Identity News • Smart Card & Identity News • Smart Card & Identity News • Smart Card & Identity News • Smart Card & Identity News • Smart Card News • Smart Card & Identity News • Smart Card & Identity News • Smart Card & Identity News • Smart Card & Identity News • Smart Card & Identity News • Smart Card & Identity News • Smart Card & Identity News • Smart Card & Identity News • Smart Card & Identity News • Smart Card & Identity News • Smart Card & Identity News • Smart Card & Identity News • Smart Card & Identity News • Smart Card & Identity News

August 2009

Volume 18 • Number 8

Smart Card & Identity News

Smart Cards, SIM, Payment, Biometrics, NFC and RFID
www.smartcard.co.uk

UK ID Card Hacker Cloned

This month the Daily Mail has brought us the news, a hacker, not an ordinary hacker but a genius in the form of Adam Laurie has cloned a UK ID card in 12 minutes. Well in fact we could just as easily say he has cloned himself because the same logic as that presented by the Daily Mail would hold and what a remarkable discovery that would be.

Not wanting to dispute the talents of Adam Laurie because we agree that the security of the UK National ID Card scheme is flawed but the real problems are being hidden in smoke by parts of the media, perhaps this is a government ploy to avoid disclosure? So what are the facts surrounding this bit of sensationalism in the UK media?

Laurie obtained one of the new ID cards issued for foreign nationals working or studying in the UK. Not in dispute is the fact that the card has an integrated circuit chip which contains details of the authorised holder including their name, date of birth and some biometric data such as their photo and fingerprint images. It is also agreed by the Home Office that the National ID card will have the same format as this foreign national's card.

Our Comments

Patsy Everett

Dear Subscribers

I came across an interesting article this month, apparently when we read about these news items on data loss like CDs being lost in the post or tapes (do people still use them?) falling off the back of a lorry it's not true and is typically just a cover up.

Eric Hibbard is a member of the SNIA technical council and CTO for security and privacy at Hitachi Data Systems who in a discussion with iTWire reported that organisations sometimes talk to him when they won't talk to the authorities. What they make public is not really the way it happened and often the perpetrator got to the source of the privacy information which an organisation is legally obliged to report but they don't have to report how it happened.

Now this takes a bit of thinking about and yes we're back to the same question of human behaviour. Now this one is really interesting because it comes in two parts, does the responsible person report the compromise of the data and if so does (s)he report it correctly?

It's simple game theory really and not that I pretend to be an expert on the maths but I sure know about people who will think along these lines: Am I likely to get caught and if so what will be my punishment compared with the punishment for admitting the offence in the first place?

I'm the first one to be surprised at how many cases we hear of lost memory sticks and laptops because I believe that what we hear about can only be the tip of the iceberg. It's the case of when the miscreant can't cover it up. Missing laptops may be discovered although with the MOD losing £30 billion of equipment I'm not too sure of that one either.

However missing memories sticks, now who is going to admit to that? Only the most conscientious of employees are likely to own up. And this is my personal experience that only a small percentage of people admit to faults that are unlikely to be exposed.

Perhaps worse is the number of people that seem remarkable adept at concocting fiction with unbelievable conviction when the occasion arises. In security more noise is made about confidentiality but when you get down to it integrity of people is much underrated.

So back to Eric's hypothesis, that companies misreport what really happened when it comes to a security breach. Now I think this is really the point that somewhere the corporate arm makes a statement. I know that there are people in side, quite remote from the breach reporters, but they are faceless and will do all in their power to protect the organisation. So will they misrepresent what really happened?

The answer to this one is surprisingly straight forward not only in my

experience but also those of colleagues. The larger companies with a structured management tier try to get it right and in general seem admirably conscientious about their security responsibilities and behave accordingly.

The problem comes with organisations that are run in an autonomous fashion which is usually where the people involved are an integral part of the organisation. In other words their perceived destiny is totally intertwined with the health of the organisation. In these examples you can throw away the book.

There has recently been a body of opinion that believes the UK government (and others) operates in an autonomous fashion? I hope they are mistaken!

Patsy.

Contents

Regular Features

Industry Articles

Events Diary

September 2009

1 – 3	Mobile Payments World Asia 2009, Singapore -www.terrapinn.com/2009/mpayments
2 – 3	Mobile NFC, London, UK -www.mobilepaycom.com/newt/l/mpayments/mobilenfc
6 – 9	Cryptographic Hardware and Embedded Systems 2009, Lausanne, Switzerland - www.chesworkshop.org/ches2009/start.html
9 – 11	Cards & Payments 2009, Paris, France - www.efma.com
10 – 12	E-payments India 2009, New Delhi - www.electronicstoday.org/epayments2009.htm
10 – 12	Smart Card Expo 2009, New Delhi - www.electronicstoday.org/smartcardsexpo2009
15 – 16	Prepaid Cards & e-money CEE, Warsaw, Poland - www.prepaid-conference.com/cee
15	The 5th ISG Smart Card Centre Open-Day, Royal Holloway, University of London, Surrey, UK - www.scc.rhul.ac.uk/events.php
22 – 24	5th Symposium on ICAO MRTDs, Biometrics & Security, Montreal, Canada - www2.icao.int/en/mrtd/Pages/
22 – 24	The Biometric Consortium Conference, Florida, USA - www.biometrics.org/bc2009/

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

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

UK ID Card Hacker Cloned …. Continued from page 1

The chip operates in contactless mode as per ISO 14443 and as the Daily Mail puts it has a tiny antenna (aerial to UK nationals) that allows the card to bounce back information when contacted by a special electronic reader. Still OK at this point? but now the Daily Mail starts to get carried away,

"and it is this which was supposed to be the 'unbreakable' security measure that would ensure ID cards could never be cloned or faked"

What Laurie has shown is that you can establish a cryptographic session with the smart card because the key is derived from information displayed on the card, i.e. ID card number, holder's date of birth and expiry date. This is the same approach as that used by the UK's new biometric passport as standardised by the International Civil Aviation Organisation (ICAO) which is called Basic Access Control (BAC). In other words the ID card scheme is following the same ICAO standards. It should be noted that in the case of the ePassport at least that BAC is optional although it is applied by the UK.

Above: Front & Rear - UK ID Card

Now I have never heard anybody from the Identity and Passport Service (IPS) to have claimed that the ID card or ePassports as being unbreakable. You also really need to start with the ePassport because that's where the ICAO standards come from. The assumption is that a travel document in the form of a passport will now in addition to all the other security features including the Machine Readable Zone (MRZ) also include a contactless integrated circuit chip. So the primary purpose of the chip is to provide storage of electronically protected and readable credentials. This is referred to as Passive Authentication in the ICAO world, in other words the data stored in the chip is digitally signed which means that it should not be possible to modify the data without detection.

4

Yes, we've got there, ePassports and UK ID cards operate against the ICAO standard for machine readable documents and they incorporate an integrated circuit chip that stores digitally signed data relating to the holder of the document. There is at this stage no mention of anything to do with the security, authenticity or correctness of the chip. What we do know is that the data is authentic and unmodified (lets accept here that the digital signatures are well implemented).

