is exactly where G&D and SmartTrust have enormous potential for growth together,” said Dr. Karsten Ottenberg, CEO and Chairman of the Management Board at G&D.

G&D believe that acquiring SmartTrust as an independent company will strengthen their ability to help operators use new, innovative technologies to meet the up and coming challenges. SmartTrust's special focus on openness and interoperability will continue within the G&D group.

SmartTrust has 178 employees worldwide and generated Euro 31.3 million in revenues last year. The company is profitable, with a solid financial structure and with main headquarters in Stockholm, it maintains eight branch offices around the world. Over 200 cellular network operators worldwide trust SmartTrust technology. Giesecke & Devrient GmbH (G&D) will acquire all ownership shares of SmartTrust from its present owners including the Carlyle Group, Eqvitec Technology Fund, TeliaSonera and GE.

Infineon Voluntary Delists from New York Stock Exchange

Infineon Technologies AG announced that it has applied to voluntarily delist its American Depository Shares ("ADSs") from the New York Stock Exchange ("NYSE"). The Company delisted the ADSs on April 24, 2009, and as of that date, the ADSs will no longer be traded on the NYSE.

Infineon intends to file for deregistration and termination of its reporting obligations under the Securities Exchange Act of 1934 (the "Exchange Act") as soon as possible following the first anniversary of the delisting.

The Frankfurt Stock Exchange represents Infineon's principal trading market, with trading on the NYSE accounting for a relatively low percentage of trading of its ADSs and ordinary shares on a worldwide basis. Infineon has weighed the benefits of listing on the NYSE against the associated costs and reached the decision that continuing the listing of the ADSs is no longer commercially justifiable.

Infineon will maintain its ADS facility as a "Level I" program and pursue a listing of its ADSs on the over-the-counter market OTCQX. Infineon's ordinary shares will continue to be traded on the Frankfurt Stock Exchange, and the Company will continue to comply with the rigorous German disclosure and transparency requirements. Infineon will continue to publish its financial reports, press releases and other information in English for investors on its website.

After the delisting and until deregistration is effective, Infineon will comply with its reporting obligations under the Exchange Act. After deregistration, Infineon will continue to maintain the level of disclosure expected by the international financial markets.



Gemalto Joins SAFE-BioPharma Association

Gemalto is joining with biopharmaceutical and healthcare industry leaders to help the industry achieve its common goal of a fully electronic business environment by 2012. Gemalto will contribute its expertise in smart card-based solutions for authentication, network security and digital signature.

Gemalto is the first smart card provider to join SAFE-BioPharma. Gemalto has been an active industry partner since 2004, when it began working with Pfizer to implement smart card employee badges that converge physical and logical access control onto a single identity credential. Gemalto is also a leading supplier of smart card based solutions for healthcare identity management worldwide.

The SAFE-BioPharma Association, based in Fort Lee, New Jersey, is a non-profit association that created and manages the SAFE-BioPharma digital identity and signature standard for the pharmaceutical and healthcare industries. The standard provides users with a secure, enforceable, and regulatory compliant way to verify identities of parties involved in electronic transactions and to apply their digital signatures to electronic documents.

"We welcome Gemalto to the growing SAFE-BioPharma vendor partner community. The company's broad experience in smart cards, digital security, digital signature and identity management for healthcare, makes it a valuable global resource for life science companies," said Mollie Shields-Uehling, president and chief executive officer, SAFE-BioPharma Association.

CSC & IBM Awarded £650 Million IT Services Contract by UK Identity and Passport Service

CSC announced that the UK Identity and Passport Service (IPS), an executive agency of the Home Office responsible for issuing UK passports and ID cards, has awarded the company a 10-year managed information technology (IT) services contract to upgrade the IPS application and enrolment system. The agreement has an estimated value of \$570 million (385 million pounds sterling).

Under the terms of the contract, CSC will assume responsibility for several existing legacy IT service contracts supporting the IPS. CSC will upgrade the existing application and enrolment system with new

capabilities to process applications for passports and ID cards. The additions to the system include the ability for customer online applications; improved background checking; a new system for reporting lost and stolen passports and ID cards; customer support for updating personal data; and new IT and telephony systems.

In conjunction with the IPS and its other partners for the National Identity Service, CSC will play a key role in enabling the agency to deliver the next generation of biometric passports and support the introduction of ID cards.

"The British passport is already one of the most secure in the world, and it is vital we maintain that strength by moving with the rest of the international community," said James Hall, chief executive of the Identity and Passport Service. "CSC has shown it is superbly placed to deliver this contract and we are delighted they are working with us."

IBM have also been rewarded a contract worth £265 million, to replace the UK Border Agency's Immigration and Asylum Fingerprint System and build a database to store the fingerprint and facial biometrics of applicants for passports and ID cards. It is no surprise to see IBM succeeding in this public sector. IBM already has at least two contracts with the UK Border Agency, being involved in the Home Office eBorders programme and is the systems integrator partner for the Immigration Case Work Programme. The latter three-year contract was awarded in December 2008 and is thought to be worth £3 million. This latest win builds on these two contracts and its identity management work globally.

James Hall also recently pointed out that there were no technical reasons for not using Chip and PIN technology in the forthcoming UKID Card, highlighting that he takes a serious interest in the possible advancements for the card

James Hall commented that the cards have the format to be used in card readers and potentially in existing networks, e.g. the ATM network.

