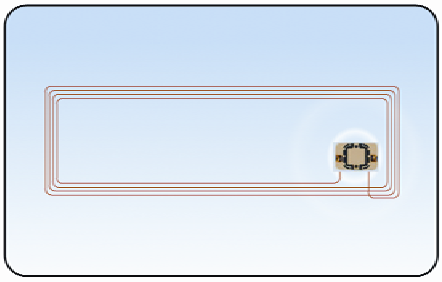
March 2009

Volume 18 • Number 3

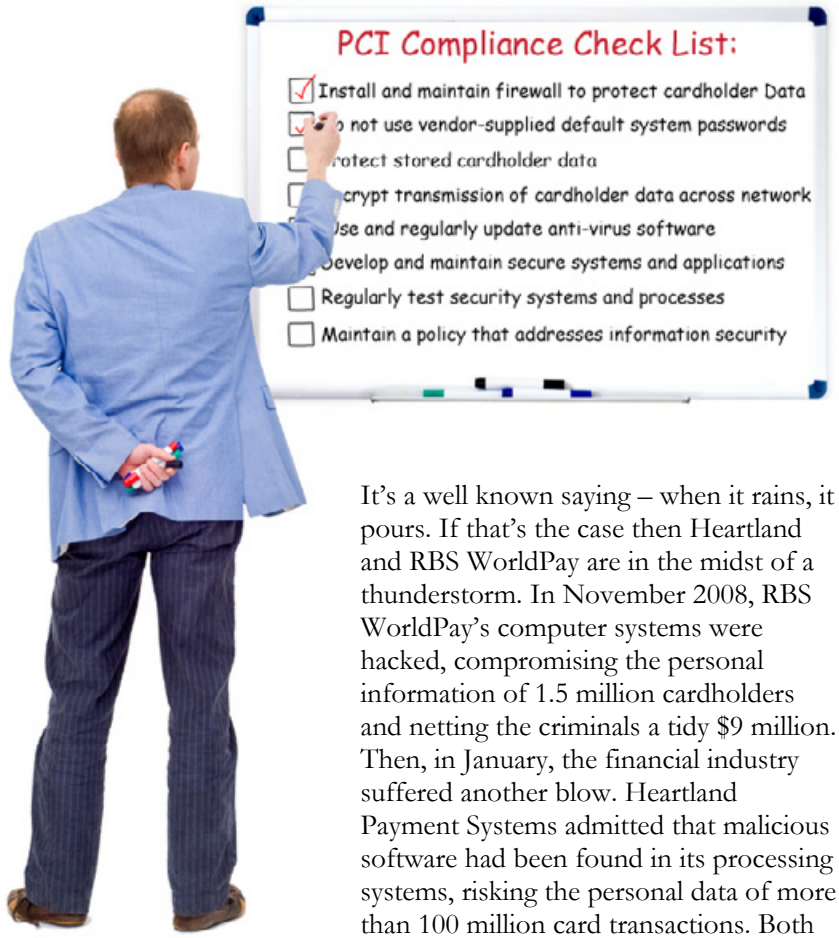
Smart Card & Identity News

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

www.smartcard.co.uk



Visa Condemns Hacked Payment Processors



It's a well known saying – when it rains, it pours. If that's the case then Heartland and RBS WorldPay are in the midst of a thunderstorm. In November 2008, RBS WorldPay's computer systems were hacked, compromising the personal information of 1.5 million cardholders and netting the criminals a tidy $9 million. Then, in January, the financial industry suffered another blow. Heartland Payment Systems admitted that malicious software had been found in its processing systems, risking the personal data of more than 100 million card transactions. Both companies probably couldn't have imagined the situation could get any worse, but the news that both have been removed from Visa's list of Payment Card Industry Data Security Standard (PCI DSS) could prove the final nail in the coffin.

Heartland is under siege from all sides. Currently undergoing investigation from the US Department of Justice, the SEC, the Federal Trade Commission, the Office of the Controller of Currency, as well as

Continued on page 4….

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 - Lesley Dann, John Owen

Contributors to this Issue – Tom Tainton, Peter Tomlinson, Luther Martin, David Hobson.

Printers – Hastings Printing Company Limited, UK

ISSN – 1755-1021

Disclaimer

Our Comments

Patsy Everett

Dear Subscribers

Data loss heads the news again this month. Heartland and WorldPay have both been removed from Visa's list of PCI-DSS compliant companies. The trouble is that the poor old consumer is now getting totally confused, well I am anyway. Both these companies have been certified as complying with the PCI Data Security Standard, isn't that meant to offer re-assurance that these losses of credit card data won't happen? If two of the biggest players have passed certification but failed to avert large scale attacks then isn't there something wrong with the system?

Now the problem may get worse, the credibility of the banks has been obliterated over the last 6 months, consumers do not trust banks anymore and we are now even getting vigilantes attacking the property of some of the offenders as on Fred Goodwin's house this week. Fortunately he wasn't home at the time. So far Visa, Mastercard and other major payment organisations have stayed under the radar but perhaps these losses of data will have bigger repercussions than anybody has so far imagined.

It gets worse, we have reports this month that credit/debit card fraud is on the increase but Chip & PIN was supposed to stop all that, who is to blame, why is it all going wrong?

Well here is the common thread, people are involved and how well do we really understand human behaviour? Some times the problems are easy but when we get around to Ross Anderson and his concerns about government data bases it all starts to get a bit more difficult.

First let's look at Chip & PIN, is it really as secure as the specialist tell us? Here I have insider information and I'm told (more than my life's worth to argue!) that the core security mechanisms of Chip & PIN are more than fit for purpose, it's all a matter of how it's implemented. The problem is nothing to do with the security of the smart cards per se but more about how they are used. Apparently the banks are primarily using the lower security SDA mode of operation which relies on an on-line connection for security authentication/authorisation. In off-line mode it can be fooled.

But it's really much worse than that, the smart cards still have a magnetic stripe and the contents of the magnetic stripe stored in the chip. If a crook can gain access to your card and see you enter your PIN then he can easily create a magnetic stripe counterfeit that will work anywhere that a magnetic stripe card is accepted. And where is that? Well lots of places in the East and also North America, home of Visa and Mastercard. Something about fraud migration comes to mind here.

You just try arguing with a bank over a withdrawal from your account, they start with the assumption that you are wrong and the onus is for you to prove that you didn't make the payment or withdrawal. Yes, note the word withdrawal the crooks could be

emptying your bank account if it was a debit card that was attacked. You have to say that at the moment I'd rather not use a debit card at all because this is a big risk. Which would you rather do, Have an argument with the bank over payments made on your credit card or trying to get back the money fraudulently removed from your debit card account?

Ross Anderson was on the TV this month talking about the government setting up and handling of (unnecessary?) data bases that affect citizen privacy. I find myself starting to agree with him, if major corporations can't get it right then what hope do we have with government departments or the major consulting houses that so prominently have gone round losing memory sticks and laptops containing very sensitive information.

I agree with Ross, it can only get worse!

Patsy.

Contents

Events Diary

April 2009

20-24	RSA Conference 2009, San Francisco, USA - www.rsaconference.com
21-24	SIMposium 2009, Wienna, Austria – www.simalliance.org
21-24	Card Asia 2009, Singapore - www.terrapinn.com/2009/cardsasia/
22-24	WiMA 3rd NFC Business & Technical Developers, Monaco - www.wima-nfc.com
28-30	Infosecurity Europe 2009, London, UK - www.infosec.co.uk
29	UK Gift Card & Voucher Conference, London, UK www.ukgcva.co.uk/conference2009/

May 2009

3-5	Digital Identity Assurance 2009, Dubai, U.A.E - http://digital-idassurance.com
6-8	Payment China 2009, China – www.globaleaders.com/en/2009/payment/
5-6	MMT (Mobile Money Transfer) Africa - www.mobile-money-transfer.com/africa/
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

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

…. Continued from page 1

several states, the beleaguered company also faces sixteen class-action law suits filed by ticked-off consumers, and four lawsuits filed by financial institutions. Bad news for Heartland and bad news for the financial sector, where consumer confidence is already at rock-bottom as a result of the crippling state of the global economy. The loss of PCI DSS accreditation is just as concerning, and Heartland and RBS WorldPay will certainly remember the demise of CardSystems Solutions in similar circumstances back in 2005.

