

Smart Card & Identity News

Is published monthly by
Smart Card News Ltd

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

Telephone: +44 (0) 1903 734677

Fax: +44 (0) 1903 734318

Website: www.smartcard.co.uk

Email: info@smartcard.co.uk

Editorial

Production Team - John Owen,
Lesley Dann, Suparna Sen

Researcher – Patsy Everett

Technical Researcher –
Dr David Everett

Contributors to this Issue –
James Hesse and Charlie Stevens,
Dr David Everett, Suparna Sen,
Abdelmajid Moujane, Tom Tainton,
Richard Fine

Photographic Images - Nejrion -
Dreamstime.com

Printers – Hastings Printing Company
Limited, UK

ISSN – 1755-1021

Disclaimer

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

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

© Smart Card News Ltd

Our Comments

Dear Subscribers



Patsy Everett

David Birch is starting a war on cash and this was the theme behind this year's Digital Money Forum held in London on March 2nd/3rd and arranged by Consult Hyperion. A report of the event is given elsewhere in the Newsletter.

At times it was hard to hear a good word about cash, vitriolic reverberations would tell you that

cash is bad and is the invention of governments to control the economy and to surreptitiously devalue the assets of its citizens as and when required. It must be a crusade because it wasn't obvious exactly how mobile payments are going to solve this and yet it seemed with few exceptions to be the general view of the room that mobile payments will be the saviour of mankind.

I must confess that the Digital Money Forum has brought about its fair share of excitement over the years but this year it was quieter, the odd spat but actually none of the battles that perhaps the organisers might have hoped for. There was to me a strange acceptance that cash is going to be replaced, not totally you understand, and that the mobile phone is everything. Look no further the future is clear.

I want to argue that both assumptions may be wrong, and there is no evidence that I can think of that would prove that physical cash will continue to exist. Do we really believe that cash as it currently exists will still be around in 50 years time? The protagonists here assume that the products from Visa and MasterCard will move into the cash space and will mop most of it up leaving just the very bottom end behind which is totally uneconomic to process. This of course assumes that nobody puts forward a real cash alternative.

The second argument is to think about how the mobile phone might develop over the next 50 years, will it be a fundamental part of our life? Of course it will be an integral part of our day, just as much as the computer is today but with an even wider capture of the population. The thing is that you need to just stop and think what's going on here. The mobile phone or at least the smart incarnations now dominating the mobile phone sales are capable of providing a voice channel as and when required and here's the new bit (well relatively new) it can also store, process and communicate data.

Now here is my argument, the mobile phone could do anything, take my electronic toothbrush, it's pretty sophisticated, it has Bluetooth, with data and processing ability to ensure I get the right amount of brushing but I wouldn't actually want my mobile phone to act as my tooth brush. When necessary I'm quite happy to carry a separate object in my bag. The main argument of the mobile futurists is that we the citizens only want to carry one object, the mobile phone, because it can do everything. In addition they can show through market research that we never forget our phone whilst other objects like our wallet might well get left behind.

Of course, I deliberately picked an obscure situation with the toothbrush but I think the assumption that you must have your wallet and by inference all your payment items in the mobile phone is equally flawed. At the very least surely we want to distribute risk?





Security is one of those subjects that many find easy to ignore, as long as it hasn't happened to me then it will be alright. I remember once a good friend explained to me that selling security was like trying to sell a bad smell, you certainly don't get long queues. In the news today there are stories of Google removing malicious applets from the Android market and the Zeus Trojan infiltrating the Blackberry phone and effectively taking control, there have been earlier reports of it attacking both Symbian and Windows Mobile phones as well.

My next proposition is that Mobile phones will become the prime target for malware (actually they probably already are the target) and it will not be easy to stop. Any device that allows the user to download executable code is going to have a problem that is not going away any time real soon. You might imagine that it would be possible to security audit software before allowing the modules to be downloaded, that's a problem that people have been looking at on PCs for at least the last 20 years with no silver bullet in sight. Of course you could restrict the software to do very little but then nobody would want it.

But it's a fun world ahead of us,

David (on behalf of Patsy)

Contents.

Regular Features

Lead Story – VeriFone Attacks Square	1
Events Diary	3,4
World News In Brief	8,13,18,20

Industry Articles

Biometrics in Travel and Identity Documents:	
The Case for Front Line Verifiable Features	6
Digital Money Forum London March 2/3rd 2011	10
India to Block Imported SIMs:	
Over Risk to National Security	14
Five years of SEPA and the journey continues	16
Interview with Karen Walsh,	
Head of Financial Services at Everything Everywhere	17
Get Secure, Not Security	19

Events Diary

April 2011

- 4-6** Security Document World 2011, London, UK – www.sciencemediapartners.com
- 5-7** Euro ID 2011, Berlin, Germany – www.euro-id-tradefair.com
- 12-14** IEEE RFID 2011, Orlando, USA - www.ieee-rfid.org
- 13-15** Card Asia 2011, Singapore - www.terrapinn.com/exhibition/cards-asia
- 19-21** Infosecurity Europe 2011, London, UK - www.infosec.co.uk
- 27-29** 23rd Annual Card Forum & Expo, Florida, USA - www.paymentssource.com/conferences/cfe11

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





May 2011

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

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

VeriFone Attacks Square Continued from page 1

Square is a small, magnetic credit card reader that works with iPads, iPhones and Android devices. The device is plugged into the headphone socket of an iPhone or iPad. When a credit/debit card is swiped by the reader, a signal is sent through the headphone/microphone socket. Square's application software interprets the signal, and then sends transaction data using either a Wi-Fi or a 3G internet connection to back-end servers, which in turn communicate with the payment networks to complete the financial transaction.

Square offers receipts displaying the merchant's name who swiped the card, a map of the location where the transaction took place, and an itemised description of what was purchased. Customers can save their receipts from Square merchants in their email archives.

On the other hand VeriFone's PAYware Mobile device works only with the Apple iPhone (3GS, and 3G). The PAYware Mobile is bigger than the Square card reader. Every financial transaction can be tracked on PAYware Mobile through the single PAYware Mobile Gateway. In case the device is lost or stolen, customer can deactivate the Mobile via the Gateway. PAYware Mobile emails transaction receipts to customers, and a transaction record is made accessible in the application and PAYware portal, which can be easily reprinted.