The UK IPS are currently in discussions with the financial services industry with a compelling view of the rationale for Chip & Pin for them, and has mentioned that Chip & PIN could be used for online customers to assert their identities.





Interview with Georges Liberman, CEO of Xiring

By Tom Tainton, Smartcard & Identity News



Tom Tainton

Created in 1998, XIRING is a security solutions provider and develops security software embedded in smart card readers for strong authentication and digital signature. XIRING has distributed over 10 million strong authentication solutions based on banking cards and compliant with MasterCard and Visa programs, and is the leader of the professional solutions market for the SESAM-Vitale French healthcare scheme.



Georges Liberman

You're a leader in the healthcare market, with latest financial figures showing turnover of 2.5 million euros. What are the strengths of XIRING in this sector?

In its Health activity, XIRING is supporting the French national healthcare industry's move to a paperless system with its terminals which can be used to generate and sign e-medical claim forms and update medical cards. The programme is designed to speed up reimbursements and support the fight against fraud by ensuring the authentication of patients, secure access to medical information and increased confidentiality of transferred data.

XIRING first entered the healthcare market in 2002, and has since developed a complete range of dedicated solutions for the French market certified by the GIE SESAM-Vitale and designed to meet the specific needs of healthcare professionals. Currently, 38% of our revenues come from healthcare. Last year, XIRING announced that over 12,500 pharmacies were using 'le Point XIRING V2', the company's second generation remote service for updating the French Vitale health card. Operated by XIRING, the 'le Point XIRING V2' network is now one of the largest machine-to-machine GPRS networks in France.

At the start of the year XIRING announced a target turnover for 2009 of 30 million euros, is that realistic?

As a listed company on the Paris stock exchange, XIRING gives a full year forecast to the financial market once a year. At the beginning of the year, XIRING announced a target turnover for 2009 of €30 million, with a possible variation of +/- 10%, depending on the pace of banking solutions deployed in the second half of 2009, and a target operating income in excess of 7%. In April 2009, XIRING announced a turnover of €4 million as of 31 March 2009, which is in line with the company's roadmap. To date, XIRING has always achieved, and indeed in some instances surpassed, its financial targets.

XIRING provides strong authentication solutions such as the widget for online banking. What has the widget done for security, and how will it impact on authentication in the future?

Remote Card Authentication solutions are based on the use of the EMV bank card coupled with a card reader. The card, used in the device, generates a one-time-password based on the secrets stored securely on the card's chip, and the card cryptographic mechanism. Pocket-sized, portable EMV-compliant smart card readers offer the best answer to online authentication challenges today - at least in those countries with EMV.

XIRING has experienced particular success in the UK with its range of Home Chip and PIN readers, boosted by the introduction of the Faster Payments Services (FPS) earlier this year, as the banks' systems were not up to the challenge of receiving a payment instruction from a variety of different channels and strongly authenticating that person to prove they are who they say they are within the 15 second transaction processing time limit introduced by FPS. In total, 21 million bank card based strong authentication solutions have been delivered in Europe to replace the static password for online banking services and to secure e-commerce payments. Of these, XIRING has issued more than 10 million solutions to date.



Are there any new products or innovations in the pipeline?

Unfortunately XIRING can't disclose details of products to be launched this year. However, with research and development at the heart of the company, XIRING will maintain a high level of innovation and also widen its range of solutions and services to meet its customers' expectations.

How is the international recession in the banking sector affecting your business?

First of all, it is pertinent to note that XIRING's customers are retail banks as opposed to investment banks. Despite everyone feeling the effects of the financial crisis, retail banks must continue to equip their online banking customers with the most effective fraud protection solutions. British banks, for example, which have generally speaking been seriously impacted by the crisis, continue to equip their internet users with two-factor authentication solutions at a sustained pace. As use of the internet continues to grow, as does internet banking, banks have an obligation to develop their online banking services and encourage growth and sales of financial products online.

What challenges has XIRING experienced as a result of the economic climate and how has the company adapted?

XIRING is keeping to its strategy, as previously touched upon. Even those at the brunt of the financial crisis in the retail banking sector still need to equip their internet banking users with appropriate fraud protection solutions. XIRING is very well positioned in this developing market space. According to Mastercard, 21 million Europeans were equipped with strong authentication solutions by the end of 2008; we expect this figure to reach 60 million by the end of 2010.

Turnover is down compared with the same period in 2008, can you return to the growth margins experienced last year?

XIRING actually outperformed the operating margin target announced at the beginning of the year 2008 (above 7%) and the revised target announced last September (above 8.5%). For the full-year 2008, operating income amounted to €3.5m. This corresponds to a margin of 12.4% on turnover and represents 62% growth, which is highly satisfactory.

Cambridge University researchers reverse-engineered card readers from NatWest and Barclays. They discovered that the technology was vulnerable to sophisticated phishing attacks. Is this a concern and how can the security be improved?

It is not a concern for us and the research has been widely discredited, including by APACS.

What does the future hold for Xiring?

XIRING has a strong presence in high growth markets. For the Healthcare market, XIRING aims to maintain its leadership position in SESAM-Vitale business solutions by building on areas of growth such as the deployment of the Vitale 2 healthcare benefit cards, upgrades to the SESAM-Vitale system architecture and the integration of additional insurance benefits. For the Banking industry, there remains strong potential for the two-factor authentication solution market and this is underpinned by the growth in e-commerce and remote banking and the associated security requirements.