Now the daily mail story goes on to tell you how Laurie was able to simply change this data and store it on an equivalent RFID chip. The Daily Mail seems to think that ID chips are based on Mifare as used by the London Oyster card scheme but we'll ignore their lack of understanding in this area. However the gist of the story is correct in that you could modify the data and you could store it on another similar chip **BUT** you would not be able to provide the correct digital signature that goes with the data. In this sense you have not breached that part of the ICAO standard. Their security policy relies on the security of the complete passport document and the correctness of the data in the chip by means of the digital signature.

And this is the punch line, it is pointless having a scheme using cryptographically protected data if you don't check the protection features. This is no different to the chip and PIN card operating in off-line mode when using Static Data Authentication, if you don't check the cryptogram then you won't know if the card/transaction is authentic. You can copy ePassports, ID cards and Chip and PIN cards but they won't fool any terminal that is checking the digital signatures (or cryptograms). It's no different to photo copying a £20 note it's just that in this case the receiver has a habit of checking that the note looks valid.

You are not really cloning the chip and in the case of the ID card you could more amusingly imagine that you can clone the holder of the card.

So what do we do about all this? Well there are two issues, the first is easy to solve, and the second one is really where the problem lies,

    1)   Apply a chip authentication mechanism
    2)   Sort out the key management

It is easy to apply chip authentication mechanisms, most smart cards have them and its part of the fundamental ISO 7816-4 standard for Identification Cards with Integrated Circuit Chips. Passports and ID cards have it as well with Extended Access Control (EAC). It's not actually being implemented at the moment but this would not only provide chip authentication but terminal authentication as well.

Key management will stir the heart of all enthusiastic security practitioners, that's because they know how difficult it is. This is the real problem with ePassports and ID cards and the trouble is that nobody has worked out how to get all the right keys in the right place at the right time in a secure fashion. For the UK assuming the ID card is for home consumption then it is relatively easy but for international use particularly passports well then you need international governments to come together – don't hold your breath!

Dr David Everett.

World News In Brief

Global Shipment of Smart Card Surpassed 5 Billion in 2008

The smart card industry has been continuously expanding, with countries across the globe identifying its true potential. The number of Smart card application projects has also been rising, demonstrating the versatility and robustness of the technology. The growing security needs, possible multiple usage and greater storage and processing capability are driving the growth of smart card industry world over and will also continue to do so in future. The global shipment of smart card surpassed an estimated 5 Billion units in 2008 and this figure is projected to surge at CAGR of nearly 11% through 2012, according to ""Smart Card Market Forecast to 2012", a recent market research report by RNCOS.

The telecom sector is the biggest application market for smart cards, occupying more than 70% of the global smart card shipment in 2008. Growing number of mobile subscribers remain the largest contributor, driving sales of SIM cards worldwide. Use of smart cards in financial services sector has also been on rise buoyed by increasing use of Europay, MasterCard and Visa standard (EMV) standard.

5

Increasing use of internet for making online payment transactions is also fuelling growth in the global smart card industry as this technology enables consumers make secure and reliable transactions. Use of contactless smart cards in this regard has gained remarkable consideration and is forecasted to grow at CAGR of more than 30% through 2012.

The research anticipates the transport sector to experience the largest growth in usage of smart cards worldwide, CAGR projected at nearly 26% in near future.

Cryptography Research Announce License Agreements with both Atmel Corporation & INSIDE Contactless

Atmel Corporation & INSIDE Contactless both signed patent agreements to use Cryptography Researches smartcard attack countermeasures.

Atmel & INSIDE Contactless hope CRI's patents will enhance the security of their tamper-resistant chips against Differential Power Analysis (DPA) and related attacks.

The licenses also cover third-party software executing on microcontroller chip products, allowing customers to develop their own DPA countermeasures without the need for a separate license from Cryptography Research.

Atmel's Marketing Manager Hervé Roche said, "Security is one of our main focus areas, and our strategy is to develop the most advanced secure microcontrollers with state-of-the-art protection mechanisms against a multitude of attacks. This agreement enables Atmel to strengthen its leadership in the security market"

"Cryptography Research has made pioneering contributions in the area of tamper-resistant semiconductors with its DPA technology and intellectual property portfolio," said Charles Walton, executive vice president of payments for INSIDE Contactless. "This agreement allows INSIDE to distribute MicroPass products with DPA countermeasures to our manufacturing customers without their need to distinctly obtain licensing from CRI."

DPA is a form of attack that involves monitoring the fluctuating electrical power consumption of a target device and then using advanced statistical methods to derive cryptographic keys and other secrets. Strong countermeasures to DPA help protect tamper-resistant chips used in applications such as banking, pay television, mass transit, secure ID, and wireless telecommunications.

Cryptography Research has been awarded a portfolio of approximately 50 patents covering countermeasures to DPA attacks.

Cryptography Research, also announced the hiring of Pankaj Rohatgi as technical director, hardware security solutions. Rohatgi an experienced cryptographer and security researcher will help Cryptography Research's engineering team expand its research and development capabilities.

Rohatgi worked for IBM for 13 years as a research scientist and was manager of the information security group for the past four years. He played a significant role in developing products such as the IBM 4758 crypto co-processor and IBM's System S, and he led several security projects within IBM and with commercial and government customers. He also conducted research in cryptography, side-channel analysis, network and systems security and security for embedded systems.

Dutch Ministry of Foreign Affairs selects Siemens and Bell ID for Card Management System

Siemens IT Solutions and Services (SIS) has signed an agreement with the Dutch Ministry of Foreign Affairs to supply a card management system for the Rijkspas, the new multifunctional card for Dutch civil servants. The solution, ANDiS4Rijkspas, relies on commercial software by Bell ID. The system enables the Ministry to manage the lifecycle of the cards, and is scheduled to be operational by October 2009.

Based on their previous card management experience, Siemens and Bell ID were able to configure a ready-made solution to issue and manage the Rijkspas for the Ministry of Foreign Affairs. ANDiS4Rijkspas is also designed so that it can be swiftly implemented and deployed at other State departments.

ANDiS4Rijkspas will initially be used for access control within the department. In the second and third phases, the Rijkspas will facilitate interdepartmental access and secure access to their IT systems.

ANDiS4Rijkspas is an all-in-one card management system that supports, both issuing and withdrawal of cards, as well as the monitoring and auditing the various processes involved. ANDiS4Rijkspas also offers the capability to manage applications for logical access and the platform can be enhanced with a module that facilitates secure PC logon and secure e-mail traffic using the Rijkspas.

6

European Banks Consider Magnetic Stripe Card Ban

By Tom Tainton, Smartcard & Identity News

Tom Tainton

The chairman of the European Payments Council (EPC), Gerard Hartsink, recently announced that European banks may consider a ban on magnetic stripe cards by 2011, as widespread adoption of chip-and-pin credit cards continues to flourish. The EPC, established in 2002, is driving the transition to the Single Euro Payments Area and advised its members to stop accepting magnetic stripe cards. The technology is deemed less secure than the EMV alternative, an international standard specifying how smart card chips can replace the magnetic stripe on bank cards.