Key Points Table:

Square	VeriFone
Has a simple pricing structure, and charges a flat rate of 2.75% on every monthly transaction	Has a complex fee structure with interchange, assessment, processor mark-up fees and a monthly standard charge. PAYware Mobile only starts to get competitive when the average transaction is over \$30 and the merchants turn-over is high (see: http://feefighters.com/square-vs-verifone#comparison_details) for an interactive comparison tool.
Works with the iPhone, iPad and Android devices	Works only with the Apple iPhone
Small Square dongle attached to headphone/microphone Socket	VeriFone shell which encapsulates the phone, using the dock connector.

The Accusation against Square:

Douglas G. Bergeron wrote: "In less than an hour, any reasonably skilled programmer can write an application that will "skim" – or steal – a consumer's financial and personal information right off the card utilizing an easily obtained Square card reader. How do we know? We did it. Tested on sample Square card readers with our own personal credit cards, we wrote an application in less than an hour that did exactly this".





All you need is a Square dongle that is available for free and create a fake Square application on your smartphone. Then, insert the dongle into the audio jack of the smartphone or iPad, and that how so simply you get a mobile skimming device that fits in your pocket and that can be used to illegally collect personal and financial data from the magnetic stripe of a payment card.

VeriFone believes the culprit (of course Square's owners) have build in a "poorly constructed" credit card reader that has no ability to encrypt a customer's personal data.

VeriFone's CEO fears Square's credit card reader will give cyber criminals enough room to turn the reader into a skimming device, thereby leading to large-scale cloning of consumer credit cards around the world.



Figure 1: Square Reader



Figure 2: VeriFone PAYware Mobile

In response to VeriFone's accusation of the magnetic credit card reader posing serious "security flaws", Square CEO Dorsey published his own open letter "on credit card security and Square" on 9 March 2011 where he argued: "Today one of our competitors alleged that the Square card reader is insecure. This is not a fair or accurate claim and it overlooks all of the protections already built into your credit card. Any technology -- an encrypted card reader, phone camera, or plain old pen and paper -- can be used to "skim" or copy numbers from a credit card. If you provide your credit card to someone who intends to steal from you, they already have everything they need: the information on the front of your card".

According to Jack, anybody and at anytime can forge a credit card. For instance, a person can take photos of your credit card or simply write down the card number when you are busy enjoying a drink or chatting with your friend.

On March 9, 2011, Greg Kumparak (the editor of MobileCrunch.com) calls Verifone CEO's open letter a "FUD" - Fear, Uncertainty, Doubt. Greg believes the problem lies with the credit card system itself, which is working more on trust rather than on heavily built security measures.

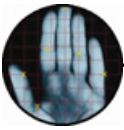
Over the years, experts have shown how easily encoding in magstripe cards can be copied. Fraudsters swipe the card through a second magnetic-stripe whilst your card has been taken out of sight - in restaurants for instance.

According to Elvira Swanson, a spokesperson for Visa: "a magstripe card contains the card holder's name, a 16-digit credit card number, an expiration date and a credit verification value (CVV) - a three- or four-digit number used in transactions in which the card is not present and the signature cannot be verified (mainly, online purchases)".

To prevent future misuse of magstrip cards, The European Payments Council passed a resolution on 31 January 2011. The Council spoke clearly on limited use of swipe cards, permitting the banks "to refuse magnetic stripe transactions if they so wish". [Source: European Payments Council - Doc EPC424-10]

By Suparna Sen, Smartcard & Identity News





Biometrics in Travel and Identity Documents: The Case for Front Line Verifiable Features ***By James Hesse and Charlie Stevens***



James Hesse



Charlie Stevens

The introduction of biometrics to travel and identity documents represents a major step forward. While adding a welcomed improvement to the overall security of such documents, biometrics should not be relied upon as the answer to document fraud.

Authentication of Identity

The purpose of travel and identity documents is to verify identity and citizenship, and the authenticity of these documents is exceedingly important. Before biometrics was introduced, a photograph and biographical data of the bearer were attached or printed into the document to assist the examiner in determining its authenticity. Unfortunately, the advancement of document scanners and colour printers over the years made it relatively easy to counterfeit and/or alter these documents.

Biometrics changed this by providing an additional machine-assisted accurate method to authenticate the bearer. Biometrics identifies a person based on matching physiological or behavioural characteristics of the person stored in the document with those of the person actually presenting the document.

The International Civil Aviation Organisation (ICAO) laid out standards, accepted by the more than 190 ICAO participating states, for incorporating biometrics in global international travel documents. ICAO chose facial recognition as the mandatory biometric for machine readable travel documents (MRTDs), with fingerprints and iris as approved options. In international travel documents, there is an ICAO standard machine readable zone (MRZ) containing biographical and document details that could be checked against watch list databases.

It would seem that a credential containing a securely stored biometric is the solution to document fraud and there is little need for additional security features on such a document. Nothing could be further from the truth. If a document reader read every credential that contained a biometric and a live “one to one” verification was conducted then that might be the case. The reality is that 95% of travel and identity documents are not read by a reader!

ICAO, however, has never considered biometrics to be a panacea in itself for identity verification but simply to provide an additional security measure. However, there is a serious concern that some examining officers will develop a false sense of security when examining a biometrics-based credential. If the document is not read and doesn't have front line verifiable features it maybe actually less secure than non-biometric documents.

Front Line Verifiable Features

Because of these risks, ICAO has continued to promote physical security features in its standards for all machine-readable travel and identity documents. Indeed, it has stated that a biometrics-based travel and identity document should retain all of the physical security features contained in non-biometrics documents so that examining officers can confidently verify identity and citizenship even if the biometrics chip is non-functional or a suitable reader is not available.

ICAO introduced biometrics standards for ePassports and travel documents in 2006 and it is likely that it will be some time before the global uptake of biometrics specifications in travel and identity documents by all States. The deployment of readers is even slower, and it is not likely that there will be biometrics documents readers will be used at all control points around the world for many, many years to come. To ensure that examining officers can reliably and consistently authenticate all credentials, biometric or not, such documents must contain the highest level of front line “eye-readable” and “tactile” security features. These are proven visual and tactile security features that officers can quickly and confidently rely on. It is essential therefore that all document examining officers must be trained to verify credentials through physical security safeguards alone.





Eye readable security features with basic tools: The Optical Security Media offers a layer of security with over ninety (90) extremely high-resolution (24,000 dots per inch) and detailed micro images. When these images are viewed with a simple magnifier, examiners will be able to differentiate genuine images from counterfeits due to the quality of the resolution. The PRC also contains fluorescent inks that are revealed when viewed with an ultraviolet light source. Further, there is a latent (hidden) “diffractive” image that can be viewed with a small hand held tool.