World News In Brief

Sharp Rise in On-line Banking Fraud Driven by Keylogging

Fraud loss figures released by APACS, the UK payments association, show that card fraud losses totalled £609.9m in 2008. The two main areas of fraud were on transactions not protected by chip and PIN: specifically internet, phone and mail order fraud; and fraud abroad committed by criminals using stolen UK card details in countries yet to upgrade to chip and PIN - which has nearly doubled in two years.

On-line banking fraud losses totalled £52.5m in 2008 - a 132 per cent increase from 2007 losses. Although phishing incidents continue to increase, online banking customers are increasingly being targeted by malware attacks.

Malware includes computer viruses that can be installed on a computer without the user's knowledge, typically by users clicking on a link in an unsolicited email. Malware is capable of logging keystrokes thereby capturing passwords and other financial information.

Card-not-present fraud losses have increased by 13 per cent over the last year and account for 54 per cent of all card fraud losses, tackling this fraud is a priority.

Visa Launch Commercially Available NFC Point-of-Sale Service

The service marks for the first time consumers can purchase an NFC-enabled mobile device off the shelf and use that device to make Visa payWave-enabled transactions at the point-of-sale instead of using their payment card.

Launched in Malaysia, the service allows users to pay for goods by waving their NFC-enabled Nokia 6212 classic handset in front of a contactless reader, according to a statement from Visa. The launch signals the move from pilots to real roll-outs, it said.

The contactless chip embedded in the device will also power a number of additional functions, including a contactless transit application that enables Malaysian commuters to pay for charges while using metropolitan transit systems, bus terminals, highway toll gates and car park facilities at more than 3,000 contactless payment touch points throughout Malaysia.

Besides Nokia, Visa has teamed up with mobile operator Maxis and Maybank. To get started users can download their Visa payWave credit account details directly to their phone. Currently, 1,800 shops accept the system in Malaysia.

First Data and INSIDE Contactless Launch Partnership for Go-Tag Payment Sticker Technology

INSIDE Contactless, and First Data, this month signed a three-year agreement to develop contactless payment stickers to affix to mobile phones or other devices. First Data will market the stickers as GO-Tag products. With this agreement, INSIDE will supply MicroPass payment sticker preforms exclusively to First Data-qualified card manufacturers for production.

GO-tag stickers work like contactless gift cards, loaded with a prepaid amount of credit. The stickers are intended to be stuck on key-chains, badges, phones and other personal items.

First Data will be marketing and distributing GO-Tag products to financial institutions, major U.S. merchants, and other distribution channels in a variety of form factors.

Gemalto Provides National e-ID Cards to Saudi Arabia

Gemalto has announced it is delivering electronic ID cards to the National Information Centre (NIC), the IT entity of Saudi Arabia's Ministry of Interior.

The ID Card-Phase 2 program extends the country's initial electronic ID initiative launched in December 2007. Gemalto will provide NIC with cards for the next three years, as well as support and maintenance for the centralized personalisation centre in Riyadh.

The National ID card is a wallet-sized card that will be mandatory for all citizens above 15 and valid for ten years. The card embeds a microprocessor containing the cardholder's digital information such as demographics, facial image, digital signature (available through a Public Key Infrastructure application) and fingerprints. It also features a bar code and an optical stripe to ensure enhanced security to citizens. The card can act as proof of identity and can be used as a travel document that facilitates legitimate travel within all gulf co-operation council countries (Saudi Arabia, Kuwait, Bahrain, Qatar, UAE and Oman).



Profits halved on EU Interchange Revenue

EU issuers may lose €2.6 billion in credit card interchange revenue, and more than half of profit per credit card.

EU payment card issuers will experience conflicting emotions as a result of MasterCard Europe's interim multilateral interchange fee (MIF) arrangement with the European Commission (EC). The arrangement reached on 1 April 2009, clarifies the acceptability of MIFs under EU antitrust rules, but the level of those fees is far below historical rates.

The arrangement establishes a new methodology under which the maximum weighted average MIF per transaction will be reduced to 30 basis points for consumer credit cards and 20 basis points for consumer debit cards. Previously, MasterCard's cross-border MIF ranged from 80 to 190 basis points for credit cards, and between 40 to 75 basis points for debit cards.

While the arrangement covers intra-European Economic Area, cross-border transactions only (which account for less than 5 percent of MasterCard Europe's total billed volume), the EC view regarding cross-border transactions within the EU could raise the threat of reductions on domestic interchange rates.

Since the EC is committed to eliminating cost differences between cross-border and domestic transactions under the Single Euro Payments Area (SEPA), their agreement on the new MasterCard MIFs may indicate the level at which they are also comfortable regarding domestic transactions.

If the 'acceptable' cross-border MIF was applied to 2008 figures for all credit card transactions within SEPA, the issuing industry would stand to lose €2.6 billion in interchange revenue.

Debit cards carry lower interchange rates than credit cards, and would therefore be less adversely affected, but higher-revenue debit brands would be disadvantaged in the new environment. For example, MasterCard has been pushing its 'Debit MasterCard' brand in the UK to compete with higher interchange on Visa Europe's 'Visa Debit' brand - the transfer of acceptable cross-border MIFs to the domestic market would negatively impact the strategy of both networks.