The decision to discard magnetic stripe cards altogether could have serious implications for U.S credit card merchants, who use magnetic stripe technology over chip-and-pin. While Europe made the switch to Chip-and-PIN in 2004, largely due to the fraud protection benefits, the reluctance of the U.S to follow suit has left them lagging behind in credit card technology. So is it too late for the U.S industry to make the switch, and how will this affect American travellers?

Well, U.S citizens travelling with their magnetic stripe cards can rest assured – European Chip-and-PIN readers are capable of processing magnetic stripe cards as well. So any horror stories you may have heard (i.e. Joe Weiss, the U.S attorney who couldn't use his card anywhere in France) are either a case of fear mongering, or an unfortunate rarity. Across the pond, the challenge lies in the cost and complexity of making the transition to EMV technology. Chip-and-PIN cards are processed using different terminals than those used for magnetic stripe cards. In Europe, the issuer is involved with the payment, as EMV uses 'smart card' technology which renders the card powerless without a PIN. However, in the U.S, issuers are separated from the payment processing system and subsequently are in no position to force merchants to purchase the new Chip-and-PIN terminals.

Another stalling point is the complexity of America's multilayered payment system. Frankly, converting to Chip-and-PIN just wouldn't be as simple as it was in Europe. Even with the inflated costs, the switch made sense for Europe as EMV technology dramatically improved efforts in preventing credit card fraud. Europe's system is essentially offline, which means that transaction information isn't instantly updated when a purchase is made. As a result, credit card fraud can't be detected at the point of sale.

The U.S system is online, so fraud is more frequently detected at the point of sale and suspicious activity can be flagged. Some experts argue that the reason the U.S is less hasty to adopt smart cards is because the risk of fraud is significantly lower than in Europe – where fraud detection isn't possible until after the event. Yet, there is conflicting evidence that suggests international credit card thieves are beginning to target the U.S. According to the U.K. Payments Administration, growth in credit card fraud cost the UK consumers £535.3m in 2008. In comparison, fraud and identity theft cost the U.S $48 billion – a vast difference.

Last year, eleven fraudsters stole 45 million credit and debit card numbers from companies such as TJX, Boston Market and Barnes & Noble – the biggest case of identity theft in U.S history. Then, in 2009, Heartland Payment Systems were targeted, and millions of card transaction details breached. Even the hackers themselves aren't safe! In a twist of delicious irony, criminal hackers pulled off an ATM 'skimming' scan at the annual Defcon conference in Las Vegas, a meeting of hackers from all over the world. It seems nobody is immune to the threat of identity theft.

The decision for card issuers in the U.S is a tough one. The switch to Chip-and-PIN is not an easy one, but after significant data breaches which resulted in millions of cards being compromised, and issuers, banks and consumers all suffering, it would seem that a solution is drastically required. American credit card companies are already sharing higher costs driven by the increase of data breaches and online crime. For those reasons, it's about time issuers reconsidered the economics of EMV migration.

7

Datacard Group to Provide Solution for National Identity System in Guatemala

Datacard Group was chosen this month to supply card personalisation equipment and software for the new national identification system planned in Guatemala. The country's Registro Nacional de Personas ("RENAP") intends to issue electronic identity (eID) cards to more than 11 million residents to both improve the process of citizen authorisation and reduce benefits fraud. Issuance of the cards began July 1, 2009.

Guatemala's new civil registry database will utilise Automated Fingerprint Identification System (AFIS) and facial recognition biometrics. When a citizen enrols in the program, two fingerprints will be taken and a face-print will be made using facial recognition software. These biometrics, along with the citizen's biographic information, will be stored both in the civil registry database and on a smart chip imbedded into the identification card.

The cards for this program need to provide an expected usage life of up to 10 years, so polycarbonate cards were chosen. The printed personalisation was laser engraved into the substrate, enhancing both durability and card security. The card designs incorporate three levels of security measures - those visible to casual visual inspection (level 1), those visible using special enhanced visual inspection techniques (level 2) and those that require laboratory or forensic inspection (level 3) - to ensure the highest resistance to fraud and counterfeiting.

"This new eID program will be rolled out immediately as Guatemala's primary national identification card," said Fred Ketcho, regional vice president of Americas Sales and Service for Datacard Group. "Once the entire infrastructure is in place countrywide there are plans to use the cards for banking and services at other government facilities."

Innovision Raises nearly $9 million to Fund its next NFC Growth Phase

Innovision Research & Technology this month announced that it has secured funding of nearly $9 million (£5.4 million) from existing and new institutional investors to take advantage of its strong position in the growing Near Field Communication (NFC) market. The funding will be used to further develop and capitalise on opportunities for the company's NFC Intellectual Property (IP) and tags

and help consolidate its position as the foremost NFC IP technology developer.

Ultimately, the company sees its tag technology enabling a multitude of applications and smart objects. In March this year, Innovision announced it is supplying NFC tags for mobile operator mobilkom Austria; and it has also deployed tags in NFC-enabled electronic photo frames and speakers developed by Parrot.

Innovision is also making progress in its planned entry into the Chinese market, winning its first significant RFID contract for supplying analogue technology, which will see two chips launch in 2010 in China for a major Smartcard company. The firm has also sub-contracted manufacturing of its chips and complete tags within China - an important step in enhancing its position in the growing tag market in the country.

"As far as Innovision is concerned, our business model for NFC will continue to focus on propagating our IP with major semiconductor vendors for use in 'combo' and other chips designed for the mobile handset, laptop and consumer device markets. We believe 'combo' chips are a major growth area in handsets, combining multiple wireless functions, such as Bluetooth, WiFi, FM and GPS on a single chip.

L-1 Identity Solutions Receives $9.6 Million in Mobile Biometric Systems

L-1 Identity Solutions, Inc. have received new orders totalling $9.6 million for HIIDE and PIER mobile biometric recognition systems to be deployed in areas of conflict as part of existing customer agreements. Two thirds of the HIIDE order and all of the PIERs are expected to ship in the third quarter. The remaining HIIDEs will be shipped in Q4 2009. The order was received by the Biometrics Division of L-1.

HIIDE is a ruggedized tri-modal mobile biometric enrolment and recognition device providing real-time identification using iris, finger and face biometrics. First introduced in 2005, it is the most pervasive device of its kind with over 10,000 devices fielded into areas of global conflict. It is also the most widely deployed multi-modal device with defence agencies. More than 4,500 PIER devices are in the field today, used for iris-based mobile biometric enrolment and identification.

8

The Challenge of EMV at the ATM

Martin Macmillan, Business Development Director, Level Four, discusses how the roll out of EMV smart cards has impacted upon the ATM channel and how automated testing can help manage this change.

Martin Macmillan

Since the standard's introduction in the UK in 2004, EMV has caused a substantial reduction in card fraud, which declined by 25% within the first two years. However, this comes at a cost. EMV Chip and PIN cards are far more complex than the previously used magnetic stripe card and, as a result, ATMs have had to evolve significantly to account for this.

The difference between the magnetic stripe card and Chip and PIN is that the latter is dynamic making it possible to write data in the Chip. Consequently, the ATM must be able to read the data within the Chip and also interact with that data.

Because this process is more complicated, there are more systems within the ATM which could potentially fail. Consequently, ensuring ATM uptime is now a key focus for banks at the ATM since crashes can negatively impact brand reputation and customer loyalty.