Unique personalisation features: The Optical Security Media contains high-resolution, high contrast eye readable security features, which are laser etched into the stripe to include the bearer’s photograph, name, signature and other pertinent biographical data. Also, lasers produce a clear tactile personalisation of the bearer’s date of birth and gender and there is additional black tactile laser engraving on the front of the PRC.

Biometrics: The Optical Security Media, which can store up to 1.6 Mbytes, is used to accommodate the biometrics in the PRC. The OSM contains all digital files and multiple biometrics to include high-resolution photo, fingerprint and signature of the bearer. The OSM also provides the unequalled flexibility of adding additional biometrics and/or other digital data in the future i.e. records of dates and location of exits and entries.

Database access: The PRC uses a Radio Frequency Identification (RFID) chip to instantly access a database that displays the photo image and other biographical information that should appear on the card that is being read. The document and bearer are also checked against a watch list.

Forensic security features: The PRC contains numerous security features that can only be accessed in a forensic laboratory environment.

To summarize, the introduction of biometrics in travel and identity documents is a necessary advance in document security but the existence of stored biometrics in credentials should not be viewed as the total answer to document and identity fraud. There continues to be a very important part for excellent quality physical security features to play in biometric credentials. The layered security methodology, incorporating a wide range of high quality and proven physical security features from front line to forensic level, will result in the production of the most secure, accurate and counterfeit resistant travel and identity documents possible. The U.S. Green Card sets an extremely high standard among government identity card programs worldwide and it demonstrates the strength of the layered approach in delivering a secure, ICAO-compliant credential that can be confidently authenticated in multiple scenarios from front-line to forensic verification.

World News In Brief

AT&T to Acquire T-Mobile USA for \$39 Billion

AT&T is said to buy rival T-Mobile USA from Deutsche Telekom AG for \$39 billion (24 billion-pound) making it the largest mobile phone company in the US. The deal would give AT&T about 43% market share, putting it well above the industry leader Verizon Wireless.

T-Mobile customers will get access to AT&T’s phone line-up, including the iPhone. AT&T is looking to increase its network capacity to handle the rapidly increasing consumer demand for videos and data.

AT&T expects the deal to be completed in 12 months. AT&T Chief Executive Randall Stephenson told reporters "the company had done its 'homework' on the regulatory side of things". He believes the deal could generate savings of more than \$40 billion.

RIM Silent about Embedded Chips in NFC Phones

Research in Motion (RIM) is continuing to decline comment on its plans for embedded secure chips in its forthcoming BlackBerry NFC phones. The handset maker in the past has said it would work with mobile operators as it begins to roll out NFC phones in 2011. But a new report contends that RIM is seeking to go around telecommunication firms to put applications on the embedded chips. Among the assertions are that RIM has talked directly to banks about putting payment applications on the secure chips and that it seeks to use the chips to bind users to its phones.

RIM has declined to comment on the article. At the 2011 Mobile Financial Services conference in London, in response to a question from NFC Times, one RIM representative said the handset maker, "for



obvious reasons," was "very restrictive" about revealing what it has planned for NFC.

UK Data Breach Hits a New Record Cost of £2 Million

The cost of a data breach in the UK has risen for the third time in consecutive years to reach on average £1.9 million, with malware-related hostile attacks causing significant damage, according to the latest annual research from Symantec.

Symantec's '2010 UK Cost of a Data Breach' report found the cost of data breach in the UK had risen 13% year-on-year to an average of £71 per record. The incident size ranged from 6,900 to 72,000 records, with the cost of each breach varying from £36,000 to £6.2 million. The most expensive incident increased by £2.3 million compared to 2009.

Hostile attacks were the most expensive for firms to deal with as they have to pay for things like detection and notification and also risk losing customers due to diminished trust. These were also the fastest growing form of threats, increasing in volume by 22% from the previous year, according to Symantec European product marketing director, Robert Mol.

The most common form of threat was system failure, accounting for 37% of incidents, while threat from negligence was 34%. However, an increasing concern for those surveyed was the threat from insecure mobile devices connecting to the corporate network. Some 64% of those studied said they recognised the risk, while a whopping 84% said that insecure mobile devices were likely to have accessed corporate data. "Mobile devices are a growing cause of concern because of their ability to carry confidential information": said Mol.

LaserCard Receives \$2.1 Million Order for Saudi Arabia National ID Card Program

LaserCard Corporation has received an order valued at approximately \$2.1 million for chip-ready, optical security media-based credentials for the Saudi Arabia National ID Card program. The ID cards are issued to Saudi citizens nationwide for identification, e-government and regional travel purposes.

LaserCard's advanced ID credentials are trusted by governments worldwide to protect the personal identification of their citizens, foreign residents and government employees, and to provide official documentation such as driver licenses and vehicle registration cards.

Vodafone is the Top UK Mobile Phone Brand

Vodafone has emerged as the leading UK telecommunication company in a league table of the world's top brands, standing at fifth place in a list dominated by American companies. Google topped the latest Brand Finance Global 500 report, boasting a brand value of more than \$44 billion. The top ten also features Microsoft, in second place with a brand value of nearly \$43 billion, IBM and Apple, whose brand was given a value of nearly \$30 billion over 2010.

Vodafone achieved the 5th place compared with 7th place in the previous report. It is the only UK company to make it to the top 10, with a brand value of nearly \$31 billion. The only other UK representatives in the top 25 are HSBC bank and the retail giant Tesco. HSBC slipped out of the top 10, going from 8th to 11th place, while Tesco was also down, from 17th to 19th.

Apple had a good year, moving up to the 8th place from number 20 from that of 2009 owing to the success of its iPhone and iPad.

Google, VeriFone to Become Mobile-Payment Partners

Google Inc. is working on a potential partnership with electronic-payments company VeriFone Systems Inc., to allow shoppers to use Google's mobile devices rather than physical credit cards, to pay for goods in retail stores.

VeriFone makes point-of-sale terminals that retail stores across the country use to process credit-card payments. As part of the potential tie-up with Google, VeriFone's terminals would be able to accept payments from mobile devices that are embedded with technology called near-field-communication, or NFC, according to news sources.

RIM Faces New India Shutdown Threat from April 1, 2011

Indian intelligence agencies, the interior ministry and telecom ministry have issued a fresh deadline of March 31 to RIM on getting full access to corporate enterprise services on all BlackBerry handsets.

The Canadian company had recently provided encryption keys for its Messenger and Internet services to Indian security agencies after the government had threatened to shutdown these facilities. Corporate enterprise services are also facing a shutdown threat in the Indian market if RIM does not provide investigators access to India.