Northrop Grumman for RFID III Contract

Northrop Grumman Corporation was one of four companies selected to receive a contract to provide radio frequency identification (RFID) hardware, software, and engineering services to the U.S. Department of Defence under the RFID III contract, providing increased network functionality, visibility, and security control.

RFID III is a multiple award, indefinite delivery/indefinite quantity contract with a \$429 million ceiling available for task order awards. Work on the contract will be conducted over a three-year base period with up to seven, one-year option years.

Under the terms of the contract, Northrop Grumman's Information Systems sector will supply active RFID tags, readers, mobile kits, software, and the technical engineering services to implement this technology. The terms also include providing the hardware, maintenance, design, development, integration, deployment, training, and data management of the tags.

European ATM Fraud Attacks Up 149%

EAST (the European ATM Security Team) has reported a 149% rise in ATM related fraud attacks during 2008. This reverses a previous trend and is primarily led by the 129% increase in card skimming incidents, with a total of 10,302 reported. Despite this significant increase in incidents, fraud related losses increased by just 11% with a total loss of €485 million reported. This smaller increase in losses, relative to the significant rise in reported incidents, is indicative that that deployed counter-measures, such as anti-skimming devices, are increasingly effective, as are fraud monitoring and detection capabilities.

EAST Director and co-ordinator, Lachlan Gunn said, "This increase in reported incidents is of great concern to EAST members. While the year on year fraud loss figures show an increase, the half year figures show a declining trend for such losses over the past three six month periods, with international losses due to card skimming falling by 18% in the second half of the year. This indicates that the EMV rollout in Europe continues to be effective, although international losses are expected to continue while criminals are able to illegally withdraw cash from ATMs abroad that are not EMV compliant".





Five Steps to prevent terminated employees from accessing sensitive data

By Adam Bosnian, Director at Cyber-Ark



Adam Bosnian

Redundancies and corporate re-organisations are an unfortunate reality in today's economic climate. Too often, businesses leave themselves vulnerable to a data breach or serious security incident during the redundancy cycle by not immediately revoking the network and application access points of terminated employees.

Security threats from inside the organization are not a new phenomenon, but layoffs and economic uncertainty can significantly exacerbate the problem. A recent Cyber-Ark survey, "The Global Recession and its Effect on Work Ethics," found that 71 percent of the employees surveyed declared they would definitely take company data with them to their next employer. The study further stated that "Top of the list of desirable information is the customer and contact databases, with plans and proposals, product information, and access/password codes all proving popular choices." Moreover, the "Jobs at Risk = Data at Risk" survey published by the Ponemon Institute, found that 59 percent of employees who were laid off, terminated, or who quit their jobs in the last 12 months admitted to stealing company data, and sixty-seven percent admitted to using their former company's confidential information to leverage a new job.

When a security incident of this nature occurs, we tend to file it away as an example of an "employee gone bad." In reality it constitutes a failure of the organization to uphold their responsibility on behalf of the business to manage, control and monitor the power it provides to its employees and systems. At a basic level, the organization and its management has a fiduciary responsibility to ensure that access to critical information and applications is authorised and that it is continually monitored to make sure the resulting activity is authorised as well. The failure stems from the 'perception of control' an organization has over their most sensitive networks, systems and devices.

The threat to an organization is increased exponentially when the access is through administrative, shared or privileged accounts – these represent the most powerful IT users in an organization, often providing wide-ranging access to most systems, application or database within the enterprise. These privileged identities, which exist on virtually every one of the thousands of servers and applications within a typical enterprise, very rarely get changed, due to the presumed extra IT effort involved and the need to communicate the new settings to the IT staff, which if not done effectively could potentially impede or slow down an administrator doing a time-critical task.

This type of uncontrolled access can lead to dire situations. In fact, failure to control these privileged identities led to two of the more critical security incidents in the past year. Last year, the city of San Francisco was brought to its knees because an employee locked down the city's IT system through a privileged account. And more recently, a Fannie Mae employee implanted a logic bomb on the company's network because access to his privileged accounts was immediately revoked upon his termination.

Here are specific steps you can take to help prevent severe security incidents:

1. Improve internal security controls around privileged accounts via encryption, password protection, and auditing of system access;
2. Reduce the risk of internal data misuse by implementing policies and technologies which provide special treatment for privileged identities and ensure compliance with regulatory requirements;
3. Ensure administrative and application identities and passwords are changed regularly, highly guarded from unauthorized use and closely monitored, including full activity capture and recording;
4. Avoid sloppy habits when exchanging privileged and sensitive information, such as sending sensitive or highly confidential information via email or writing down privileged passwords on post-it notes;
5. Ensure provisioning, and more importantly deprovisioning of user access in an immediate timeframe after employee status or role changes.

Remember, trust is not a security policy, and the damage that insiders can do should not be underestimated. To thwart this threat, the first big step is making that key decision to effectively manage these privileged accounts, and then doing so in a streamlined manner that makes it efficient and transparent to the user. Streamlining the management of privileged accounts by controlling who has access, when access was gained, what is being done with the sensitive data and why access is needed is critical in preventing a major security incident from occurring at your company.