In order to maintain maximum levels of uptime, ATMs must be regularly tested in order to anticipate and correct any potential problems, such as ATM software malfunctions or faults with the chip card hardware. Therefore, banks need to conduct extensive end-to-end testing across their ATM networks to account for every possible card scenario and also to check the consistency of these results.

Typically, End-to-end testing must encompass the ATM, all the relevant card types, the host that drives the ATM, as well as the external switching and authorisation networks (e.g. card schemes) that are involved in the transaction chain. Consequently, testing of EMV-based ATM transactions requires hundreds of different test scripts and, when multiplied by the number of different card types, this results in thousands of test case scenarios.

Under the magnetic stripe card system, when there was only one type of card and far fewer tests were required, banks used to test their ATM networks manually. Nowadays a manual testing regime for EMV-based transactions is untenable. Manual tests can take up to one hour and a complete test cycle would take months to conduct, during which time and ATM network might experience high levels of undetected downtime. Consequently banks are increasingly migrating to automated testing to ensure they are able to successfully maintain high levels of uptime.

Using automated testing, banks can complete a full test cycle in as little as 48 hours. Furthermore it allows banks to test their entire networks on demand. Whilst the risk of faults in a network would never reduce to zero, effective test automation means that downtime can be reduced to a minimum. However, there is much confusion surrounding how to implement best practice automated ATM testing.

There are five key points that banks must consider when implementing an automated and integrated ATM system test strategy:

1. Understand the business drivers and establish the deliverables against investment.

2. Get buy-in from the relevant stakeholders within the bank.

3. Set the strategy upfront and have a clearly defined test plan in place.

4. Create specific and granular test cases. Best practice dictates that a test strategy should encompass between 5,000 and 8,000 test cases depending on the complexity of the ATM software application and level of available functionality.

5. Finally, ensure these tests can be run regularly. A handover from the domain staff to the day-to-day test staff is essential and there is also a need for a centralised repository of information, including a master list of cards and accounts.

With migration to EMV in the UK virtually complete, banks must evolve their testing strategies in order to address the true complexity of the ATM channel. With solid processes in place, banks will be in the best position to fully realise the potential of the ATM channel.

9

Commerce Commission and Visa reach agreement to settle credit card interchange fee proceedings

The Commerce Commission has signed an agreement with the Visa International Service Association and Visa Worldwide Pte Limited (Visa) settling the Commission's claims against Visa in relation to credit card interchange fees. The Commission's proceedings allege that the rules of the Visa scheme providing for the payment of multilateral interchange fees, together with related rules, breached the restrictive trade practices provisions of the Commerce Act.

As a result of the agreement, Visa will make changes to the way the Visa scheme rules will apply in New Zealand. Those changes are:

Credit card issuers will now be able to individually set the interchange rates that will apply to transactions using their credit cards, subject to maximum rates determined by Visa. These rates will be publicly available.

Merchants will no longer be prevented from applying surcharges to payments made by credit cards or by specific types of credit cards. Merchants will also be able to encourage customers to pay by other means.

Visa has confirmed that non-bank organisations or companies who might wish to provide acquiring services to merchants are permitted to join the Visa network as acquirers if they meet relevant financial and prudential criteria.

"The Commission considers that the agreed changes to the Visa rules will, over time, improve competition between companies that provide credit card services to retailers in New Zealand. Those changes are in the long-term best interests of both New Zealand consumers and retailers," said Commerce Commission Chair Dr Mark Berry. "The Commission considers that this increased transparency will assist retailers and customers in making decisions about their payment choices."

Infineon Firmly Expands Its Market Position

Infineon Technologies AG expanded its market position in semiconductors discrete components and modules for power electronics for the sixth year in a row. According to IMS Research's 2009 report "The World Market for Power Semiconductor Discretes & Modules" the global market for these devices grew by 1.5 percent in 2008, to US $13.96 billion (from US $13.76 billion in 2007), whereas Infineon grew by 7.8 percent. Infineon now commands 10.2 percent of that market, with its nearest competitor holding 6.8 percent. Infineon also continues to lead in the EMEA region (Europe, Middle East, Africa) and the Americas capturing 22.8 percent and 11.2 percent share, respectively, in these regions.

With demand for increased energy efficiency in motor vehicles, consumer and industrial applications and growth in the traction and renewable energy segments, Infineon is determined to further build its power semiconductor discretes and power modules sales. For the renewable energy sector market research firm IMS Research anticipates a five-year CAGR (Compound Annual Growth Rate) of 18.2 percent with wind power and solar power installations being the main drivers. Infineon's discrete IGBTs and MOSFETs help raise solar inverters' efficiency above 98 percent and feed as much of solar-based electricity into the power grid as possible.

" Power semiconductors play a central role in global efforts to improve energy efficiency in automotive and industrial applications, and to help improve the utilisation of electrical energy in home appliances", said Arunjai Mittal, Infineon Technologies.

Giesecke & Devrient Publishes Offer to secunet AG Shareholders

Giesecke & Devrient (G&D) is making secunet Security Networks AG (secunet) shareholders an official offer of EUR 5.70 per share. Germany's Federal Financial Supervisory Authority (BaFin) has now approved the offer. The offer has a time limit and closes on September 30, 2009 at midnight. G&D holds a 76.4 percent stake in secunet. G&D had announced the voluntary public offer for purchasing the remaining shares in July when it acquired the share package from RWTÜV AG, the major shareholder.

G&D's purchase offer of EUR 5.70 per share gives all secunet Security Networks AG shareholders the opportunity to sell their shares at the same price as RWTÜV AG, the long-standing major shareholder. The offer price includes a 43 percent premium over the average XETRA price on the 200 days before the decision to make the purchase offer was published. secunet shares have not traded at that level in over a year.

10

secunet is a specialist in high-security IT solutions, with international enterprises and public authorities among its customers. IT security technology is a strategic business field for G&D. Acquiring these shares will allow the Munich-based company to strengthen its foothold and continue expanding its market position in this segment.

G&D initially acquired the majority stake of 50 percent plus one share from RWTÜV AG and T-Systems in February 2004. In July 2009, G&D increased its stake to 76.4 percent by purchasing the RWTÜV AG shares.

Sony Ericsson Announces Changes to Company Leadership

Sony Ericsson Mobile Communications has announced that Bert Nordberg, currently Executive Vice President of the Ericsson Group and Head of Ericsson Silicon Valley, will join Sony Ericsson as Co-President effective 1st September. Mr. Nordberg will work closely with Sony Ericsson President Hideki (Dick) Komiyama and the entire senior management team to effect a smooth management transition. Mr. Nordberg, who will be based at Sony Ericsson's global headquarters in London, will assume the role of President, Sony Ericsson Mobile Communications, on 15 October, and Mr. Komiyama will retire from the company at the end of the year.

In 2014 Monthly Mobile Data Traffic Will Exceed 2008 Total

In 2014, the volume of mobile data sent and received every month by users around the world will exceed by a significant amount the total data traffic for all of 2008, according to a new study from ABI Research.

"When people think of mobile data they think of BlackBerry and iPhone handsets," says senior analyst Jeff Orr. "But the bulk of today's traffic is generated by laptops with PC Card and USB modems." While add-on cellular modems represented two-thirds of traffic in 2008, computers with embedded 3G/4G modems will lead in 2014 with more than 50% of the world's mobile data traffic.