Digital Money Forum London March 2/3rd 2011

By Dr David Everett, Smartcard & Identity News



Who moved my cheese?

The well known parable by Spencer Johnston also co-editor of the One Minute manager but probably less well known is that ice was the second major export from the USA in the 19th century, you don't need to ask but Cotton was number 1. Of course the refrigerator put an end to all that and this was the way the forum was started by Dave Birch of Consult Hyperion, the implication from him and others is that the mobile phone is today's refrigerator for the world of payments. This was truly the cold frosty start to the Forum.

Metal and paper currency should be dead but they are not

A leading statement from Richard Watson (author of Future Minds) on the future of money but preceded by the statement that the future has many possibilities it's just that we don't know which one. As he said the best way to predict the future is to invent it. There were really two things that stood out here, the enormous change in the connected world with mobiles and the internet and the realization that nationalism and tribalism are on the increase. Most of our internet world is made up of walled gardens, Facebook being an obvious candidate, but so too in the mobile world with the likes of Apple, Android, Blackberry and others including the Mobile Network Operators (MNOs). The future as Richard sees it is based on the consumer demand for simplicity and security. I can't disagree with that but I'm not convinced that consumers have quite got to the security bit yet.

Alternative currencies are OK but where is the guarantee I'll get paid

Almost a common theme from the panel on alternative currencies, how much better it would be to have tokens or the rights to food and welfare as required. But and there were some big buts, if you were to have tokens for electricity in Kilo Watt Hours for example how do you know it will be honoured in the future. The problem here is that communities have changed, it is almost impossible to live entirely within a local community, you have to involve foreigners.

Money is to allow governments to apply taxes

A much repeated statement during the course of the forum, I never realized people were so against taxes. Perhaps everybody really fantasizes about going back to the local village disconnected from the rest of the world. Anyway money is the means by which governments are able to control the economy and so there is no way it can be allowed to disappear. Banks (i.e. central) create most of the money in circulation and therefore by default they effectively control the value of that money over time. As we shall see later that hasn't done too well against for example gold.

The best toilets are in Japan

Or at least that's what Michael Salmony from Equens would have you believe. Certainly the pictures of the fully electronically controlled seat and bits and bobs that work on some of the more delicate parts of the anatomy would seem to provide the necessary evidence. However Michael was at pains to point out that Japan is not actually as far ahead as you might think. It is a high tech country as per the toilets but also it is low tech, overhead power cables are strung everywhere to cope with earthquakes and it's also one of the highest cash per capita countries in the world (\$6617/capita versus €2250 for Europe). Contactless is everywhere fragmented amongst many players although the terminal somehow manages to select the right one. The social community is dominated by the environment, and there is a shortage of land because the Japanese Islands are so mountainous. Accordingly houses are small and typically don't have a PC, so it's down to the internet café or now onto the smart phone. An interesting figure from Gartner was that in Japan the average for mobile payments is 1 transaction per person per month, not quite as many as some would have you imagine.

Trojans crack mobile phones

Not really in doubt but Riten Gohil from Visa wanted to concentrate the mind and set the backdrop for Visa's new CodeSure smart card with a keyboard and display. He was referring to the Zeus Trojan which has recently been reported to having infiltrated the Blackberry mobile phone and to effectively crack the 2-factor SMS authentication often used for mobile banking. The issue here is that if you accept this proposition then what is the future for mobile payments, won't you always have to use a separate security token, smart card or what have you? I agree in the sense that I can't see how the security of mobile phones is going to suddenly solve all the problems.



Bank liable for customer authentication

Well this is now the case in Japan under the 2007 Act. The problem is how do you do it? Is biometrics the right way? Martyn Gates of Acram Int'l put forward a pretty good case showing that vein palm and finger are doing quite well. It was however probably the bit at the end that was the most significant. The liability issue as we mentioned but of course using biometrics will still give you errors. Martyn pointed out that really you do need to go multi-modal (i.e. use several techniques on which to base your decision) but this gives you registration problems which now become quite time consuming. However against this background there is a need to accept that your identity (biometrics) may become compromised. So you need to have multiple identities and be prepared to delete them. Now here is an interesting point, exactly how do you do this?

NFC too slow for mass transit

In the expert panel on transit Ben Whittaker from Masabi, was keen to point out that NFC is just not fast enough as a replacement for London's Oyster card. Passing through those transit gates means that the contactless application needs to do its business in about 300 mS according to Shashi Verma from Transport for London and he should know. Apparently mobile phones can't work at this pace and the consensus seems to be that contactless cards from Visa and MasterCard will be the future payment instrument for London Transport. I gather they would like to phase out the Oyster card and let others worry about payments. Somebody did ask an interesting question, how does the ticket inspector know you have paid if you are using your contactless payment card?

Nine million bicycles in Beijing

That's a fact according to Katie Melua in her hit single. I'll leave others to complete the lyrics but as Tomi Ahonen from Communities Dominate Brands, and others pointed out there are 5.2 billion mobile phones in the world or during the course of the forum various numbers up to 6 billion. So far more phones than PCs but does this mean they are going to be the end of cash? Nobody seriously doubts the impact but equally few actually believe it will be the end of cash. I'm not sure even Tomi thinks that but as he pointed out mobile phones can be used for payments in ways that you may not have imagined including a means for buying ice cream in Brazil using an SMS message.

There's a street in Amsterdam that doesn't take cash

Not perhaps what you might think but Dave Birch was full of tales of Holland and particularly Amsterdam where cash is on the way out. Apparently there is such a street where all the shop keepers got together to agree that they would not accept cash, isn't there some contradiction about legal tender here? Anyway there is also a whole town where they are planning to give up cash. Call me cynical if you like but it sounds like a tourist attraction, we would all like the idea of spending the day without cash.

Coins are a problem, how do you get rid of them?

The Mint that produces coins won't take them back and this was one of the many insights from George Selgin from The University of Georgia, USA, on the history of private coinage and innovation. What was most interesting was how copper tokens produced by tradesmen back in the 18th century became far more popular than the coins of the realm. Not only were they far better produced, more difficult to counterfeit, readily available but they also carried the words 'we promise to pay the bearer'. Because the Mint wouldn't take back coins nobody wanted to be left holding them. The banks in particular didn't really want to know the low value coins. Gold and silver were OK but the copper coins for the man in the street just weren't readily available. This was where the manufacturers and trades people produced their own tokens. Apparently these tokens would often carry a premium because the merchants didn't like accepting the regal coins. Government apparently stepped in once these tokens gained too large a presence. George left us with something to muddle over, Cash benefits the poor, crime even more. Well that was an interesting thought for the day.