Card Not Present Fraud

By Jane Crossley, JaywingDMG



Jane Crossley

The last few years have seen card issuers developing new defences against Card Not Present (CNP) fraud, in an effort to combat this growing threat; the main examples being 3-D Secure systems, such as Verified by Visa and MasterCard SecureCode. Consumer uptake of these online authentication schemes has increased by 600 per cent in the past two years, according to APACS figures; the 3 D Secure scheme now boasts registration of more than 25 million UK debit and credit cards.

Yet whilst 3-D Secure is protecting an increasing number of transactions, it is not without its own issues.

Though not the fastest growing type of fraud, CNP is still by far the most significant, accounting for 54% of all card fraud losses. With a 13% increase in 2008, CNP fraud was responsible for a staggering £328.4m in fraud losses in a single year, despite the widespread addition of verification techniques like those offered by 3-D Secure.

This continued growth may be, in part, due to the continued increase in online shopping, which grew by 19 per cent year on year in January (according to the latest IMRG Capgemini e-Retail Sales Index). Even in the current economic climate, online sales continue to be buoyant, as consumers take advantage of the lower prices and convenience of shopping online. This continued growth presents fraudsters with even greater opportunities to carry out these costly attacks.

So why is 3-D Secure not solving this issue completely?

The problem for many retailers, and card issuers, is that up to 30% of sales are lost when 3-D Secure processes are invoked. When asked to provide another level of verification a high proportion of consumers click away from their shopping basket at the final stage of the purchase process. Some 3-D Secure processes route consumers to a separate (and often not well branded) web page; so for some cautious customers this can look too much like a phishing attempt, resulting in a high 'click off' rate. For many retailers then, this method is not the answer to the problem when they consider the potential loss of sales; it stands to reason that for many, the opportunity cost outweighs the fraud prevention benefit.

So, whilst the card issuer does not have to be concerned about the fraud cost of such transactions, or indeed the immediate loss of sales by the retailer, the increased number of charge backs to the retailers to recover the fraud is bound to have an operational impact. And in the current climate, costs are under scrutiny.

So what else can be done to help?

For the retailer, there are other options which will help them to maintain a slick purchase process for most of their customers, whilst still preventing the majority of fraudulent transactions.

When we used our generic, simple to use, postcode level fraud identification model for an on-line electronics retailer we found 50% of fraud cases were identified in the top 10% of highest fraud-propensity and 80% of frauds in the top 20%. The implication is that for a retailer to reduce their fraud losses by 80% they need only have alternative payment and delivery strategies for 20% of their customers. These results were further enhanced when we developed a bespoke model based on the retailer's own known fraud cases. Models such as these can significantly enhance existing fraud prevention strategies and tools, and easily integrate into existing processes, further strengthening a brand's fraud defences. The power of the model lies in it being built using a large pool of known fraud cases, combined with other data.

This is good news for the card issuer as resources can be streamlined if enough retailers implemented such an approach. Essentially the card issuer can take an impartial stance as the fraud loss is not theirs, and then provide advice to retailers about the number of different options available, how they work, and where to find them.

But what of a card issuer's own fraud prevention procedures? If the retailer finds the fraud prevention process loses them custom, is the same true of the card issuer?





As consumers, we have undoubtedly noticed an increase in fraud checking procedures, although these can vary significantly between card issuers. Genuine in store transactions that are automatically referred for fraud checks can cause considerable inconvenience – and embarrassment - to the customer. They worry that the cashier and other customers think they can't afford the goods they're trying to purchase, or that they are a fraudster. Similarly, automated services that call immediately after you have used your card, to check your transaction is genuine, can be badly timed and if persistent may be down-right irritating. Equally, automatically blocking a card puts the onus on the blameless customer to call their card issuer to re activate the card, and jump through various hoops to prove their authenticity.

Clearly, issuers need to strike a balance between putting in place adequate and efficient defences whilst avoiding becoming too annoying and time consuming to the consumer, after all it is on the whole not their liability. Essentially, this balance can be achieved through a more accurate understanding of customer data; specifically in understanding patterns of usage.

Fraud procedures are normally triggered by certain patterns of account activity, usually where threshold criteria have been exceeded; typically value, number and type of transaction(s). However these limits have tended to be applied at a portfolio level, without due consideration of a customer's normal behaviour profile.

Certain types of transaction, such as paying for train tickets from an automated machine, can be easy pickings for fraudsters. But a customer who regularly does so, using the same station for their commute week in, week out, doesn't want to be repeatedly having a conversation with the card issuer to verify that the transaction is genuine. Better understanding of their unique behaviour patterns can prevent inconvenience to the customer, and make better use of resources.

Applying fraud prevention analytics and rules at an individual level could dramatically reduce the likelihood of the customer losing patience with the card issuer. Such analytics can be complex, but they are by no means impossible; applications of such analytics are emerging strongly in value management techniques. It doesn't require a big mental leap to imagine the positive impact of individual level analytics, both in reducing customer 'nagging' and increasing your ability to prevent fraud.

Both of these issues rely upon striking a fine balance between customer service and fraud prevention, and only a solid analytic approach can deliver. Getting this approach right is fundamental; the difference between a fruitful ongoing customer relationship, and the end of one.