The payments firm processed transactions for MasterCard and Visa, before misplacing more than 40 million card accounts. As a consequence of the breach, CardSystems was dropped by all major credit companies, eventually filing for bankruptcy in 2007 and closing its doors a year later. There's frightening similarity between the two cases. Both CardSystems and Heartlands were payment processors, both suffered hacking attacks, and both, at the time of the crime, were the largest breaches ever. Negative publicity from the breach has already resulted in increased merchant attrition, and Heartland could also lose the sponsorship of its primary banks and stock sales are plummeting. Interestingly enough, Heartland CEO Robert Carr sold his shares around the time that the breach was discovered, fuelling speculation that he was attempting to cash in before prices fell.

Heartland and RBS WorldPay are now considered to be 'on probation', and both will undergo PCI recertification and assessment for undisclosed fines as a result of the data breach. Heartland gained PCI accreditation in April 2008, and RBS WorldPay received compliance two months later in June. Neither company held PCI certification for longer than a year. But the fact that both were PCI DSS compliant providers when they suffered security breaches has raised questions over the validity of the PCI system, with companies only needing to shape up when the annual assessment comes around.

It's fair to say that PCI DSS has copped quite a bit of criticism from industry experts over the Heartland debacle. Many have been opposed to the standard from the outset, and data losses in organisations that is using PCI DSS as the framework for their security practices is certainly going to leave people questioning the purpose and overall benefits of the system. Of course, any standard that encourages better, safe practice is a good thing, but the company must also be equally committed to the ongoing impetus upon protection of data, a focus that sadly is lacking in many banking and e-finance institutions. Until data protection is higher on the agenda, there will always be a greater risk. The real question is: Had Heartland not been 'protected' by PCI DSS, could the effects have been even worse?

Tom Tainton

World News In Brief

Professor Johannes Feldmayer Leaves Infineon Supervisory Board

Professor Johannes Feldmayer at his own request stepped down from the Supervisory Board of Infineon Technologies AG.

Johannes has served on Infineon's Supervisory Board since January 25, 2005. Infineon thanks Feldmayer, a renowned industry authority and strategy expert, for his professionalism and competency in the execution of his duties as a member of the Supervisory Board.

NXP Launches Disposable MIFARE

NXP announced the latest IC in its MIFARE family of contactless identification technology, the MIFARE Ultralight C. The chip is the first of its kind introducing open standard 3DES cryptography for authentication of disposable ticketing solutions against fraud and cloning.

The MIFARE Ultralight C provides a replacement for conventional paper tickets. It facilitates an easy implementation into contactless applications for events, loyalty vouchers and limited use transportation tickets. MIFARE Ultralight C offers extended user memory, easy integration into existing MIFARE infrastructures and a range of additional security features previously unavailable on disposable tickets.

"The MIFARE Ultralight C significantly steps up security levels for disposable ticketing solutions and providing operators with a number of unique features against fraud and enables them to expand their service offering," said Henri Ardevol, general manager, automatic fare collection, NXP.

New Report Reveals Additional Details on the Real Cost of Fraud to Companies

Finjan Inc. said that a newly issued report from CyberSource - which clams to show that one in eight online UK firms are losing more than five per cent of their revenues to fraud - illustrates the phenomenal cost that card fraud is costing UK organisations.

"The UK edition of the CyberSource Online Fraud Report notes on the lack of co-ordination and government support in the fight against fraud. This all confirms our strategy that investing in anti-fraud IT security technology really is worth its weight in gold," he added.

According to Ben-Itzhak, in the absence of the report's recommendation of the creation of a centralised anti-fraud body to co-ordinate efforts across the financial and enforcement industries, it is clear that companies are largely on their own when it comes to planning an effective strategy to beat financial fraud.

For more on the CyberSource UK report: http://tinyurl.com/cwqtmj

Nominations Open for Smart Card Alliance 2009 OSCA Awards

The Smart Card Alliance will once again honour the companies and individuals who have significantly impacted and influenced the market for smart cards in North America with its prestigious "Outstanding Smart Card Achievement" (OSCA) awards.

The 2009 OSCA awards will be presented during the Smart Card Alliance 2009 Annual Conference held in conjunction with CTST 2009 - The Americas Conference on May 4 - 7, 2009 in New Orleans.

Nominations are open in three award categories - two for organisations and one for an individual.

- Outstanding Issuing Organisation Award.
- Outstanding Technology Organisation Award.
- Outstanding Individual Leadership Award.

A judging panel consisting of North American smart card industry suppliers, end-users and individuals from the analyst and media communities will review all qualified OSCA applications. They will select three finalists in each category based on the nominee's merits and qualifications as outlined in the applications and determine the award for 2009.

Bluehill ID Completes Acquisition of Assets of Syscan International

Bluehill ID AG announced that it has completed the acquisition of all of the assets of Canadian animal ID and tracking company Syscan International. Bluehill ID thus enters the animal ID market and expands its North America presence.

Syscan ID Inc. a wholly owned subsidiary of Bluehill ID based Montréal, Canada completed the acquisition. All of the former Syscan International employees and products have been transfer to the new company and Syscan ID is already in full operation.

Researchers Reverse Engineer Home Banking Reader

A number of UK banks are distributing hand-held card readers for authenticating customers, in the hope of stemming the soaring levels of online banking fraud. As the underlying protocol CAP is secret, we reverse-engineered the system and discovered a number of security vulnerabilities. Our results have been published as "Optimised to fail: Card readers for online banking", by Saar Drimer, Steven J. Murdoch, and Ross Anderson.

In the paper, presented at Financial Cryptography 2009, we discuss the consequences of CAP having been optimised to reduce both the costs to the bank and the amount of typing done by customers. While the principle of CAP two factor transaction authentication is sound, the flawed implementation in the UK puts customers at risk of fraud, or worse.

The research was carried out by reverse-engineering hand-held card readers from UK banks NatWest and Barclays. Cryptographic problems uncovered by the Cambridge team include "reusing authentication tokens, overloading data semantics, and failing to ensure freshness of responses".

When Chip & PIN was introduced for point-of-sale, the effective liability for fraud was shifted to customers. While the banking code says that customers are not liable unless they were negligent, it is up to the bank to define negligence. In practice,

the mere fact that Chip & PIN was used is considered enough. Now that Chip & PIN is used for online banking, we may see a similar reduction of consumer protection.

Another problem highlighted within the report is that CAP readers may be used during mugging. Previously, muggers marched a victim to an ATM to ensure he gave them the right PIN. Now, with CAP, criminals have a portable device that will tell them if their victim is lying.

XIRING Posts Annual Results

XIRING has reported for the 2008 financial year, 20% organic growth in turnover, to €28.5m. For its part, operating income increased by over 60%, to €3.5m, and corresponds to a margin of 12.4% on turnover.

Georges Liberman, Chairman and CEO states: "I am particularly proud of XIRING's performance in 2008 as, yet again, we have fulfilled our commitments in terms of turnover and have even exceeded our profitability target. While the uncertain economic outlook leads us to be somewhat prudent in terms of our 2009 targets, it does not pose any threat to the pressing need to secure remote transactions or the prospects for development. XIRING benefits from technological, commercial and financial advantages to meet European market demand for online banking and e-commerce security, as well as demand from the healthcare markets."