Other key findings from the study include:

Global mobile data traffic surpassed 1.3 Exabytes transferred during 2008. By 2014, an average of 1.6 Exabytes will be sent and received monthly.

Nearly 74% of the world's mobile data traffic will be from Web and Internet access by 2014. By the same time, 26% will come from audio and video streaming. Peer-to-peer file sharing and VoIP

contribution to overall mobile data traffic will be less than 1%.

Video streaming will experience the fastest growth of any IP traffic type at a CAGR of 62% between 2008 and 2014.

Western Europe accounted for nearly 31% of mobile data traffic in 2008, but the region will yield to Asia-Pacific, which will account for over 28%, by 2014.

"The launch of 4G services promises even more data capability - full multimedia on a greater number of devices," notes Orr. "But it's a more pragmatic approach than 3G's: data-centric devices will be adopted first, rather than a large number of phones. As network coverage and service plans satisfy market expectations, a variety of specialized consumer electronics devices with the ability to connect anywhere will emerge."

CTA Outlines Next Generation Fare Collection Project

Chicago Transit Board was provided a report on plans to transition to a new fare-card payment system. This project would introduce the use of contactless credit cards, debit cards and prepaid cards to ride the system. CTA expects to issue the request for proposals for a two-step competitive procurement process this month.

The transition would save the CTA money now used to issue fare media and manage the fare payment and collection system. The contactless fare payment system would reduce the need for customers to carry cash or have the right denomination or currency to ride the system. In addition, the same card could be used for everyday transactions such as purchases at retail outlets.

The first phase of the procurement process will examine the CTA's options for developing the card - considering possible procedures, management and cost of the program. After reviewing these proposals and developing a final plan, the second phase will give companies the opportunity to submit proposals for the actual implementation of the program.

The farecard would be a smart card containing a computer chip that allows customers to pay a fare and also serves as a standard credit or debit card tied to a customer's bank or credit card account. A prepaid card could provide the option for customers who choose not to have the card tied to a bank account.

The CTA expects to complete the two-step RFP process and begin the transition to an open fare system next summer.

11

Is the web browser your nemesis for data leakage?

By: Yuval Ben-Itzhak, Chief Technology Officer, Finjan, Inc.

Yuval Ben-Itzhak

The incidents of data intentionally or unintentionally leaving corporate networks are rising. The CSI Computer Crime & Security Survey of 2008 showed that 44% of the polled companies registered data leakage to be the second biggest problem of their corporate IT security. In a survey conducted among German companies, less than 25% were found to use HTTP traffic monitoring systems for protection from confidential data leakage. An older survey conducted in the US, investigated how data is being leaked through communication tools. Survey results showed that HTTP was the leading avenue for data leakage. Furthermore, it was found that customer data represented the vast majority of data leaked to unauthorised parties, followed by confidential information and Protected Health Information (PHI).

Data Loss Prevention or Data Leakage Prevention (DLP) is now a major issue, affecting the bottom line of enterprises. According to recent research, the total number of data loss incidents in 2008 has risen by 2600% compared to the total number of data loss accidents in 2004.

Not only companies, but also governmental agencies are at risk. One of the latest incidents occurred in May 2009 consisting of accidental data leakage. Some parties received electronic data consisting of the latest unemployment and average earnings figures from the Office for National Statistics (ONS) before their official publication date. The ONS was forced to officially release these figures ahead of time, resulting in the Pound Sterling bouncing higher. (The released data showed a smaller than expected rise in claimant count unemployment even as the overall unemployment rate rose to 7.1 percent). This incident is the latest addition to string of data breaches the British government has suffered over the past two years. They include leakage of secret intelligence files, the details of every prisoner in England and Wales, and information about thousands of potential army recruits.

Data leakage has grown into a global problem, as the following incidents show.

- In February 2009 in Hong Kong, more than 60 restricted government documents were leaked on the internet through file-sharing software "FOXY", forcing the Privacy Commissioner for Personal Data Mr. Roderick B. Woo to take immediate action.

- In the beginning of 2009, Dartmouth College researchers (US) searched file-sharing networks for key terms associated with the top ten publicly traded health care firms in the country. Over a two-week period, they discovered numerous sensitive documents, including a spreadsheet from an AIDS clinic with client details; hospital databases containing detailed information on more than 20,000 patients; a 1,718-page document from a medical testing laboratory containing patient data; and more than 350 megabytes of sensitive patient data from a group of anesthesiologists.

- In April 2009, a data leakage incident occurred in a Prague hotel (Czech Republic). The flight details and passport numbers of around 200 EU leaders, including those of a Finnish state delegation, were leaked by accident. The data was related to a recent EU-US summit held in Prague and attended by U.S. President Barack Obama.

- In April 2009, an employee of Mitsubishi UFJ Securities Co., who was deputy chief of their computer department, sold personal data on more than 49,000 of its customers to three dealers who specialise in personal data lists, which in turn sold them to more than 80 real estate agents and other firms.

- In March 2009, a spreadsheet containing customer data of Kabel Deutschland (a German provider of Internet, cable TV and telephony) was leaked to questionable call centres.

12

Data leakage prevention (DLP) is gaining more and more attention as governments and organisations also realise the danger to their compliance status and to their commercial health. Web 2.0, especially Peer-to-Peer (P2P) networks, provides conduits through which information can leak. Especially intellectual property and patient information disclosed on P2P networks are at risk. IBM's Many Eyes, which is essentially a mashup application for visualising data, contains a lot of data that probably shouldn't be there, such as sales forecasts, corporate income statements, and data from government agencies, including the CIA.

Although most data loss is unintentional, we see a growing number of intentional data loss incidents. During mergers, layoffs and reorganisations, corporate data are vulnerable. An employee could leak data for their personal benefit. Such data include customer lists, intellectual property (IP) and other business data that could be useful for the (former) employee.

Organisations around the world have become aware of their need to protect their outbound data in transit. This growing demand has resulted in a booming market for DLP solutions; expected to reach $2 billion by 2012. Protecting loss of data in transit is complicated, even more so when malware is involved as in the case of "Trojans phoning home". The optimal way to prevent data leaking out of the network is the use of a Gateway-based web security solution. Such solutions consist of dedicated hardware/software platforms. They analyse network traffic to search for unauthorised information transmissions, including IM, FTP, HTTP, and HTTPS.

When selecting a DLP solution, an enterprise needs to focus on the following elements:

- All outbound communication should be analysed in real time and identified by their true content payload, not just by their file extensions. True Content Type detection capabilities prevent selected file types from leaking out or being downloaded by users.

- Administrators should be able to set policies based on dictionaries/lists containing words or formats (such as customer or employee information with names, addresses, social security numbers and other identity-related information) that should be protected. The solution should also enable lexical analysis and dictionaries/lists for words or formats relating to company-specific sensitive information (e.g., intellectual property (IP), financial information).

- A policy-based management is needed to setup and enforce granular rules per specific user or per user group (e.g. sales, marketing, R&D, finance, legal).