World News In Brief

Fujitsu Develops High-Speed Image-Capture Technology for Palm Vein Biometric Authentication



Fujitsu Laboratories Ltd. announced this month the development of the world's first imaging technology for use in palm vein biometric authentication that can operate while the palm is in motion. The new technology requires approximately only one millisecond to capture the image, and performs with

the same level of accuracy in authentication as previous iterations of this technology.

The device can capture images at approximately the same average speed as a person walks (1 meter per second) - with image quality equivalent to levels achieved with the conventional system, which required the palm to be held over the palm vein authentication sensor. This technology retains the features of the previous palm vein authentication technology, including the following: it is difficult to falsify identity because it measures a biometric feature that is inside the body, it is widely applicable because it is not prone to effects from external factors, and its non-contact hygienic factor enables greater user acceptance. In addition, the new technology can perform authentication when a palm is just passed over a sensor, resulting in a palm vein authentication system that can be used in a significantly broader range of applications.





Fujitsu will continue with technological advancements to resolve issues to enable practical use, such as reducing the size and cost of the image-capture module.

Bulgaria's Biometric Passport Deal Frozen by Court

This month Bulgarian Interior Minister Mihail Mikov signed the 116 million euro agreement with Siemens for the development of Bulgaria's new biometric passports, four hours after the Supreme Administrative Court (SAC) halted the deal. The day before Mihail Mikov had said "We will start issuing them within six months," and the new passports would cost around £23 each.

The SAC froze the deal after three companies who competed for the order contested the selection of Siemens.

The procurement to select a company to produce Bulgaria's new biometric passport has been restarted several times over the last couple of years. Its introduction is desperately behind schedule. The new biometric passport was supposed to be introduced before the country joined the European Union in January 2007. The delay could trigger EU procedures against the country.

New UK Biometric Identity Card Keeps Sheep Shearers Away

Sheep farmers are on a collision course for a major welfare crisis this summer as a massive shortfall in shearing gangs from abroad means millions of sheep will have to carry heavy fleeces throughout the hottest months of the year - and some may not even get sheared at all.

Over a quarter of the UK's 14.5 million sheep are sheared by gangs of shearers from New Zealand and Australia. Around 500 shearers work in the UK every summer and most would normally have now made arrangements for the trip.

But new Government rules covering work permits threaten to keep the southern hemisphere workers at home. So far only one shearer has confirmed he will be coming to the UK.

UK-based shearing contractors - who traditionally hire hundreds of Australian and New Zealand shearers each summer - say a new biometric identity card system introduced by the Government for foreign workers looks like keeping the workforce away from the UK.

The biometric card - costing £200 per applicant - requires workers to travel personally to Canberra for fingerprinting and photographic identity details.

The single shearer who has acquired a biometric card to work in the UK this summer had to travel for eight hours for a three minute interview to supply identity details.

And now shearers have been told that even if they apply for their biometric card it will take at least nine weeks to issue - a delay making it no longer worth them coming to the UK this summer.

East Sussex farmer Frank Langrish, Chairman of the British Wool Marketing Board, says the situation is ridiculous and poses a serious welfare issue for UK sheep and major problems for farmers.

Minister Leaves Confidential Papers on Train

Arriving at London's Euston station, Andy Burnham, Culture Secretary left confidential documents marked "restricted" in a briefcase.

The case, believed to have contained Cabinet papers, was handed over to police in Glasgow after it was discovered by a passenger on the train's return journey.

Andy Burnham said, "What happened was unacceptable and I apologise unreservedly".

The Department for Culture, Media and Sport have said they will conduct a review of security procedures, but that the papers did not contain sensitive information. A spokesman for the Culture Secretary added "Andy deeply regrets this breach and realises it is wholly unacceptable."

The security breach comes shortly after the top counter-terrorist officer, Bob Quick was photographed carrying a secret document containing details of an operation to dismantle an alleged al-Qaida bomb plot, forcing Quick's reluctant resignation and a speedy Police response to carry out raids on addresses related to the papers exposed.





Why Outsource?

By Bruce Schneier, Chief Security Technology Officer BT



Bruce Schneier

More and more companies are outsourcing their network security. This trend is driven by one truism: there is no other way to deal with the shortage of skilled computer security experts, the increasing requirements for businesses to open their networks, and the ever-more-dangerous threat environment. For the Internet to succeed as a business tool, security has to scale. Outsourcing is the way to achieve that.

But if the decision to outsource network security is a difficult one, the decision of precisely what to outsource seems impossible. Managed security service companies can monitor your networks, manage your security devices, scan your networks, implement your security policies, install your security devices, and more. Other companies offer similar services, often tied to particular products or suites of products. And sometimes outsourced network security comes in a package with other outsourced network services.

On one hand, the promises of outsourced security are very attractive: the potential to significantly increase your network's security without hiring half a dozen people or spending a fortune is impossible to ignore. On the other hand, giving over your network security to another company feels inherently risky.

In reality, there's no dichotomy. Hiring a specialist organisation to handle your network security can be less risky than building your own expertise inside your company. And it most definitely can be both cheaper and more effective. You already understand why; you just might not have thought of it in terms of network security.

Arguments for Outsourcing

The primary argument for outsourcing is financial: a company can get the security expertise it needs much more cheaply by hiring someone else to provide it. Take monitoring, for example. The key to successful security monitoring is vigilance: attacks can happen at any time of the day and any day of the year. While it is possible for companies to build detection and response services for their own networks, it's rarely cost-effective.