XIRING hit its stated annual turnover growth target of 20% over the prior year, and achieved sales of €28.5m. Turnover from its Banking business was up by 24.2% compared with 2007 and reached €15.7m. Its Healthcare business achieved a 17.3% rise in turnover, to €10.9m. Accordingly, XIRING's turnover has increased more than two-fold in two years.

Aconite and Traderoot Partner to Strengthen Support to African Payments Market

Aconite has announced a partnership with Traderoot, a South African supplier of e-commerce transaction management solutions. Under the terms of the partnership, Traderoot will supply Aconite's EMV and Smart Product solutions to African institutions issuing chip-based payment products, in sectors such as banking, retail, transit and healthcare.

Traderoot is an e-commerce company providing companies with expertise and solutions for secure and reliable transacting in both the physical and virtual worlds. Through combining with Aconite, Traderoot will be positioned to offer card issuers a one-stop-shop for all aspects of secure card issuance, management, transaction verification and payment processing.

CardXX Announces New Patents

CardXX, Inc. has announced that it has been awarded patents in Singapore and Mexico for its proprietary encapsulation technology for the production of advanced smart cards, active RFID tags and other devices, and currently has over 30 patent applications pending in a number of other countries. CardXX's patent portfolio protecting the unique advantages of its RAMP Technology continues to expand.

Reaction Assisted Molded Process (RAMP) is used in the production of advanced powered Smart Cards, Active RFID tags, and other small form factor devices. RAMP enables the integration of electronic components such as batteries, data displays, keypads, chemical sensors, fingerprint sensors, and other elements.

NXP to Transfer its Mobile Services Business to Gemalto

Gemalto and NXP, have entered into an agreement whereby NXP would transfer its mobile services business to Gemalto. The related unit based in Sophia Antipolis, France will continue to develop and market software and service solutions compliant with the MIFARE4Mobile interface specifications which manage MIFARE-based applications in Near Field Communication (NFC) mobile devices.

MIFARE is the leading contactless technology globally, predominantly used within transportation networks, ticketing and access management applications. This strategic move by the two industry leaders aims to accelerate the global adoption of NFC technology in existing contactless infrastructures and further promotes the deployment of MIFARE.

Commenting on the transaction, Olivier Piou, CEO of Gemalto noted, "We believe that transportation will be a favourite application for NFC phones and will help spur adoption of the technology. ".

Adding this MIFARE4Mobile software further strengthens Gemalto's Trusted Service Manager (TSM) platform offer linking transport operators, banks and mobile phone operators enabling the

mobile phone to be used with existing payment and contactless ticketing infrastructure. The TSM notably makes the entire process of downloading tickets and subscriptions onto the cell phone more efficient and secure.

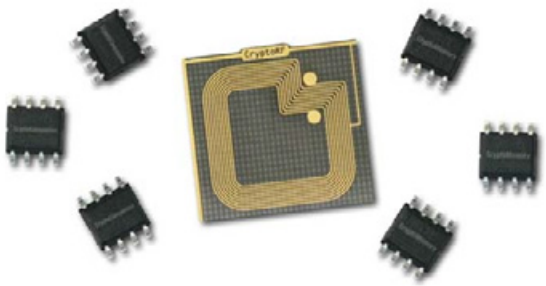
NXP will continue to invest in the development of industry-leading NFC chips fully compliant with current standards and interoperable with existing contactless infrastructure.

The specifications of the MIFARE4Mobile interface and the associated intellectual property will remain in the ownership of NXP who will ensure interoperability and full availability to all market players on terms released in December 2008.

The deal is subject to regulatory approvals and labour council consultations. The terms of the transaction, which is expected to close in Q2 2009, were not disclosed.

Atmel Offers Embedded System Protection with CryptoCompanion IC

Atmel Corporation, announced its next generation CryptoCompanion (AT88SC018) plug-and-play embedded security chip. CryptoCompanion provides designers an affordable option for cryptographic hardware security on systems that are currently prone to firmware theft and/or product counterfeiting. CryptoCompanion, when used in conjunction with Atmel's CryptoMemory chip, provides secure storage of the secrets necessary to authenticate consumable items or software IP. The combination of CryptoCompanion (host-side security) and CryptoMemory (client-side security) enables an embedded system security solution for less than a dollar in volume. An AVR-based demonstration kit, Aris+ (AT88SC-ADK2),is now available to show the capabilities of these two chips in an embedded environment.



CryptoCompanion provides host-side cryptographic security for embedded systems. Designers do not have to design or test the cryptographic algorithms. The companion chip implements the necessary algorithms and the entire protocol completely in hardware.

CryptoMemory for client-side security is the only family of EEPROMs with a 64-bit embedded hardware encryption engine, four sets of non-readable, 64-bit authentication keys and four sets of non-readable, 64-bit session encryption keys providing a low-cost, secure means of preventing product counterfeiting and/or piracy.

Until now, developers had to choose between high component costs or complicated development cycles in order to include hardware security in their embedded system designs. This combination of value and functionality sets a new benchmark for securing embedded systems.

Identification Technology Partners, Inc. announces its Architecture for a Smart Card Mutual Registration mechanism.

Identification Technology Partners, Inc. (IDTP) announced that it has developed a smart card application architecture referred to as Mutual Registration - Personal Identity Verification (MR-PIV).

The MR-PIV architecture was conceived by IDTP, to initially solve the challenges of managing interoperability and secure physical access control for the government Homeland Security Presidential Directive -12 Personal Identity Verification (PIV) smart card program.

MR-PIV provides an authentication mechanism for trusted communication between a smart card and a PACS reader by registering the reader to the smart card. MR-PIV can enable a single credential to be used in any number of PACS for secure entry, while supporting the local system operations, policies and secure access protocols of each.

For example, this enhanced capability allows a security officer to grant PACS privileges to an external PIV cardholder who can then use his/her PIV credential that was not issued internally, for managed local access.

When MR-PIV is applied to the system, this same scenario can occur for that cardholder in any number of locations where access privileges may be granted. IDTP is very active in the development of operational systems and readers for smart card identity credentials. MR-PIV answers a lot of issues for using secure credentials in today's PACS architectures.

What is the Future of ITSO?

By Peter Tomlinson, Iosis Associates

Peter Tomlinson

In this month of March there have been two significant UK conferences and exhibitions associated with smart media in the hands of the public. There is also in the background a running sore, lasting 10 months or 10 years, depending on your point of view: it is integrated ticketing and journey management and reporting for surface and sub-surface public transport.

9th to 11th March saw ID 09, exceedingly well hosted in the cavernous Royal Armouries in Leeds. Everything from bar codes through RFID to smart cards, plus applications in business systems and equipment, was represented. RFID manufacture and use, is primarily a business to business activity, in which there is a true and successful market, but the organisers for this event (the Halifax AIDC Centre www.aidc.org) also have a growing commitment to support for the smart card market and the use of smart media in the public sector and for privatised services to the public.

The 12th featured the ITSO Customer Media Alternatives Conference, with over 150 delegates. It was held in the portentous Porchester Hall in London's Bayswater, and turned out to be more of a really useful networking opportunity than a clear view ahead. Many Local Authorities need a clear view down a negotiable road, now that ITSO Ltd has decided to start on phasing out the Mifare® Classic platform that so many of them use. The key application area so far is mainly bus passes (English National Concessionary Travel Scheme, ENCTS) plus a small number of paid tickets, but rail season tickets and also local citizen service functions are slowly adopting smart cards.