- The ability to set up compliancy lists for PCI, HIPAA, GLBA, SOX, CISP, FISMA, governmental regulations, etc. is needed, especially for publicly-traded companies, financial institutions, and healthcare providers.

Numerous enterprises are now looking for DLP as an integral part of their web security solution rather than dedicated DLP solutions which are available as a stand-alone solution. This enables administrators to turn specific features on and off, deploy security features in stages and even disable superfluous functions. This type of integrated DLP solution prevents intentional (as a result of malicious activity) and unintentional data leakage with low cost of ownership.

Heartland Hacker Charged for Massive Attack on U.S. Retail and Banking Networks

Albert Gonzalez, 28, of Miami, has been indicted for conspiring to hack into computer networks supporting major American retail and financial organisations, and stealing data relating to more than 130 million credit and debit cards, announced Assistant Attorney General of the Criminal Division Lanny A. Breuer.

In a two-count indictment alleging conspiracy and conspiracy to engage in wire fraud, Gonzalez, AKA "segvec," "soupnazi" and "j4guar17," is charged, along with two unnamed co-conspirators, with using a common hacking technique called "SQL injection".

 "The problem is 'SQL Injection'. If an SQL database cannot deal with escape characters (a single character designated to invoke an alternative interpretation on immediately subsequent characters in a character sequence) then it is vulnerable to the injection of variables and strings that will give hackers direct access to data. Hackers can extract data from a vulnerable database by simply heading onto the login page and entering an exact string of code. This string selects a particular user's password and potentially their credit card details. This occurs because the input into the form in the web page is unverified or unsanitised. Commented Neil O'Neil, a Certified Ethical Hacker.

Among the corporate victims named in the indictment are Heartland Payment Systems, a New Jersey-based card payment processor; 7-Eleven Inc., a Texas-based nationwide convenience store chain; and Hannaford Brothers Co. Inc., a Maine-based supermarket chain.

The indictment, which details the largest alleged credit and debit card data breach ever charged in the United States, alleges that beginning in October 2006, Gonzalez and his co-conspirators researched the credit and debit card systems used by their victims; devised a sophisticated attack to penetrate their networks and steal credit and debit card data; and then sent that data to computer servers they operated in California, Illinois, Latvia, the Netherlands and Ukraine. The indictment also alleges Gonzalez and his co-conspirators also used sophisticated hacker techniques to cover their tracks and to avoid detection by anti-virus software used by their victims.

If convicted, Gonzalez faces up to 20 years in prison on the wire fraud conspiracy charge and an additional five years in prison on the conspiracy charge, as well as a fine of $250,000 for each charge.

Gonzalez is currently in federal custody for his alleged role in the hacking of a computer network run by a national restaurant chain.

Gonzalez faces an additional series of indictments for a number of retail hacks affecting eight major retailers and involving the theft of data related to 40 million credit cards.

Cloud Computing will Increase the Risk Card Data Breaches

Reports that a major data breach at Network Solutions - potentially impacting more than 570,000 cardholders around the world - is almost certainly the result of cloud computing making such network hacks highly attractive, says Imperva, the data security specialist.

"Although the data breach appears to have been discovered in early June, here we in late July - six weeks later - reading about a breach affecting more than half a million cardholders, around half of the Internet service company's customer base," said Amichai Shulman, Imperva's chief technology officer.

"As the dust settles on this major data breach - which appears to be right up there alongside the Heartland Security card data breach of the start of the year - heads will undoubtedly roll," he added.

But, says the Imperva CTO, "the basic problem is that the rise of cloud computing - with many more companies now hosting their data on the Internet - makes such databases and the servers they are hosted on, phenomenally attractive. The attackers here aimed on the big prize -- the servers. Instead of dealing with a site here and there, once they broke into the hosting servers and all the sites were open to them. The lesson: once you've penetrated the cloud, you've got an easy path to the important, underlying data."

According to Shulman, as the newswires report yet another major card database hack, it is interesting to note that Network Solutions says that malware planted on its servers appears to be at the heart of the data loss.

"It is also worth noting that they actually knew of the breach on June 8 but took more than six weeks

14

to reveal the problem to the media and customers." "This case does not appear to have been handled well by the company and the delay in going public could prove expensive if, as seems likely, a class action lawsuit results from the data losses," he added.

Hackers Take a Break This Summer Before Winter Hacking Spike

Enjoy the rest of your summer vacation say the hacking community, as you're far less likely to be targeted now than during your Christmas and New Year vacation. That's according to the results released today by Tufin Technologies who have released the findings of its "Hacker Habits" survey conducted amongst 79 hackers at the annual gathering of hackers at Defcon 17 in Las Vegas this month. Eighty nine percent of hackers admitted that IT professionals taking a summer vacation would have little impact on their hacking activities, as a whopping 81% revealed they are far more active during the winter holidays with 56% citing Christmas as the best time to engage in corporate hacking and 25% naming New Years Eve.

"It's received knowledge in the security world that the Christmas and New Year season are popular with hackers targeting western countries," said Michael Hamelin, chief security architect, Tufin Technologies. "Hackers know this is when people relax and let their hair down, and many organizations run on a skeleton staff over the holiday period."

If you want to know when you should be most on your guard it's during weekday evenings with 52% stating that this is when they spend most of their time hacking.

Ninety six percent of hackers in the survey said it doesn't matter how many millions a company spends on its IT security systems, it's all a waste of time and money if the IT security administrators fail to configure and watch over their firewalls.

"This may be stating the obvious," said Hamelin, "but poorly configured firewalls remain a significant risk for many organisations. It's not the technology that's at fault, but rather the configuration and change control processes that are neglected or missing altogether. Best practice suggests you should test and review your firewall configuration regularly, but many organisations fail to do so."

New Measures To Cut Off UK File Sharers Could Do More Harm Than Good

IT security and data protection firm Sophos reminds computer users and businesses of the importance of protecting internet connections and networks following news that the UK government will propose new laws to suspend internet connections where illegal file-sharing is suspected.

The new proposals will mean that home or business users suspected of illegal downloading will still receive warning letters from ISPs, but if they are believed to be continuing to share copyrighted material, internet connections will temporarily be suspended - a measure that was initially rejected by the British government's Digital Britain report earlier this year as a step too far.

The penalties, thought to have been pushed through by business secretary Peter Mandelson, are likely to cause serious problems for both ISPs and users of Wi-Fi networks. Customers who are about to be cut off from the internet could claim that other computer users have been illegally using their internet connection - piggybacking - to download and share copyrighted material.

"Worryingly for businesses, if the alleged illegal downloads appear to originate from the workplace - will the entire company be disconnected from the net?," said Graham Cluley, senior technology consultant at Sophos. "The bottom line is that people who illegally download material that they haven't paid for aren't going to have any qualms about using someone else's internet connection. This not only means there are likely to be innocent victims, but it also gives the real pirates a plausible defence. These proposed laws to stop illegal file-sharing are not only unworkable, they're ridiculous."

U.S. Department of Justice Approves Oracle Acquisition of Sun

Oracle Corporation this month announced that the U.S. Department of Justice has approved Oracle's proposed acquisition of Sun Microsystems and terminated the waiting period under the Hart-Scott-Rodino Act.