Staffing for security expertise 24 hours a day and 365 days a year requires five full-time employees—more, if you include supervisors and escalation personnel with specialized skills. Even if an organization could find the budget for all of these people, it would be very difficult to hire them in today's job market. But if you think hiring them is difficult, retaining them is an even harder challenge. Security monitoring is inherently erratic: six weeks of boredom followed by eight hours of panic, then seven weeks of boredom followed by six hours of panic. Attacks against a single organization don't happen often enough to keep a team of the needed calibre engaged and interested. This is why outsourcing is the only cost-effective way to satisfy the requirements.

Medical care is a prime example of outsourcing that we can use for comparison. Everyone outsources healthcare, in the sense that we don't act as our own doctor, nor does anyone hire a private personal doctor. Certainly cost is a factor in our decision to outsource, but there's more to it than that. I may only need a doctor twice in the coming year, but when I need one I may need him immediately, and I may need specialists. Out of a hundred possible specialties, I may need two of them—and I have no idea beforehand which ones. I would never consider hiring a team of doctors to wait around until I happen to get sick, so I outsource my medical needs to my clinic, my emergency room, my hospital. Similarly, it makes sense for a company to outsource its network security needs to a variety of experts.

The benefits of security outsourcing are enormous. Aside from the aggregation of expertise, an outsourced monitoring service has other beneficial economies of scale. We can more easily hire and train our personnel simply because we need more employees and we can build an infrastructure to support them. We can learn from attacks against one customer, and use that knowledge to protect all of our customers. And from our point of view, attacks are frequent. Vigilant monitoring means keeping up to date on new vulnerabilities, new hacker tools, new security products, and new software releases. We can spread these costs among all of our customers.





To return to our medical care analogy, you get better medical care from a doctor that sees patient after patient, learning from each one. To an outsourced security company, network attacks are everyday occurrences and its experts know exactly how to respond to any given attack, because in all likelihood they have seen it many times before.

What to Outsource

There are, however, limits on what you should outsource. The bottom line is that you won't outsource everything, because some things just don't outsource well. Things that don't outsource well are often too close to your business, or they're too expensive for an outsourcing company to deliver efficiently, or they simply don't scale well. Knowing the difference is important.

Think about healthcare again. We all know what aspects of medical care we like: the ambulance picks us up in seconds and rushes us to the hospital, a team of medical experts spares no expense in running tests to figure out what's wrong and in doing whatever it takes to cure us. And we all know what aspects we don't like: ill-equipped and ill-staffed hospitals, HMOs telling us that we can't have that particular test or that a specialist isn't warranted in this case. The aspects of outsourced healthcare we like involve immediate access to experts. Any medical emergency requires experts, and the faster they can pay attention to us, the better off we'll be. The aspects of outsourced healthcare we don't like involve control of the process. Our healthcare is our responsibility, and we don't want someone else making life and death decisions about us. Network security is no different. Outsource expert assistance: vulnerability scanning, monitoring, consulting, forensics. Don't outsource control of the process.

An IT specialist can monitor networks. It can manage firewalls, IDSs, and IPSs and provide vulnerability scanning, e-mail scanning, and "clean-pipe" Internet connections. It has the expertise to deal with compliance issues. It can build a whole new security infrastructure for you from the ground up. In short, an outsourced IT specialist can take the problems of network security off the backs of a corporate IT department and let them focus on their strategic decisions.

What it cannot do is determine how an organisation's IT security interacts with its business. For example, when a hacker is inside a corporate network, only the organisation can tell what the business ramifications of different responses are. An IT specialist can detect an insider attacking your network and find out what they are doing, but they won't know whether he's malicious or performing authorized testing. Outsourced experts work best when they work with their customers, combining expertise with their knowledge of the business processes.

How to Choose an Outsourcer

Choosing an outsourcing partner is difficult, because it's hard to tell the difference between good computer security and bad computer security. But by the same token, it's hard to tell the difference between good medical care and bad medical care. If we're not health experts ourselves, we can sometimes be led astray by bad doctors that appear to be good. So how do you choose a doctor? Or a hospital? I choose one by asking around, getting recommendations, and going with the best I can find. Medical care involves trust; I need to be able to trust my doctor.

Security outsourcing is no different; you should choose a company you trust. To determine which one, talk with others in your industry or ask analysts. Go with the industry leader. In both security and medical care, you don't use a little-known maverick unless you're desperate. Watch companies that have conflicts of interest. Some outsourcers both sell products and offer managed security services. This worries me. If the service arm finds a problem with one of its products on my network, will the company tell me, or try to fix it quietly? If they discount their services in an attempt to sell products, who does their services division really work for?

In any outsourcing decision that involves an ongoing relationship, the financial health of the outsourcer is critical. Look for companies that are leaders in their field, have a strong history of security services, and don't try to do everything.





The Future of Outsourcing

Modern society is built around specialization; more tasks are outsourced today than ever before. We outsource fire and police services, government (that's what a representative democracy is), and food preparation (restaurants). In general, we outsource things that have one or more of three characteristics: they are complex, important, or distasteful. In business, we outsource tax preparation, payroll, and cleaning services. Outsourcing security is nothing new: all buildings hire another company to put guards in their lobbies, and every bank hires another company to drive its money around town.