ID 09

The Royal Armouries features prominently in the attractively restored Clarence Dock canal basin area of Leeds (#28 bus terminus). That is an area that 50 years ago us kids in Leeds never went near, but is now totally transformed. As a conference and exhibition venue, although labyrinthine, the Armouries deliver to a very high standard, with separate spaces for exhibition and refreshment, and the best of lecture theatre provision. The broad spread of subject matter at this conference put the spaces to good use, with both exhibition area and theatre busy throughout the conference sessions – but a major reason for smart card people to be there was to discuss a major expansion project being formulated by and with the organisers, the AIDC Centre team: can we, should we, all collaborate in developing a UK ITSO ticketing technology support service? The answer was an emphatic 'Yes'.

AIDC Centre

AIDC, a not-for-profit organisation based in Halifax and with facilities also in Sheffield, is the European Centre of Excellence for Automatic Identification and Data Capture, now firmly established as one of the world's leading bodies in AIDC technology. The Centre has a mission to encourage UK industry, commerce and services to become world-leaders in such technologies as barcoding, RFID, smartcards and biometrics. It is supported by Yorkshire Forward, the regional development agency, and states that it has been described as "leading the world as the first totally independent Centre devoted to the whole range of AIDC technologies." In association with LASSeO (Local Authority Smartcard Standards eOrganisation), the Centre has developed an independent standards testing facility where local authorities and suppliers can have multi application smartcards tested for compliance with the LASSeO specification. Plans are in hand for the Centre to develop a similar service for transport ticketing applications using the ITSO Environment: functional testing, and pre-certification testing, in collaboration with key industry ITSO Members. Already AIDC provides, at its Sheffield site, management services for the Sheffield citizen service smart card scheme. This area of technology is predicted to become increasingly important as user demand for applications working across authority boundaries increases.

The Centre aims to help businesses and public sector organisations discover the information that they need in a variety of ways: through targeted seminars and training and by visiting the Centre and its state-of-the art technology demonstrator area – the only one of its kind in Europe. Here visitors see and use the technology in inspiring application areas covering logistics, manufacturing, the food supply chain, health and well being, local

authority/utilities, sport and leisure, travel, library, a classroom for the future and financial services. The target of the demonstrators is to show the AIDC technologies in context and to inspire, inform and involve visitors through interactive use of equipment. As a recent visitor, I can testify to the range and quality of the facilities, and to the commitment to continue to add new application area demonstrators.

The Centre also runs a Business Assist Programme to provide free information and consultation – plus grant aid for implementation. That Programme is now creating interest in other parts of the UK and Europe.

The Centre has recently expanded its Membership Scheme so that more individuals, technology user companies, public sector organisations, associations and solution providers can take advantage of the benefits membership can bring. These include access to new technologies, business information and partnership projects, as well as use of hot desks and Members' Suite, use of meeting rooms, free use of event facilities, and discounts on seminars, training, tailored events and educational reports. Anybody wishing to find out more about the Centre and its support services, or to contribute to the development of the smart card and equipment test facilities, can contact Peter Collins on 01422 399499 or by email at peter.collins@aidc.org.

ITSO Customer Media Alternatives

Both the relevant, substantive presentations and the provided ITSO Customer Media Handbook, proved to be actual supplier-provided information, or material strongly influenced by suppliers. Thus we received a fulsome portrayal of the situation now, but to the over 50% local authority and related participants (who are currently, directly or indirectly, the major users of the ITSO Environment), this was of lesser importance than that all important roadmap for the next few years. Suppliers are also more than a little concerned…

The sore point…

…is the ten year failure (and it is a public sector failure) to bring about anywhere near enough improvement in the passenger experience of public transport. Of course we have a unique demography, so that we cannot import ready-made solutions, and indeed our best is equal to the best of the rest, but for ten years there has been a policy for significant improvement: "We need a new approach, bringing together the public and private sectors in a partnership which benefits everyone." (A new deal for transport: better for everyone – white paper, 1998, Cm 3950)

The ten month grief has been two studies by the Department for Transport into ticketing, journey management, and reporting, for surface and sub-surface public transport, using smart media technology. One study is into a strategy for ticketing, the other is into the commercial (and, it turns out, organisational) future of ITSO Ltd. Not happening in public (the studies, that is) is the sore point. But we hear things.

There is reported to be a positive case (when the public good is included) for a full rollout of smart media ticketing. This would provide interoperability and inter-changeability across a whole set of ITSO Licensed schemes, an upgraded Oyster scheme, and possibly a small number of other super-efficient schemes in metropolitan areas. The case is, however, predicated on near 100% deployment – and it predicts a positive cost benefit for the service operators.

Not in there is positive regulation of the whole outcome of public transport. Not in there is Information Assurance, that combination of service quality and information security that is a Cabinet Office policy created over 5 years ago but never let out of the cabinet. Not in there is incorporation of smart media ticketing support into the Critical National Infrastructure on grounds of promoting wellbeing and keeping people moving in the event of a national emergency. Not in there is safeguarding ITSO Ltd (albeit under the gaze of the regulator) as a development and support organisation with Members from all quarters.

What is here, now, is a new willingness at the top to let good ideas come through. The 2007 rail white paper needed challenging, and challenges have not only come forward but have brought results. For example, electrification of more rail routes is back on the agenda, not just major routes but also important in-fills across the existing network. And High Speed Rail is being encouraged with the formation of a new development company. That new approach is not (yet) much seen in the DfT ticketing studies. Better regulation of public transport and better use of technology have been waiting in the wings for a long time.

Security through Obscurity

By Luther Martin, Solution Architect, Voltage Security.

Luther Martin

In an 1883 article in Journal des Sciences Militaires, Auguste Kerchoffs defined six principles that a secure communication system should follow. Despite the considerable changes in technology, these principles are still as valid today as they were in the nineteenth century. The second of these principles is widely known today as "Kerckhoffs' Principle," and is often stated as the rule that the strength of a cryptographic system should rely only on the secrecy of a cryptographic key. Kerckhoffs' original statement, however, was actually more general than this, and deserves revisiting by many users of security technologies.

Kerckhoffs stated his second principle as "Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi," which can be translated roughly as "It must not require secrecy, and can be used even if it falls into enemy hands." So even if hackers know everything about your system, if they don't have the cryptographic keys you use to encrypt, any data they manage to get will be useless to them because they won't be able to unscramble the encrypted information.

In a more general sense, a hacker should be able to know everything about your security systems and still be unable to defeat them unless he knows the secrets that you use to identify authorized users. Those secrets could be encryption keys, but they could just as easily be other secret information, like a password. So a good security architecture should always be created under the assumption that attackers will know everything about the architecture except secret authentication information. This certainly includes assuming that attackers know what they're attacking. So "security through obscurity" is bad, and has been known to be bad for 125 years.

This principle seems to have been forgotten by many corporate IT departments, who all too often require security vendors to agree to extremely draconian terms of secrecy as part of the terms and conditions of buying security products. This unnecessary secrecy clearly violates the tried-and-true principles that Kerckhoffs laid down in 1883, but it also causes considerable inefficiency in the information security market, which benefits neither security vendors nor their customers.

Many security products are what economists call "experience goods," those for which you can't easily tell their quality before you buy them, but for which the quality becomes obvious after they're consumed or used. You may not know in advance if an intrusion-detection system will be effective before you deploy it, for example, but you can easily look at the logs of a deployed system and see that it's working. Some are even "credence goods," those for which you generally can never tell their quality, even after they're used. Encryption may be an example of this, because it's essentially impossible for all but experts to tell strong encryption from very weak encryption due to the rare and specialized skills needed to analyze it.