Sun's stockholders approved the transaction on July 16, 2009. Closing of the transaction is subject to certain conditions, including clearance by the European Commission.

15

Industry's First Full-Face Foil Contactless Payment Card achieves Visa Certification

Perfect Plastic Printing, this month introduced the industry's first full-face foil PVC card certified by Visa Inc. for contactless payment transactions.

More than one year in development, the card enables card issuers to now provide contactless payment cards with the same high aesthetic appeal of foil as their traditional cards, and opens the door for contactless technology to a significant portion of the overall market. This card product is based upon MicroPass 4003 and an innovative antenna design from INSIDE Contactless.

Foil cards have attractive metalized foil applied across the entire face of the card, offering a mirror-like reflection unattainable with printing ink alone, and have carved out a significant portion of the premium-level card market because of their high aesthetic appeal. But getting contactless technology to work with these foil cards has been a huge technical challenge because the metal foil layer ordinarily blocks the radio signals contactless cards rely on to perform transactions.

"The challenge in developing this revolutionary product was to find the right balance between having enough metal content in the foil layer to provide the desired appearance but not so much that it interferes with the radio signals," said Matt Smoczynski, vice president of Perfect Plastic Printing. "We worked closely with INSIDE Contactless to create this breakthrough, designing a solution and developing the technologies required to produce a contactless foil card that meets the required industry certifications while maintaining the card's striking visual effect."

One in Five Hit by Card Fraud in Past Five Years

ACI Worldwide, Inc. announced that its global card fraud survey revealed that 18 per cent of consumers questioned have been victims of credit or debit card fraud in the past five years. The research, of more than 2,400 consumers across eight countries, also

found that if an individual or someone they knew was hit by card fraud, 22 per cent would change financial institutions, and a further 27 per cent would consider changing financial institutions.

In the light of these findings, ACI Worldwide has launched its Guide to "Stopping Card Fraud in its Tracks", with contributions from Nationwide Building Society, to provide advice to fraud managers in banks to help combat card fraud and protect their customers.

The survey highlights some wide variations in fraud trends around the world. In the US and UK, 27 per cent of respondents have been hit by card fraud in the past five years, compared to only seven per cent in Dubai, eight per cent in Germany and 15 per cent in Australia, China and Singapore. When it comes to customer attitudes to card fraud, a fifth of the respondents said they are not confident their financial institution can protect them, with this number rising to over a third in China.

Pete Corrie, head of financial crime at Nationwide Building Society, comments: "The number of card payments globally has increased drastically over the past few years and, consequently, the whole industry has seen associated fraud levels go up. The Guide produced by ACI Worldwide not only highlights that fraud detection and reduction is one area where financial institutions are able to take decisive and positive action to reduce losses but also explains how financial institutions will be able to protect their image and retain the trust of their customers."

David Nussenbaum, vice president and product line manager at ACI Worldwide, adds: "The international research we have conducted shows that although card fraud trends vary around the world, it is still a persistent problem for banks. In order to protect themselves and their customers against potential fraudulent attacks, financial institutions are looking for ways to implement effective anti-fraud strategies."

The ACI Worldwide research on card fraud was conducted during July 2009 in Australia, Brazil, China, Dubai, Germany, Singapore, the UK and the USA surveying a total of 2,408 respondents.

SHAZAM Network to Pilot Internet PIN Debit Technology

SHAZAM an interbank network providing electronic funds transfer services to more than 1600 financial institutions in 29 US states, has agreed to test Acculynk's PaySecure Internet PIN debit service. SHAZAM will conduct a pilot program where interested SHAZAM financial institutions can

16

participate in testing the latest in Internet PIN debit technology. The pilot program will help gauge consumer acceptance of using a debit card with a PIN when making online purchases.

With the PaySecure software, consumers enter their PIN on a graphical PIN-pad at the merchant checkout, and only need their existing debit card and PIN to complete the transaction. There are no hardware devices, passwords, enrolment, or redirection to another website for payment.

"PaySecure is one of those rare emerging payment methods that satisfy the needs of consumers, merchants, and financial institutions," said Ashish Bahl, CEO of Acculynk. "PaySecure helps issuers retain and grow their debit revenue stream, merchants decrease transaction processing expenses, and consumers reduce signature-based debit card fraud. We are pleased that SHAZAM recognises the value PaySecure brings and has chosen to pilot our service."

easycash buys the German POS acquiring business of RBS WorldPay

Payment service provider easycash has bought the German merchant Point of Sale (POS) portfolio of RBS WorldPay GmbH, the German domestic acquiring arm of the Royal Bank of Scotland. The portfolio consists of several thousand merchant relationships. Through this acquisition, easycash actively enters into the credit card acquiring market and completes its choice of products in this area with a full offering of credit and debit card acquiring services. The purchase agreement was signed on June 22, 2009. The parties involved have agreed not to disclose the purchase price.

The purchase of RBS WorldPay GmbH's German POS acquiring business will enable easycash to offer merchants credit card acceptance for MasterCard and VISA as well in future. The recent granting of the acquiring licences from MasterCard and VISA to easycash was the pre-requisite for this acquisition.

Subscriptions to DOCOMO's Credit Payment Service Top 10 million

NTT DOCOMO, INC. subscriber base topped 10 million in Japan on August 24.

Launched in April 2006, DCMX reached 1 million subscribers in November 2006, 5 million in February 2008 and 10 million, just three years and four months since the original launch.

DCMX is a service brand for DOCOMO-issued credit cards, which allows subscribers to make

purchases using their mobile phones as credit cards via iD(tm), DOCOMO's branded mobile payment platform for handsets equipped with contactless IC cards (Osaifu-Keitai(tm)). For security, DOCOMO's Osaifu-Keitai phones can be locked remotely over the wireless network if misplaced or stolen.

The rapid penetration of DCMX was helped by the popularisation of Osaifu-Keitai and iD reader/writer terminals as well as its customer loyalty program. Currently, over 30 million DOCOMO customers use Osaifu-Keitai-compatible handsets and about 60% of all DOCOMO customers are using Osaifu-Keitai services. As of July 31, 2009, there were approximately 420,000 iD readers/writers nationwide. iD is now used in various settings in daily life, such as shopping at convenience stores and electronics retailers, eating at fast food restaurants and taking taxis.

There are three plans offered under the DCMX brand: "DCMX mini" with which payments within a monthly credit line of 10,000 yen (approximately 104.7 U.S. dollars) will be billed together with the user's monthly DOCOMO phone charges, the standard "DCMX" plan and the premium "DCMX GOLD" plan.

Oberthur Technologies is the first Smart Card supplier to obtain CUP (China Union Pay)

Oberthur Technologies, announced the successful completion of CUP (China Union Pay) certification for its Shenzhen manufacturing centre in China.

The Oberthur Technologies Shenzhen manufacturing site is already providing several hundred million SIM cards globally for the Telecom industry, and is now supplying magnetic stripe and EMV cards to banking customers in China and throughout the Asia Pacific region.

Already certified by Visa, MasterCard and Amex, as a response to the steady growth of the EMV market in Asia, the Oberthur Technologies Shenzhen production unit is increasing the scope of its operations with this successful certification payment scheme standard.