Gold, no clearing, settlement or risk

If you didn't believe it before by the time John Turk from Gold Money Foundation had finished his presentation you were convinced. He made a very good case supported by facts that show the purchasing power of gold has been preserved with time while this is clearly not the case for currency for which the Pound Sterling has fared particularly poorly. Don't keep cash under the mattress, lumps of gold will do you far better? I'm not sure how you move it around electronically but that's for another day.





Myths: Cash is forever, payments instruments change slowly and are consumer led

You might not imagine that getting rid of cash would have been the future of PayPoint but David Steed wanted us to look at what he saw as inevitable. He wanted to point out that the cost of handling cash is far higher than people realize and that other instruments such as direct bank account transfers are much cheaper to manage. He asked the question, ‘why would cash be around’ when you are also seeing increases in counterfeiting which for the UK pound coin is currently running at 2.5%. He predicts that this can only increase and will also be more difficult to detect.

Mobile transaction fees can be 25% or more

People complain about the 2.5% merchant fee typically charged by the merchant (transaction) acquiring bank but get prepared for 25% says Erich Ringewald from Boku. In fact the audience joined in here and pointed out that when making payments through the Mobile Network Operator you might even want to be prepared for a 50% transaction fee. The problem of course is the cost of funds, in many cases the user account held by the MNO is funded on some prepaid basis where the consumer may top up at the corner shop. In such situations it is not unusual for the commission on top up to be anywhere between 10 and 20%. If you are buying virtual goods then these high fee levels may be accommodated but it really doesn’t work for the sale of tangible goods. Erich also offered the view that he felt that prepaid service providers need to be regulated whereas post paid providers do not.

Two bottoms wide

Have you ever wondered why railway tracks are 4ft 8.5 inches wide? Mark Hartley of American Express gave an interesting discussion on standards as relates to EMV but was able to explain the significance by drawing on history. It was a long story but along the lines that the USA gauge was based on the British gauge which in turn came from the width of the roads which came from the Romans, you get the drift. Anyway the final measurement came down to the width of two horse bottoms which had to pull the Roman chariot along the road. Anyway back on topic Mark made it very clear that the issuer must choose the Secure Element (in the phone) whether the UICC (i.e. SIM), chip in phone or the MicroSD card. I know where my money is and it’s not on the SIM card, can you see the MNOs and the FIs coming to an agreement on sharing the SIM in the next 10 years? The funny thing is there is actually a standard for accessing the SIM card for NFC use called the Single Wire Protocol (SWP) and very little else for the use of MicroSD or what have you. The phone manufacturers are betting on it but we will see.

Contactless is all about speed and convenience

Maybe nothing has changed, anyway John Conlon from Barclaycard re-emphasized that selling contactless cards to the consumer is all about speed and convenience. Anyway he gave a table of figures for how he sees the future of contactless.

Year	Cards Issued	Accepting Retailers	Comments
2010	12 million	5%	Launch
2011	25 million	10%	More big retailers
2012	50 million	20%	Buses and Tube
2015	100 million	40%	Billions of Txns

Just one interesting figure for me, in 2015 only 40% of retailers will be accepting contactless. So in 2015 at least the phone will not be everything. This rather supports the view from the field that the merchants are not getting too excited about contactless. From their point of view its new terminals and anything else that goes with it, including terms and conditions.

85% of the world’s population is unbanked

Of course we know but we don’t often think about it. Elisabeth Berthe from the Grameen Foundation was able to bring us to our senses. So that means 1 billion people out of a total world population of 6.5 billion have a bank account (so who is using those 9 billion bicycles in Beijing?). However 40% of the unbanked have access to a mobile phone. We have seen the success of m-Pesa in Kenya but less well known is that 75% of the people actually use mobile money as the way of storing their cash. You can’t imagine it but all your wealth carried





around in a bag on your back. Stories of the rats eating your currency and the need to store cash in a tin. Then of course robbers because they know you are carrying cash. It's hard for most of us to appreciate.

Bank tellers tell the government everything

The last panel of the day was devoted in trying to decide whether cash is good or bad. A mixed view from the panel perhaps but there was certainly an assumption that cash won't go away. Cash is good because it is anonymous, non traceable, fungible and can be stored. However cash is expensive to handle and poses security problems for all those that have to handle cash. Governments meanwhile like everything to go through the bank so that they know what is going on. The state is seen as being in charge of inflation because they can interfere as and when required with the money supply. Criminals meanwhile embrace technology even more than consumers, as we were reminded banks don't get robbed any more (for cash), much nicer to do it electronically. Another assumption as well, everybody assumes that only cash is untraceable, is this correct?

World News In Brief

Lloyds TSB Launches Contactless Debit Cards

Lloyds TSB launches contactless payments on its VISA debit cards to current account customers within the M25. Any new or replacement VISA debit cards issued will enable customers to pay for small purchases up to £15 using contactless technology. Lloyds TSB is expecting to issue around 1 million VISA contactless debit cards in 2011.

When using contactless to make purchases, customers will be protected by the same high level secure technology that is behind Chip and PIN. Additionally, Lloyds TSB will continue to provide the same assurances in the event of any fraudulent use as with Chip and PIN payments.

Monitise to Develop Mobile Banking App for Blackberry Platform

Monitise plc is developing a new banking app for all UK BlackBerry smartphone users. The mobile banking app, which will be launched this summer, will deliver a high quality look, feel and user experience specifically tailored for BlackBerry smartphones. The app functionality is being developed via Globe, Monitise's technology platform which allows financial institutions, service providers, payment companies and processors to create a wide array of Mobile Money services in both developed and emerging markets.

Sweden Renews Multi-Year Contract on ePassports and eID Cards with AB Svenska Pass

Gemalto announced that the Swedish National Police Board ("Rikspolisstyrelsen") has renewed its five-year agreement for travel documents on behalf of the

Swedish Police, the Ministry of Foreign Affairs and the Swedish Migration Board. The contract has been signed with Gemalto's operating company in Sweden - AB Svenska Pass, and also includes the launch of the European Residence Permit. The company manages the end-to-end delivery process including the live enrolment solution in Sweden, production of all secure travel documents, as well as operated issuance services. The contract value for the five year period is 1 billion Swedish Kronas (over 110 million euros).