Knowing the quality of goods before they're purchased is important to the efficient operation of a market, and uncertainty in this area can lead to bad things happening, and understanding the consequences of such uncertainty can be very important. It's so important, that economist George Akerloff was awarded the Nobel Prize in Economics in 2001 for his analysis of how such uncertainty can adversely affect markets, even driving high-quality products from the market and leaving only low-quality products at high prices as the only alternative for consumers if market forces are left unchecked.

Withholding information about what security products are used and the experiences that users have had with them is almost certainly a way to increase the uncertainty in quality that's associated with security products, so it's also probably a step towards the failed markets that Akerloff described, and it benefits everyone if the quality of products is freely known. Users of security products benefit because they will more easily be able to avoid low-quality products and avoid pitfalls with the products that they have already deployed. It's tougher on the vendors of security products, because exposing the weaknesses in their products will cause additional work, and they will be more motivated to create more robust products and to fix existing problems in their shipping products.

On the other hand, the gains from more information about the quality of products should also benefit the vendors, at least those who make robust products. A significant part of the cost of enterprise security

products is due to the long and expensive sales cycle that they require, and this cycle could almost certainly be reduced in both length and cost if more information was available to potential customers. If more information about the quality of security products was widely available, the cost of sales could be much lower, so the additional effort required to develop more robust products would probably be paid for through lower expenses that security vendors would experience.

So if you're one of those organizations that require security vendors to agree to complete secrecy about the fact that you've purchased and deployed their products, you should probably reconsider your policies in this area. In addition to ignoring best practices that have withstood 125 years of scrutiny, you are not really getting any additional security by doing this. And by restricting the flow of information about the quality of security products, you are contributing to a situation that makes things worse for both the producers and consumers of security technologies. Security through obscurity has never been a good idea, and it still isn't a good idea today.

World News In Brief

Paypal joins Globalplatform to Influence Smartcard Technology

PayPal has become the latest member of GlobalPlatform, the international specification body for smart card infrastructure. PayPal will bring its expertise to GlobalPlatform and contribute to the ongoing development of standards to ensure interoperability across the payments industry.

Joining as a Participating Member, PayPal will play an active role in GlobalPlatform's Card Committee and its various working groups. Representatives from PayPal will also have the opportunity to participate fully on the GlobalPlatform Advisory Council and within the organisation's Task Forces, including the important Mobile Task Force, sharing best practice and technical knowledge with other members.

Eric Duprat, General Manager at PayPal Mobile, comments: "Membership in GlobalPlatform is a logical step for PayPal. We recognise the value of sharing knowledge in a way that will benefit the industry as a whole through robust technical standards, greater interoperability and ultimately the wider adoption of online and mobile payments around the world."

Kevin Gillick, Executive Director of GlobalPlatform, adds: "The latest amendment to our Card Specifications aims to align GlobalPlatform smart card technology with web services. As such, we welcome PayPal as a world leader in web-enabled payments and look forward to its valued input".

Cryptomathic Files Suit against BSS, Norge for Patent Infringement

Cryptomathic announced that it has initiated litigation in the courts of Oslo, Norway against BBS AS for patent infringement.

Cryptomathic has alleged infringement of its patent in BBS' BankID products related to digital signatures and user authentication using a central server for key storage and signature generation. The patent-in-suit is one of Cryptomathic's fundamental patents used for securing e-banking and e-government transactions, and is a world-leading version of a mobile, secure electronic and digital signature, which cannot be repudiated.

In its complaint, Cryptomathic alleges that BBS has infringed and continues to infringe, contributes to and induces the infringement of Cryptomathic's patent by making, using, offering for sale and selling products and services without being licensed by Cryptomathic to do so. BSS's BankID solution is used by approximately 1.75 million end-users to authenticate themselves by having messages or content signed centrally on their behalf with individual private keys.

"We have invested heavily in secure, mobile signature solutions based on two-factor authentication which offer high security as well as ease and convenience to the end-user. Our approach is based on research and development carried out over many years, and we feel strongly that we deserve fair acknowledgement from companies and organisations using our patented technology," said Professor Peter Landrock, Executive Chairman of

the Board of Cryptomathic. "This core technology contributed to Cryptomathic earning a nomination as one of the 40 most innovative companies in the world at the World Economic Forum in Davos in 2003. We prefer to resolve such issues through commercial discussions without litigation but have so far been unsuccessful with BBS. Hence we are left with no alternative but to file suit."

Cryptomathic is represented by Grette, one of Norway's leading law firms with specialty in Intellectual Property and IT.

HSBC Paraguay Selects Vasco's DIGIPASS

VASCO Data Security International Inc. announced that HSBC Bank Paraguay secures both its retail and corporate customers with VASCO's DIGIPASS technology and VACMAN Controller authentication software.

HSBC Bank Paraguay is the first bank in Paraguay to offer both its retail and corporate online customers a strong two-factor authentication solution and is the only bank in Paraguay to roll out DIGIPASS 2-factor authentication devices for retail customers. DIGIPASS allows HSBC's customers to securely log on to the bank's e-banking application HSBC PC Banking to consult their account information make money transfers and manage their banking accounts from the comfort of their own home or office 24/7.

To protect their customers' accounts from unauthorised access, HSBC wanted to implement the highest security standard using best-of-breed solutions. Another important factor for a successful roll out was a high user acceptance. HSBC Paraguay turned to VASCO to implement a secure, straightforward and user-friendly authentication solution.

Infineon and Huawei Sign 68 million Purchase Agreement for Communication ICs

Infineon Technologies AG announced that it has signed a letter of intent for framework purchase agreement amounting 68 million US-dollars with Huawei Technologies of China. This deal, as an important part of the recent European procurement tour of the Chinese business delegation, is intended to supply end-to-end chip solutions to Huawei's wireline and wireless communication systems. Infineon will provide semiconductor solutions for Huawei in the area of Central Office solutions (CO), Customer Premise Equipment (CPE) and Mobile Phone Platforms.

Globalplatform Appoints New Device Committee Chair

GlobalPlatform, the international specification body for smart card infrastructure, has appointed Christophe Colas of Trusted Logic as the new Chair of its Device Committee.

Christophe Colas is currently Professional Services Manager in the Professional & Consumer Devices Business Unit at Trusted Logic. He is responsible for technical marketing and leads customer integrations of the company's wireless security middleware. Christophe's professional experience has always been related to multi-application smart card accepting devices such as payment terminals and wireless devices, and he has been actively involved in several consortia concerned with maintaining open standards for smart cards.

Kevin Gillick, Executive Director of GlobalPlatform, adds: "Christophe has been involved in GlobalPlatform since its inception ten years ago. His participation in the development of several software architectures including Visa Open Platform Terminal Framework - which has since transferred to GlobalPlatform - and his extensive knowledge of the smart card, EMV and security areas make him an outstanding candidate to direct the activities of the Device Committee. I'd also like to thank outgoing Chairman Laurent Coureau of France Telecom and look forward to his continuing participation within the organisation."

The aim of the GlobalPlatform Device Committee is to define an open architecture and software framework for single and multi-application card acceptance devices, enabling the rapid development and deployment of acceptance device applications from multiple service providers. It is one of three committees within GlobalPlatform that conducts technical activity and specification development through specific working groups. Alongside the organisation's Systems and Card Committees, it allows members to channel their expertise and knowledge into targeted work initiatives.

Phone Data makes 4.2 Million Brits Vulnerable to ID Theft

According to the findings of a survey by endpoint data protection security experts, Credant Technologies, 80% of phone users store information on their phones that could easily be

used to steal their identities. The research surveyed 600 commuters at London railway stations about their mobile phones, typical usage and the types of sensitive information stored on them. The results were horrifying: 16% have their bank account details saved on their mobile phones, 24% their pin numbers and passwords, 11% keep social security and inland revenue details, 10% store credit card information alarmingly, 40% naively fail to protect their devices with a password.