Computer security is all three: complex, important, and distasteful. Its distastefulness comes from the difficulty, the drudgery, and the 3:00 a.m. alarms. Its complexity comes out of the intricacies of modern networks, the rate at which threats change and attacks improve, and the ever-evolving network services. Its importance comes from this fact of business today: companies have no choice but to open up their networks to the Internet.

Doctors and hospitals are the only way to get adequate medical care. Similarly, outsourcing is the only way to get adequate security on today's networks.

World News In Brief

MoD Admit SAS Data Disappears



The Ministry of Defence have announced that details about SAS soldiers has gone missing after a laptop without encryption went missing during a recent exercise in Britain.

The laptop (similar to that above) was being used by the Signals Regiment, who are attached to the elite force based in Hereford. The discovery of the missing laptop was revealed by Military chiefs during a routine audit kit check, who also identified that details of top secret anti-terror training exercises were contained on the PC, and it is believed to hold information about the names of personnel taking part.

Sources have revealed that the computer holds sensitive information about the military and counter-terrorism manoeuvres within the Signals Regiment. In a statement, the source, who cannot be named for reasons of security, has added that "the soldier in charge of the computer is panicking. It is very embarrassing because keeping tabs on kit is the most important part of working with the SAS."

The Ministry of Defence have insisted that the missing laptop does not hold information about operations or details of weapons. A spokesman from the MoD has given a press statement revealing

the opening of an inquiry into the possible theft of the computer and has also added "We can confirm that we are investigating the possible loss of a hard drive, containing only unclassified information which was being used on a training exercise." The spokesman then added, "We are carrying out our inquiries into what happened."

After the loss of many laptops last year, the realisation that the British Parliament and the Ministry of Defence should put better enforcement in to place, or actually follow what they have promised to implement into their data security for the last four years.

Whilst promising to fortify the measures of security, the MoD information is said to be protected and encrypted. However, it came to light that the Ministry of Defence loses around 15 laptops per month, through the loss or theft of computers and laptops.

Although the Mod have insisted that the latest of data losses did not contain the details of the operations or weapons within the SAS, Shadow Defence Secretary Liam Fox said that the loss was "deeply concerning". He expressed this in a further statement: "Any loss of data of this nature is deeply concerning, especially if there are security implications." The Defence Secretary then went on to say, "We will want to know the full picture from the Ministry of Defence as soon as possible to ensure that neither civilians nor military personnel are at risk."





Southampton University investigates the biometric potential of OAE

By Tom Tainton, Smartcard & Identity News



Tom Tainton

The security industry finds itself in a no-win situation. Consumers demand quick and instant access to resources, but appear reluctant to cooperate with invasive or time-consuming identity verification. But scientists from Southampton University are aiming to change that by investigating the potential for Otoacoustic emissions (OAE) to be used as a biometric application for identification purposes. The unique three year project, which began in January 2007, is conducted by researchers from the School of Electronics and Computer Sciences is set to create a new-look personal identity verification schema. All for a research grant of just three-hundred and fifty thousand pounds – a bargain when you consider identity derived fraud reportedly costs the government nearly two billion pounds every year. So how does it work?

Well, OAE are low intensity sounds produced by our ears in response to audio stimulation and are generated by the activity of the outer hair cells. The emissions produced by the human process of amplifying low level sounds can be detected at the entrance of the ear. Evidence suggests that OAE is unique to each individual and can even be used to distinguish gender and ethnicity. Not only have OAE proven to be exclusive to a person, the characteristics depend upon the input sound in a manner that also varies between individuals. This offers particular opportunities when applying the practice as a biometric system.

Leading the investigation is Dr. Steve Beeby. He said, “We hope the project will establish OAE as a robust biometric analysis which in the future will be used to identify and verify individuals. If successful, the scheme would have a significant impact on the security industry. Because a high level of classification performance can be obtained using the raw time-pressure data, the potential is there to satisfy consumer and producer demands.”

There are a number of advantages an otoacoustic-based biometric system enjoys over other forms of identity verification. Firstly, it can be embodied in a telephone handset or set of headphones, technology which everybody is familiar with and thus is socially acceptable. Secondly, OAE can be employed in a challenge-response dialogue (whereby one party presents a question and another party must provide a valid answer such as a password to be authenticated.) The stimulus dependent nature of the OAE will increase the performance and effectiveness of the biometric. In addition, OAEs can potentially help retrieve stolen mobile phones by rendering them useless if the phone recognises the user is not the legitimate owner and subsequently disables itself.

However, there are still elements that need investigating if OAE is ever going to usurp other identity verification options. Dr Beeby said, “The potential long term drift of emissions, the influence of hearing impairments such as ear infections and the effect of external noise are issues which could affect the reliability of our results. Also, in subjects who have consumed alcohol or drugs, the emissions can be deadened or altered.

There’s still a while before OAE will become a fixture in real life security applications. First the technique will have to consistently churn out low false-match rates and prove that an individual’s recorded OAE stays recognisable over a long term period. Dr Beeby said, “There’s a lot still to do but we’re working in conjunction with the Engineering and Physical Sciences Research Council (EPSRC). The first step is developing an on-the-ear probe that efficiently captures the emissions in a range of situations, and is acceptable to the user. We’re confident that in five to ten years the OAE biometric system will be a sufficiently developed application.”