The contract includes the enrolment solution including the software for registering the applicants' personal data, along with enrolment kiosks for instant capture of the holder's photograph, fingerprints and electronic signature. Gemalto supplies the operated issuance services, which ensure document personalisation from AB Svenska Pass' secure service centre, and delivery to issuing authorities. The secure solutions and the production of all secure travel documents will be delivered by Gemalto.

1.5 Million ASK Contactless Cards Successfully Deployed in Dubai

ASK has delivered the first batch of 1.5 million Nol cards in Dubai. The project was implemented by System Integrator and partner Abba Electronics, a division of well-known Al Abbas Group, for Dubai transport operator, RTA (Roads and Transport Authority).

Nol card is a multimodal contactless card with 3 different layouts and various features to be used in Dubai metro, buses, water buses and parking meters. Silver card is an anonymous card with an e-purse. Gold card holds the same features and grants the holder the privileged access to Metro's Gold Class seats for premium charges. As for Blue card, it is a personalised card with the holder's photo.





India to Block Imported SIMs: Over Risk to National Security

By Suparna Sen, Smartcard & Identity News



Suparna Sen

Early this month, the Indian Ministry of Home Affairs (MHA) warned the Department of Telecom (DoT) about the possibility of SIM cards posing a threat to national security. The MHA has written to the DoT for a status report on imported SIM cards, especially from China.

“The MHA has asked us to look into whether there is a security threat from such SIM cards that are imported and whether there are any implications on the sector if the import is banned. They want to assess the implications of such a ban” said a senior DoT official requesting anonymity.

Majority of active SIM cards in India are imported under the open general licence (OGL) from either China or from other low-cost markets across Asia like the Middle East.

MHA believes many of the SIM cards being used by nearly 700 million mobile users in the country may have malicious embedded software into them that can help compromise the encryption keys of a mobile phone SIM card.

With the encryption keys in hand, terrorists can get remote access to any SIM card operating in India, and use it to trigger various security attacks, including denial of service, disclosure of subscriber location or diverting and routing of calls and SMS.

India is also being firm in demanding full access to the encryption keys required for the lawful access of RIM's BlackBerry, Gmail and Skype for open interception by the country's security agencies.

Sale of fake SIM cards:

In the Indo-Nepal border, the sale of un-verified SIM cards has been a constant cause for concern for India's security agencies.

An interesting finding by IBN-7 (a Hindi news television channel run by Network 18 Ltd based in Mumbai) exposes how pre-activated SIM cards are being openly sold in the markets across the Indo-Nepal border for as little as Rs. 30. At Rupaidiha town in Uttar Pradesh at the India-Nepal border, hundreds of people travel back and forth every day to buy ration and other basics. But what is available even more easily than groceries are the SIM cards of different cellular operators.

According to the Indian law, when you buy a SIM card, you have to provide a copy of your identity card and a residence proof. But, at the Indo-Nepal border, all you need is money to bypass the laws. By paying anything between Rs. 30 to Rs. 200, a person may get a pre-activated SIM card almost immediately.

IBN-7 reporters went to four places at the India-Nepal border, and it seemed there was no deterrence for dealers while selling them.

At the Rupaidiha town itself, a shopkeeper offered a pre-activated SIM card for Rs 200, and after bargaining the deal was finalised at Rs. 170. What's more surprising is that at the first market on the Indian side once you cross into the town of Barhni at the Indo-Nepal border, shopkeeper's stock pre-activated SIM cards of a government owned cellular operator.

The IBN-7 reporters bought total 15 SIM cards of various cellular operators without any ID proof at the Indo-Nepal border in Uttar Pradesh.

When told about the incident, the Cellular Operators Association of India said they were aware of this problem. “It is a major cause of worry for us as it concerns national security. We hold surprise checks and have made stringent policies and we have even blacklisted some of the distributors and retailers. We have started this programme in Karnataka and plan to extend it to the rest of the country”, said Rajan Mathew, Director General, Cellular Operator's Association of India.

However, ironically in 2010, only 8 arrests related to fake SIM card have made in India.



The trio was arrested in July 2010 in Bangalore city of India on charges of selling fake mobile phone SIM cards. 400 illegal SIM cards were seized from them.

In Jammu and Kashmir, till recently, the India government imposed a ban on the use of pre-paid SIM cards. Reason being terrorists were using pre-paid SIM cards to communicate with their associates.

On January 18, 2010, during the 22-hour long gunfight in Jammu and Kashmir's capital Sri Nagar's Lal Chowk between Pakistani Lashker-e-Toiba terrorists and Indian security forces, the Indian forces recovered a handful of pre-paid SIM cards from the terrorists, who were using them to communicate with their handlers. Later, over 1000 unverified SIM cards were seized by the Jammu and Kashmir police from various parts of the region. As early as in 2007, Bharti Airtel (a leading Indian telecommunications company) had to cancel over 10,000 illegal SIM connections in the state.

In December last year, the country's home minister stated that of the 9 million SIM cards used in Mumbai, most of them are acquired via forged papers. The city police succeeded in finding only 6,300 fake SIM cards, with either false addresses or names on each of the card.

How do SIM cards pose a threat to national security?

SIM cards are personalised when a manufacturer gives a mobile phone company the secret keys and encryption data, unique to each card. It is the specific keys and encryption data that get loaded by a network operator on to their switches and is used to manage both network and the subscriber. Once the encryption keys and data gets loaded into the network, the SIM card maker and mobile service provider get access to the same set of encryption keys for every SIM.

Since in India's case, the SIM cards are imported from outside, the home ministry feels "this sensitive encryption information and keys continue to remain with the overseas SIM maker, outside India's territorial limits". Any malicious use of the encryption data and secret keys can result in large scale cloning of SIM cards.

To prevent any such duplicity in future, the Union home ministry has asked the telecommunication department to make arrangements for local manufacturing of SIM cards or allow mobile phone companies to import SIM cards only against security clearance per procurement.

The security agencies are proposing that only blank SIM cards be allowed for import and the personalisation process be done entirely by domestic firms. However, since this can only reduce vulnerability of future imports, MHA wants the industry to replace all existing SIMs at its own cost. The MHA also wants the DoT to delete all fake and duplicate IMEI numbers.

According to a government source, only 30% of the total volume of SIM cards is imported at present, though even this figure will now be subjected to a formal evaluation of installed capacity.

The India government desperately wants the use of indigenous SIM cards, since it becomes much easier for the Indian security agencies to control and scrutinise India-made SIM cards.

Furthermore, the imported SIM cards may have "malicious embedded software" inserted within them which the government may be unable to find or detect. But, if the SIM cards are manufactured within the country, the Ministry of Home Affairs feels the encryption keys will remain secure and accessible to national security agencies 24x7.