When you consider that 4 out of 10 people are not password protecting their devices, it makes many millions of users seriously exposed to the trappings of mobile phone criminals and opportunists who can use this information to clone someone's personal, or even corporate, life.

Steve Gold, Telecoms journalist and IT expert adds "People can be destroyed when their phone gets into the wrong hands - for example blackmail, abuse and threats, just by leaving it accessible without password protection. Imagine how easy it would be to assume or destroy the life of a colleague just by stealing their phone - if it was the company chairman's phone you could send emails from him announcing his resignation - a practical joke with serious consequences."

Sagem Sécurité and Hitachi combine Fingerprint and Vein Recognition

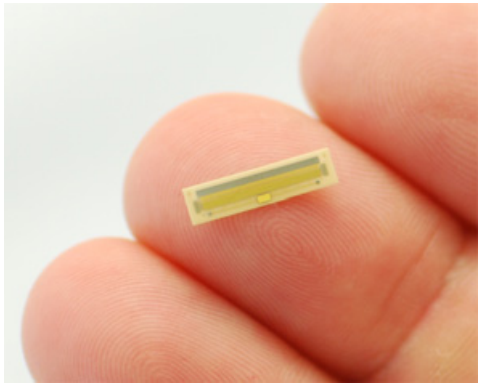
Sagem Sécurité is partnering with Hitachi, to develop a multimode biometric recognition module. Developed and produced by Sagem Sécurité, this module will combine the best of Hitachi's vein imaging technology (VeinID) and Sagem Sécurité's fingerprint identification technology (MORPHO).

The complementary nature of these two identification methods - recognition of the pattern of minute blood vessels under the skin, and simultaneously processing of fingerprint data - means that the module developed by Sagem Sécurité will offer levels of security and accuracy unrivalled worldwide. Designed to be easily integrated in any type of identification system, this module will meet requirements for a wide range of applications, including access control, identity checks and secure payments.

"By combining vein recognition with fingerprint analysis in a single, innovative module, we will be able to offer biometric equipment that boasts unrivalled security performance." said Jean-Paul Jainsky, Chairman and CEO of Sagem Sécurité. "Working with Hitachi as our partner also gives us the opportunity to develop our presence in the Asian biometric market."

"Our finger vein recognition is already widely used by Japanese banks to give customers easy, secure access to thousands of ATM machines," said Hideyuki Ariyasu, Managing Director of Hitachi Europe. "Combining this highly secure imaging technology with the world-class expertise of Sagem Sécurité, a leader in the security solutions market, provides an exciting opportunity to set a new authentication technology standard for goods and - even more importantly - to protect people's identities."

Biometrics Industry's Thinnest, Most Durable Fingerprint Sensor Announced



Sonavation, Inc., announced the introduction of the biometrics industry's thinnest, fingerprint sensor for the wireless and Smart Card markets. Called the SonicSlide STS3000, the sensor is about the thickness of a postage stamp, and is constructed from polymers similar to those used to build wings of commercial aircraft, giving it superior durability compared to fingerprint sensors available on the market today.

The SonicSlide STS3000 uses ultrasound comparable to that used in medical applications, resulting in significantly improved fingerprint imaging. Because it is not a semiconductor, the sensor eliminates the electrostatic discharge (ESD) issues that have hampered the incorporation of semiconductor-based sensors into notebook PCs, mobile phones and other consumer electronics. The SonicSlide STS3000 is capable of withstanding more than 10 million swipes, uses less power, enabling a set of applications that currently is not addressed within the commercial biometrics industry.

The fingerprint sensor module is an array of ceramics MEMS piezoelectric transducers and advanced polymers combined with a silicon-imaging

ASIC. All of these components are integrated into a single package about 35 mm in length by 14.5 mm wide with a thickness of only 0.25 mm. The sensing element alone is only 3 mm in length by 14 mm wide by 0.1 mm thick. The key imaging component of the sensor is the ceramic MEMS piezoelectric transducer array that is made from a ceramic material. This material is formed into pillars, each one-tenth the thickness of a human hair. The pillars have a unique set of properties that enable them to mechanically oscillate when an electric field is applied. The oscillations then register in 256 shades of gray to form the images of ridges and valleys of the fingerprint. This ensures a level of accuracy that cannot be achieved by most other swipe sensor technologies, including semiconductor-based sensors.

Study Claims 'Government Databases Breach Human Rights'

A report published by the Joseph Rowntree Reform Trust assesses on 46 databases across the major government departments, finds that:

"A quarter of the public-sector databases reviewed are almost certainly illegal under human rights or data protection law; they should be scrapped or substantially redesigned. More than half have significant problems with privacy or effectiveness and could fall foul of a legal challenge".

"Fewer than 15% of the public databases assessed in this report are effective, proportionate and necessary, with a proper legal basis for any privacy intrusions. Even so, some of them still have operational problems".

In his foreword of the report, Lord Shutt of Greetland, Chairman of the Joseph Rowntree Reform Trust said:

"Of the 46 databases assessed in this report only six are given the green light. That is, only six are found to have a proper legal basis for any privacy intrusions and are proportionate and necessary in a democratic society. Nearly twice as many are almost certainly illegal under human rights or data protection law and should be scrapped or substantially redesigned, while the remaining 29 databases have significant problems and should be subject to an independent review".

The Joseph Rowntree Reform Trust Ltd publishes the full report, Database State.
Available as a free download from www.jrrt.org.uk

ICO Takes Action Against Camden PCT for Data Blunder

The UK Information Commissioner's Office (ICO) has taken enforcement action against Camden Primary Care Trust (PCT) following a breach of the Data Protection Act.

Computers containing 2,500 individuals' names, addresses and medical diagnoses were left beside a skip inside the grounds of St. Pancras Hospital in August 2008. The computers, which were no longer in use and were not encrypted, were removed from the scene without authorisation and were never recovered.

The ICO has served Camden PCT with an Enforcement Notice for failing to take appropriate measures to safeguard the security of people's personal details.

Mick Gorrill, Assistant Information Commissioner at the ICO, said: "The ICO takes all data breaches seriously. Individuals must feel confident that their personal health records will be handled properly by NHS bodies. Over 2,500 individuals may have suffered anxiety as a result of this breach with the worry that their medical records could fall into the wrong hands This incident highlights organisational error and will no doubt damage public trust in the NHS locally.

"I am increasingly concerned about the way some NHS organisations dispose of sensitive patient information. Organisations need to ensure they implement appropriate safeguards to ensure personal details about patients are disposed of in compliance with the Data Protection Act."

Camden PCT is now required to ensure all personal information is removed from computer equipment as soon as it is decommissioned. The PCT has been ordered to update the ICO on progress made by 31 March 2009.

Failure to meet the terms of the Enforcement Notice would be a criminal offence and may lead to prosecution.

ID Cards for Belgium Children

Gemalto in March announced it is rolling out its eID solution as part of the Belgian government program to expand its national eID initiative. The program consists of a dedicated eID card for children aged under 12 with specific features intended to increase their security in emergency situations. In particular, a special hotline number is

printed on the card body of the child's ID card so that his parents can be alerted as soon as possible. Gemalto will deliver the highly secure microprocessor cards to Zetes, the European Auto-ID solutions provider. Fedict (FPS Information and Communication Technology), the Federal Public Service of Belgium in charge of developing e-Government projects, has just started deploying the Kids-ID program. This roll-out follows a decision from the Belgian government dated December 19, 2008.