The completion of CUP certification makes Oberthur Technologies the first major smart card vendor in China to be certified for all 4 schemes for magnetic stripe, contact and dual interface cards.

Founded in March 2002, The China UnionPay Network now links ATMs of some fourteen major banks and many more smaller banks throughout mainland China.

17

Card Technology Today
By William Lorenz, COO, EntroPay

William Lorenz

In March 2007 Peter Ayliffe, the now president and CEO of Visa Europe, stated that paying for goods with notes and coins could be consigned to history within five years. Despite being widely dismissed at the time he asserted that using credit and debit cards would become cheaper and more convenient than cash by 2012. Whilst in reality the demise of physical cash isn't going to happen in the immediate future, the technology involved in making cash free payments has advanced significantly, bringing the prospect of a cashless society ever closer.

The demise of cash

It is well known that traditional payment methods including cash and cheques are increasingly seen as cumbersome, insecure to carry in large amounts and not always available when needed. APACS figures, released in February 2009, highlighted the consumer preference for card payments with the number of card payments growing by 7.4% and 6.8% by value in 2008 against the previous year. The use of debit cards also increased to 73.5% from 71.7% in 2007. This move away from cash to electronic transactions has been further intensified as more remote payments take place.

In the electronic world, despite widely voiced concerns over the 'big brother' implications of electronic transactions, the trade-off between convenience and privacy is increasingly being won by convenience. A prime example of where convenience has won over privacy is the contactless 'cash-replacement' cards that have been eagerly adopted for transport worldwide. The Transport for London contactless Oyster card has seen unprecedented adoption by commuters, even though such cards allow their movements to be tracked. Similarly electronic money is a faster and more secure way of making payments in comparison to cheques sent through the post, particularly for cross border payments.

A call to action

From a retailers point of view cash-handling is not without cost, especially for large firms, with labour-intensive infrastructures in place to collect and account for money from the tills and deliver the cash to safe deposit. Likewise there are several obstacles for retailers associated with electronic payments. Most obvious is that the pricing for card transactions tends to include a fixed charge (irrespective of the amount) and often a variable charge (a percentage of the amount), which particularly penalises low-value payments. As on the consumer side, the strengthened control and security associated with electronic payments creates a strong call to action for retailers.

Ultimately payment is a two-sided market, requiring both payers and payees to adopt common standards. Implementation of a new payment method by consumers will only take place if enough merchants accept that form of payment, and vice-versa. Likewise, retail banks and payment institutions need to ensure that the payment methods they offer are up to speed, in such a fast moving environment innovation and expansion of products will arguably hold the key to their electronic success.

With credit and debit cards now widely accepted for electronic payment, the introduction of contactless and prepaid technology signifies further change on the horizon. However, this does not necessarily mean upheaval for existing infrastructures as new payments methods can often piggy-back existing standards. An example of this are open-loop (VISA/MasterCard) prepaid cards that work with existing bank card infrastructures, resulting in less upheaval for all concerned.

Prepaid comes to the fore

Prepaid cards in particular signify the next step change of innovation that will further reduce the dominion of traditional payment methods. Amongst the additional benefits of prepaid cards is the ability for them to be made available to almost anyone. This includes various segments of society that have been traditionally confined to cash, for example those who are under age or unable to open a regular credit or debit bank account.

In the UK, it is estimated that some two-thirds (63%, according to Equifax) of credit card applications are declined. While a proportion of these certainly represent unacceptable risk, it is likely that many of them could be served with other payment options such as prepaid accounts. Alongside this, within relatively modest limits, prepaid cards can be anonymous and can therefore offer some of the privacy benefits of cash which contactless and traditional card payments lack.

18

Another facet of prepaid cards is the fit with e-commerce. As the online market continues to grow, virtual prepay enables not only consumers but also businesses to avoid the costs traditionally associated with plastic cards and distribution. For example, consumers can cost-effectively send payments to businesses around the world, whilst also benefiting from protection against ID theft and fraud, which have become a cause for concern for many when purchasing online.

Virtual prepaid solutions also offer a highly secure alternative to credit or debit cards for banks. Currently, UK banks are liable to cover any losses to a customer's bank account which are a direct result of fraudulent activity. Especially rife in the online arena, losses from debit or credit cards can be substantial. By adopting prepaid, this risk exposure can be lessened, posing an attractive prospect for banks in today's market environment.

Establishing common standards

In order to realise the full potential of prepaid, the retail banking industry needs to set common industry standards which all can adhere to. With reputations at stake, banks must first address the risks and help build an industry standard that will ensure integrity throughout the prepaid sector.

First and foremost is the proactive management of fraud. The current unstable economic climate, coupled with the proliferation of stories about data losses, has led to growing consumer concern about the safety of their personal data and money. Managed appropriately prepaid solutions can help eliminate this fear by removing the opportunity for identity theft.

Second is to ensure the safety of customer funds. For prepaid, this means providing an equivalent of the government deposit guarantee to provide peace of mind to customers in terms of securing the funds loaded into their prepaid account. This should involve the separation and ring-fencing of their funds for protection purposes.

Finally, banks must provide clarity of terms to their customers. In particular, banks must have a full disclosure policy in terms of their prepaid fees in order to maintain customer trust in what is perceived to be a new banking innovation.

Regulators encourage innovation

Alongside consumer demand, regulations are also driving the need for greater innovation in the banking sector where in the current economic environment banks are forced to employ lower risk strategies. An example of this is the Payments Services Directive (PSD), which has been specifically designed to increase the number of competing financial institutions. This heightened competition will in turn drive the need for retail banks to adopt innovative solutions to stay ahead of their competitors and, in so doing, position themselves for market recovery.

The PSD, due to come into effect in November 2009, will significantly change the retail banking landscape, opening up new routes for institutions to become entities licensed to handle customer funds and be members of VISA and MasterCard. In line with this, over the next two years, the European Commission aims to treble the number of Electronic Money Institutions – one of the categories of competitors to the incumbent banks.

As the PSD looks to encourage more players into the payment sector, competition for the retail customer is on the increase. In addition, the Single Euro Payments Area (SEPA) is opening up the payment market across Europe. With SWIFT catering to higher value payments, typically over £1,000, virtual prepay in particular will enable banks to maximise the potential of smaller payments and therefore act as a complement to their existing business models.

While innovation is required to meet these fresh challenges, banks must, in parallel, keep in mind their reputational risk, particularly in today's cautious climate. Therefore, the most appropriate business models to select are those that have already achieved proven success and that are ripe for further development. As previously touched upon, the prepaid industry, when compared with other elements of banks' card businesses, is relatively young. Yet as the market continues to mature, it offers a number of opportunities to achieve growth, increase customer acquisition and sustain a competitive advantage.

To conclude

With credit and debit cards now firmly established, the prospect of a cashless society is becoming further realised through the adoption of contactless and prepaid for electronic payments. In addition the competition between retail banks and Payment Institutions is set to intensify as the international landscape for electronic money, particularly in e-commerce, is set to become a veritable battleground. Prepaid in particular is an attractive prospect as it has the advantage of delivering a service to new consumer segments as well as addressing fears over fraud and privacy especially in the virtual word. Whilst it would be naïve to anticipate an absolute electronic payment environment in the near future innovation in this area will seize the long term advantage.

19