Until the Indian market gets flooded with exclusive India-made SIM cards, and people start using them, Indian Ministry of Home Affairs have asked the security agencies to strictly scrutinize and certify each new SIM card as safe before being activated and sold in the market.





Five years of SEPA and the journey continues

By Abdelmajid Moujane, payments expert at Callataÿ & Wouters



Abdelmajid Moujane

In January this year, the European Central Bank's (ECB's) Gertrude Tumpel-Gurgell talked about a list of SEPA (Single Euro Payments Area) New Year resolutions for the EU payments industry. Within this list Tumpel-Gurgell identified a number of steps needed to ensure SEPA is a long-term success. However, with progress of the scheme taking longer than anticipated, it is questionable whether the industry is ready to take the steps needed.

Starting with innovation, Tumpel-Gurgell believes that there needs to be more innovation in online payment markets and it is hard to disagree. Innovation through e-commerce and e-payments solutions can only serve to help banks better support their customers' needs. However, the proposal to deliver a European wide implementation of e-payment solutions such as those that already exist at a national level, for example in Germany, Austria and The Netherlands, is to me, unrealistic at this point in time. The proposal lacks recommendations and practical ideas on how such an ambitious scheme could be rolled out across the entire Euro zone. One area where progress is being made, however, is the beginning of cooperation between payment services providers (PSPs) and mobile network operators (MNOs) with the aim of promoting mobile contactless payments across SEPA. In recent weeks, we have seen O2, VISA, Orange and T-Mobile (Everything Everywhere), MasterCard, Barclaycard, BlackBerry, and (if the rumours are true) Apple, all show interest in contactless payments using near field communications (NFC) payment systems. Several phones such as the Google Nexus S and the Nokia 7 already have the technology. It is therefore fair to say that the banks do need to embrace new payments methods such as mobile, or else the industry will simply continue without them.

Let's also look at the SEPA end-dates. The ECB's preferred timelines for a forced migration to SEPA-compliant Credit Transfers is the end of 2012, with Direct Debits following in 2013. The industry has been calling for end-dates for some time now and they will force the market in to making the move. In my experience, we are now operating in a two-tiered market. There are a significant number of banks that have taken the initiative over the past few years and moved to SEPA without the threat of a deadline. These banks are also helping their corporate customers to make the necessary changes to be compliant. However, there is another tranche of the market that is adopting a more passive attitude to SEPA and approaching the project purely with its compliance hat on. In fact, some bankers still remain sceptical that SEPA can be achieved in its current form. As a result, the end-date regulation is necessary to force widespread migration to the SEPA payments instruments.

Another of Tumpel-Gurgell's resolutions was to extend the SEPA project to create a competitive cards market using an interoperable framework based on the ISO 20022 message standard. Tumpel-Gurgell believes that work on cards standardisation is still behind and has called for a more coordinated approach to global standard-setting bodies, such as the ISO and EMVCo.

In my view, there are three key points here. Firstly, the standardisation of both terminals and cards, such as point of sales or automated teller machines, will not happen overnight. The existing hardware needs to be replaced and this is no easy task. Secondly, while the application of ISO 20022 for payment authorisation requests is desirable, it is not essential. The existing ISO 8583 is already used worldwide and does not present a roadblock in the march towards SEPA. Finally, the Electronic Check Processing (EPC) should create a specific scheme or adapt an existing one for the clearing and settlement of SEPA cards payments, as proposed by the Berlin Group back in 2009.

Tumpel-Gurgell's final resolution is the break-up of the Visa/MasterCard duopoly in the European cards market and the creation of a third, preferably bank-led, scheme. Whilst several groups are continuing to push for a pan-European EMV smart card to compete with Visa and MasterCard, if the banks create a new card scheme which operates in the same way as those two and charges the same interchange fees, then it will not represent any additional benefits for consumers or merchants. In many ways, it would be better (at least for consumers and merchants) if a third scheme were created by a non-bank which could challenge the Visa/MasterCard status quo in a similar way to how China UnionPay works in Asia.

While it is clear that there is still some way to travel on this SEPA journey, I generally welcome the sentiment behind the ECB's resolutions for SEPA and believe that this will be a vital year for the project. The original vision behind SEPA in my mind is credible with a worthy end goal. However, the path leading to this goal post is still littered with issues and hurdles to overcome. If anything, Tumpel-Gurgell's five resolutions have brought some fundamental issues and debates that still remain to be had on SEPA to our attention. Hopefully the industry will address these issues head-on. Only by doing this will the market reap the benefits that SEPA has been promising for the last five years.





Interview with Karen Walsh, Head of Financial Services at Everything Everywhere

By Tom Tainton, Smartcard & Identity News



Tom Tainton

What is the Orange Cash and how does it work?

Orange Cash is a new, easy-to-use contactless Orange Cash prepaid MasterCard that allows customers to make faster payments on the high street. It enables customers to take total control of their spending and can be used in over 30 million locations within the UK and abroad. The card costs just £5 and can be loaded up to £5,000. Orange Cash prepaid cards can be loaded with money at over 22,000 shops and petrol stations, at 12,000 Post Offices, over 450 Orange Retail stores and online on the Orange Cash website - www.orange.co.uk/orangecash

We've seen Phones4u and 02 go down the same route with general spend cards – why is Orange Cash unique?

Our proposition is very different to what is already offered in the UK market place in that we are offering rewards as well as being the first in the UK to offer contactless technology on a major prepaid card. We wanted to provide our customers with the best possible prepaid offering which we believe Orange Cash delivers.

What impact do you envisage the card having for consumers?

The Orange Cash prepaid card allows customers to take total control of their spending and is a secure alternative to carrying around cash. Orange Cash customers also earn points as they spend, which are redeemable against a great range of rewards including Pay As You Go Orange texts, airtime, credit or Orange shop vouchers, which are great ways to save up for your new phone!

How secure is the Orange Cash technology?

Orange cash is a secure alternative to carrying cash. If you lose your wallet and it contains cash, you may not see the cash again. However, if you lose your Orange cash card or its stolen you will only be liable for a maximum of £50 of any loss that takes place prior to you contacting Customer Services.

In line with the process offered on other prepaid cards across the industry, if you lose your Orange Cash Card, or it is stolen, we recommend you call us as soon as possible to cancel your card. You may lose any e-money on your card in just the same way as if you lost your wallet.

It's worth noting that contactless transactions are limited to £15, and after several transactions in a short space of time, you will be asked for your PIN.