The size of a credit card, the new Kids-ID card features three main functionalities. Firstly, it acts as an electronic National ID credential for Belgian children. Secondly in emergency situations the hotline number printed on the card body enables notification to the next of kin or friend, and lastly, the Kids-ID card can be used on the Internet for safer access to online chat, and for use of services that require identification. A built-in PIN code enables it to automatically authenticate the child and to grant them access to web services they are allowed to use.

MBTA's $15.4 Million Overrun on Fare Collection System due to Lax Oversight

State Auditor Joe DeNucci has reported that the Massachusetts Bay Transportation Authority (MBTA) incurred cost overruns of $15.4 million due to inadequate planning and oversight of the design of a $75 million'CharlieCard' automated fare collection system based on the broken Mifare Classic. In addition, delays in implementing the system cost the MBTA as much as $2.9 million in potential fare revenue. The project involved replacing the MBTA's aging mechanical fare collection system with automated equipment designed to provide better performance and reliability. It was also intended to increase revenues by reducing fare evasion and collection costs, and providing greater flexibility through "Smart Card" technology.

Between 2003 and 2008, the MBTA authorised $15.4 million in change orders due to design errors and improper planning and internal communication. This delayed the implementation of the system for one year, thereby losing the opportunity to earn approximately $2.9 million in revenue by eliminating virtually all fare evasions.

The MBTA placed itself at risk of $37.5 million by reducing the contractor's performance bond from 100% to 50% of the cost of the contract. The purpose of this bond was to guarantee that all the work would be completed in accordance with the contract requirements. The decision was questionable in view of the contractor's lack of experience in installing automated fare collection systems for large transit systems.

During 2008, the MBTA paid about $606,000 for repairs that would otherwise have been the responsibility of the contractor. This was due to the MBTA's decision to reduce the original one-year warranty period for about 1,200 fare boxes and leaving 400 fare boxes uncovered by the repair warranty.

"This is another example of a multi-million dollar project costing more than it should because there wasn't enough oversight," State Auditor Joe DeNucci said. "The taxpayers and the MBTA's riders are paying for that extra cost. In the future, the T management should provide more oversight of the design process and make sure that its contractors live up to their obligations."

Gemalto is selected by RBS Bank in Asia to Bootstrap EMV migration

Gemalto has been commissioned to carry out the migration to microprocessor EMV (Europay, MasterCard, VISA) credit cards for the Royal Bank of Scotland (RBS) across three markets in Asia: Indonesia, Taiwan and India. The first project commenced in October 2008 in Indonesia, with projects in Taiwan and India to follow, and involved the conversion of the Bank's traditional magnetic stripe cards to EMV cards. Gemalto provides RBS with a complete range of products and services including personalisation and project management.

The smooth project implementation resulted in a record turnaround time of three months, instead of a typical industry average in Asia of five to six months, translating into tangible operational savings for RBS.

Fraud reduction is the major driving force behind Asia's commitment to EMV migration. According to the Indonesian Credit Card Association, credit card fraud in the country amounted to 35 billion rupiah (approximately 2.3 million Euro) in 2007. Gemalto has already successfully completed the migration to EMV cards for 3 in 4 banks in Indonesia, well ahead of the 2010 migration mandate set by the Bank of Indonesia.

Into the Cloud we go.....have we thought about the security issues?

By David Hobson, Managing Director, Global Secure Systems

David Hobson

A new shift in computing is upon us – Cloud Computing. As our use of computing resources evolves from mainframes to PC's and networks we are now facing a major shift in the way we work. This could have dramatic effects on the way we use our computers, both for work or play. But the security issues need to be discussed, risk's assessed and judgements made knowing the risk's and issues. For some Cloud Computing makes a lot of business sense, for others, it may create confusion.

So what is Cloud Computing? For many it is the natural evolution of the Internet. The Internet has provided a major shift in the way we work. Less than 20 years ago, there was a comment, by Ray Noorda, the CEO of Novell, I think – "if you don't have an email address on your business card, you will be considered a nobody" , and most people did not believe it. 20 years later and it seems pretty much everybody has an email address, if not one at work, then a Hotmail, Gmail or Yahoo! account. And these email accounts are the first example of Cloud Computing!

Cloud Computing gets its name from network diagram's where the Internet is always shown as a cloud, as the route taken through the Internet can not normally be defined and is unknown. The route is irrelevant. The concept of Cloud Computing is that the central computer system, or systems are hosted in the Internet and their actual location is irrelevant to the application, and it's successful deployment. The architecture is relatively simple – a data store and server are hosted on the Internet, and the client can access the server from anywhere. Normally the client will have a web based front end, to make access even easier. The first major examples are the email services from Hotmail and the like's mentioned above.

The concepts of Cloud Computing have evolved to the concept being promoted today where there will be no need to purchase software, but it will be rented either on an annual basis or on a pay per use model. And now the model has added the concept of free use of software, in return for receiving adverts.

The major benefit of Cloud Computing for a user is financial. There is no need to invest in hardware infrastructure, or software. However there are a number of issues that need to be considered.

The old definition of security is as valid today as it ever was – CIA. Confidentiality, Integrity and Availability. And these three areas need to be addressed by any potential user of Cloud Computing. The major issue is confidentiality. If you are giving your data to a third party, you have no control over it. So who have you given it to? What is the access to the data? Who sees it? Can it be taken and used by someone else? Who administers this? What assurance do you have that your data is confidential? Are you happy with a contractual warranty? If so, what is your recourse if the contract is breached?

Are you convinced as to the integrity of your data? Can it be tampered with? If it was tampered with, would you know – most people would not. Are you satisfied with the segregation of data? What is the chance of "leakage" and how is this protected and tested?

And finally availability. If your data is not available to you, for whatever reason, then it is no good to you. Cloud Computing may actually provide much stronger back up and provision for disaster recovery than a private enterprise. Most solutions will provide at least one back up resource, maybe more. Any subscriber should check what provisions are made. However access is required to the Internet to access your data. If for any reason an ISP failed then all access fails with it. So redundancy in Internet access is a must. There are a number of products which offer offices small and large the ability to bind multiple ISP's to provide a virtual single access to the Internet. The other issue with availability that needs to be considered is the transfer of data. There are two major areas of concern. Firstly, one service offered in the Cloud is remote back up. If you need to get your data back from a remote data store, how long will it take to download everything in the event of an emergency? And when was this last tested. Almost certainly this will be a major issue, as the size of most people's Internet connection is relatively small compared to their LAN. The second issue is moving service providers. If you wish

to use a service like Salesforce.com for outsourced CRM, you may be limited to the data being stored in a proprietary format. If you were unhappy with the service and wanted to move to an alternative, how would you get your data back? And would it be useable?

In recent years, as well as CIA, three other areas are of major concern to business – Compliance, Policy, Risk. Compliance is now a major business issue. The data being stored in the Cloud must be considered carefully. What type of data is it? Is it confidential? Are there regulations to control how and where it is stored? In the UK we have the Data Protection Act which is very strict on data storage. If the data is being stored in the Cloud do you know where it is being stored? Are you breaking legal requirements? Your policies on data storage must address these legal issues, and any Cloud Computing must be considered very carefully.

And finally risk. We have spoken about concerns with the data and Confidentiality, Integrity and Availability – but what if your service provider goes bust? How would you get your data back? What if the ownership changes and their policies change?

One risk often not considered, is that by putting your data with a major provider, actually creates a bigger target for hacker's. If the service provider is hacked, or suffers some virus or security breach, how will your data be affected? Service providers have suffered already from hackers. Whilst they will argue they can invest more in security than many people, they are without a doubt a bigger prize. Some say there is much to be said for security by obscurity.

All these issues apply when outsourcing computing. Currently a lot of enterprises outsource their computing to save money. And the outsourcer is providing a private Cloud to give the relevant service. But all the questions we have raised apply equally, however the answers may be easier to get with an outsourcer and contracts can be drawn up to ensure compliance with your policies.

World News In Brief

ID Data Escapes Bankruptcy

After four months in Administration, Administrators concluded that the immediate closure of the business was the only option available.

Faced with this scenario, CEO Peter Cox approached a private equity group to assist him to acquire the business, as he firmly believed that there is a successful future for the business and he believes that this solution is in the best interests of the Employees, Customers and Suppliers of the business.

Card Data Management Limited (CDML), a special purpose investment company focussing on the card services industry and backed by funds supplied by Carl F Pauwels an international banking specialist, Peter Cox the founder of ID Data and a Singapore based investment fund, have committed substantial working capital for the business, to ensure its rapid development and continued delivery of leading edge card technology.

EPIC Petitions FTC to Investigate Google, Cloud Computing Services

The Electronic Privacy Information Centre (EPIC) has formally asked the Federal Trade Commission to open an investigation into Google's Cloud Computing Services to determine "the adequacy of the privacy and security safeguards."

This investigation has been requested after the recent breach of Google Docs.

EPIC have urged the Commission to take "such measures as are necessary" to ensure the safety and security of information submitted to Google.

Does Contactless technology signal the end for cash?

By Tom Tainton, Smartcard & Identity News

Tom Tainton

The development of 'cashless' initiatives across Britain has led to predictions by industry experts that by as soon as 2015 contact less technology could usurp cash transactions and banish coins from our wallets (and under our sofas) for good. Currently, 85% of transactions in the UK are conducted via credit or debit card, and the decashification process is set to rise even further. Prime Minister Gordon Brown said contact less technology would 'dramatically improve payment in the retail sector' creating a market worth £30bn when national roll-out eventually occurs. But the key to the system's success is the attitude of retailers, who have so far proved a barrier to card payments under £10, a low-value transaction which isn't deemed worth the processing costs by merchants. The pricing for card transactions tend to include a fixed charge (irrespective of the amount) as well as a variable charge (a percentage of the amount) – this in particular penalises low-value payments. An average 'interchange' fee charged to retailers amounts to 4p per transaction, a figure which many say is too high.

It's a catch-22 situation, with customers unable to use contact less until merchants invest in the technology. But retailers only have to look at Transport for London as a shining example of how the Oyster contact less application has revolutionised use of public transport in the capital, a case study that would surely compel enthusiasm towards initial adoption.

Alex Mifsud, CEO of Entropay, says the logic driving society towards the replacement of cash with electronic money is based on convenience and security. "Cash is inconvenient to carry and can more easily be stolen than electronic money. Traditional payment methods include cash and cheques. Cash is inconvenient and, in large amounts, insecure to carry, and is not always available at the point of need, whereas the electronic equivalents such as bankcards offer convenience, security and ubiquity. As more payments take place without the payer being in the same place as the payee; electronic money is a more convenient, fast and secure way of making such payments than cheques sent through the post, and particularly for cross border payments, more cost effective too."

The 'cashless' society also has very positive implications for the pre-paid industry, with the shift away from cash providing robust opportunities for pre-payment companies. Mifsud claims pre-paid cards add further benefits to the proposition of electric finances. "Prepaid cards can be made available to almost anyone, including various segments of society that had been hitherto confined to cash. In addition, within relatively modest limits, prepaid cards can be anonymous and can therefore offer some of the privacy benefits of cash, prepaid cards are making it possible for whole segments of society to enjoy the benefits of cards As prepaid enters the mainstream, retailers will realise that a larger portion of their customers will want to pay by card. However, to realise the potential of cashless, the card industry still has to revise its pricing for low value transactions."

However, cash-handling is also not without cost for large retailers, a labour-intensive infrastructure is in place to collect and account for cash from tills and to deliver the money to a safe deposit. According to Michelle Whiteman, Corporate Communications officer at APACs, the number of non-cash payments will exceed cash payments for the first time in two to three years. "Just look at spending in 2008, despite the credit crunch total debit and credit card spending was up in 2008 in terms of both value and volume, increasing 6.8% and 7.4% respectively. We are seeing an increase in use of debit cards because spending rose from £224bn in 2007 to £245bn, whilst spending on credit cards rose only slightly from £123bn to £126bn."

Whiteman also emphasised the schemes available to encourage retailers to accept the technology. "The acquiring banks involved in these early stages of rollout are working with retailers on an individual basis to encourage take-up, and a variety of incentive schemes & awareness campaigns are underway. MasterCard and Visa are supporting the banks in this work. In the future, growing numbers of consumers will see contactless technology functionality added to their cards, and as more retailers adopt the technology cardholders will be able to take advantage of this new payment option."

So what sort of timescale can we expect before we experience an entirely cashless society? Well, Alex Mifsud doesn't think it's the end of cash just yet. "I think cash will survive as long as banks will dispense it and retailers will accept it. This will continue to happen so long as there remain segments of society such as the un-banked, and the underage which do not have ready access to electronic money."

World News In Brief

MasterCard PayPass Surpassing 50 Million-Issued Milestone

MasterCard Worldwide announced the issuance of the 50 millionth MasterCard PayPass, as of 4Q 2008, which in the last year more than doubles the number of cards and devices in circulation around the world. This significant PayPass momentum demonstrates not only the demand for simple solutions when it comes to payments, but also the continued secular shift toward electronic payments as validated by recent data that indicates 41 percent of consumers use cash less often today than they did two years ago.

PayPass provides a convenient payment alternative to cash. Consumers no longer need to fumble for cash and coins, swipe a card or even sign a receipt when making purchases of US$25 or below.

Heartland Warns of Legal Action if Competitors Continue to Make False Claims

Recently Visa removed Heartland from its list of PCI DSS compliant service providers.

Heartland's competitors have been making false claims to such as: "You could be fined because you use Heartland" or "You will not be PCI compliant if you use Heartland." Through a series of cease and desist letters, Heartland has informed competitors that their untrue and misleading claims are baseless and unlawful. Heartland intends to initiate legal action against them if they do not immediately stop making these claims.

Visa issued a statement on 19 March, indicating that merchants and other card-payment-accepting enterprises can continue to do business with U.S. payment processor Heartland Payment Systems, without threat of fines from Visa. These terms will remain valid as long as the Heartland continues to work on revalidating its own PCI compliance status, which they expect to complete within weeks.

Nokia Invests in Obopay

Obopay, Inc., the pioneering service provider for payments via mobile phones, announced an investment from Nokia.

Obopay will use this minority investment to aggressively extend their product suite and enhance their global presence, as mobile devices become constantly more integrated into the daily lives of the world's 4 billion mobile consumers.

Teppo Paavola, said, "This investment reflects our belief in the global potential for mobile payments. Obopay has consistently demonstrated its ability to redefine how people spend and send money."

Google Exposes 19,000 Credit Card Numbers

An Australian IT worker has exposed 19,000 credit card numbers within googles site cache, and posted the hack on a broadband forum site.

"The alert started with a bunch of other numbers, so I went to the web page and it was just a virtual directory listing with a bunch of directories underneath and a load of files inside,", "It looks like the site might have been a payment processing gateway that handled credit card transactions for a bunch of websites before it went belly-up." said the anonymous IT worker.

Several hours after Australian news site 'iTnews' picked up the story, they were contacted by the Australian federal police.

Google issued the statement: "Please keep in mind that search engines are a reflection of the content and information that is available on the Internet. Search engines such as Google do not own this content, and do not have the ability to remove content directly from the Internet. Standards are in place that Google and other search engines follow that enable site owners to protect information on their sites from being indexed and searchable. These standards give site owners the flexibility to publish content and control how it is found."