What challenges are you likely to face with take-up of Orange Cash?

Although most customers in London are used to loading up their Oyster cards, prepaid is still a relatively new concept for lots of people and it may take a while for us to raise awareness of the benefits of control and convenience it offers customers. One of the best things about the card is the contactless technology which you can only use where there are contactless terminals in use, such as Pret, Eat, and Café Nero. But as contactless payments is the hot new thing – you will see some big names going live this year – so we don't think it will be a challenge for too long!





World News In Brief

IBM Bagged \$23.6 Million E-Health Deal from Australia Government

IBM has won a \$23.6 million contract from the Australia Government's National E-Health Transition Authority (NEHTA) to design and build the National Authentication Service for Health (NASH) project. IBM will use public key infrastructure and secure tokens such as smart cards to provide an authenticated service so that healthcare personnel and providers can exchange e-health information including referrals, prescriptions and personally controlled electronic health records.

The system aims to become the first national authentication system for electronic records gathered from various health bodies. According to a statement from NEHTA, IBM will use its hardware, software and service capabilities to manage the project delivery of the system for healthcare providers. "NEHTA is providing a software development kit (SDK) that will allow existing healthcare systems and deployments to quickly and seamlessly integrate with NASH," the statement added. The programme is said to benefit over 600,000 Australian doctors, nurses and allied health providers.

According to an IBM spokesperson, the whole infrastructure project will roll out by June 30, 2012.

TazTag Unveiled First NFC Android Tablet

TazTag, the French expert in contactless technologies, has displayed its complete range of NFC products and its latest product, the TazPad, an NFC ANDROID tablet, at the CeBIT 2011, held in Hanover, Germany.

TazPad is equipped with a 7-inch colour screen that has multi-touch capacity and a full HD and HDMI output that connects via Wi-Fi, Bluetooth, NFC and ZigBee (as do all TazTag products). Other available TazPad functions include a camera, a GPS device and an accelerometer.

The TazPad, without the biometric option, can also be used at aisle end displays or store window to inform a customer about a product presented to the tablet, to compare products, or to retrieve a promotional coupon using their NFC phone. TazTag's TazPad is set to be available by Q2 2011.

Ingenico's Contactless Terminal Sales Doubled in 2010

Ingenico announced that the shipments of its contactless NFC-based terminals doubled in 2010. Since the certification in 2004 of its first contactless terminal, Ingenico successfully carried out pilot tests in different parts of the world where the company operates.

In 2010, 21% of the terminals sold to merchants were equipped with this technology, a rate up by 50% compared to 2009. The new range of Ingenico terminals integrates the contactless reader option, which is activated depending on the customer's requirements.

Sims4U in UK's Biggest Prepay SIM Card Roll-Out

Sims4U is to roll-out around 500,000 prepaid SIM cards to all 30,000 UK newsagents and 800 independent mobile dealers by the end of 2011, claiming to be the biggest SIM card distribution facility in the UK.

The Birmingham-based Sims4U customers' include newspaper and magazine wholesalers Smiths News and Menzies Distribution. Smiths News claims to deliver to 30,000 retailers across England and Wales, while Menzies Distribution claims to serve some 22,000 customers in the UK.

Before each SIM card is supplied to a shop, it is electronically registered on the same in-house tracking system used by Voice Mobile. The system lets the company track where the card is being distributed, how many a shop has in its possession, the ratio at which it is selling and when they are being connected by the agent.

Apple Rejects 'Wave and Pay' For New iPhone

Apple will not include "wave and pay" chips in the new iPhone to be released later this year, upsetting industry rumours that the Company will adopt a universal NFC standard of technology in 2011.

Sources at several of the largest mobile operators in the UK revealed Apple had disclosed in meetings that it would not be including Near Field Communication (NFC) technology, which enables payment for products with a wave of a phone on a reader, in its latest version of the iPhone - iPhone 4GS or the iPhone 5.



Get Secure, Not Security

By Richard Fine, Grid-Tools Ltd



Richard Fine

In the security world, there's a rather unfortunate asymmetry between those of us who seek to defend systems, and those who seek to attack them. The defenders need to find every potential weakness, every point of entry, in order to defend it.

The attackers need only find one.

It's an important principle, and one that is, alas, all too often forgotten, particularly in the face of shiny technology and slick pitches from security companies. "Buy our magical box," they say, "and you'll never get hacked." The company is reputable, and the magic box does what it says it will do. With the box in place, you relax: you're safe now. And then you accidentally leave your laptop on the train home. You know the laptop with all those reports and that copy of the customer database on it?

There are no silver bullet solutions to security: It's an attitude, a methodology, not a product. You don't "get security" in the way that you'd "get a faster server" - you get secure, more like the way you'd get organized or get efficient. It's a cross-cutting, pervasive concern. It can't be outsourced or delegated; you can't just leave it to 'the security department' to take care of. (That's not to say that you can't outsource or delegate the task of designing the security policy to somebody else, but you should expect them to come back with policies that affect everybody and everything within the organization, from CEOs to cleaning contractors).

Microsoft is an interesting example of the difference this approach can make. Back in 2002, a substantial problem that Microsoft faced was a reputation for security problems: exploits, viruses, malware, and so on. It's not like they weren't investing in security: there were teams dedicated to implementing security features in Windows XP, ranging from Trusted Computing Platform support to the Windows Firewall. But these weren't enough. In the first year of Windows XP's public release, 119 different security vulnerabilities were found. Craig Mundie, then CTO of the company, started a research program to find ways to improve the situation.

Unsurprisingly, the answer they found was that they needed to change their processes: they had to become secure, instead of employing some people to 'do the security bits.' Their new process was formalized in 2004 as the "Security Development Lifecycle," extending every phase of the traditional Software Development Lifecycle with the appropriate security concerns. Ensuring that developers are informed about security basics and recent trends in security and privacy is now part of the standard developer training; security and privacy risks form part of the product requirements; attack surface analysis is performed in the design phase, and so on. The extended lifecycle is mandatory process for all products that deal with sensitive data or carry meaningful business risk.

It's worked, too, to a large extent: Compared to Windows XP's first year vulnerability count of 119, Windows Vista had 66 (and I count only 26 in Windows 7's first year). More striking is the change to other products like SQL Server; SQL Server 2000, developed under the old process, had 34 vulnerabilities in its first three years, while SQL Server 2005 used the new process and had only 3.

Security is something that needs to be continually and thoroughly considered. By far the best approach is to train all your staff to do so; and if you simply must outsource the expertise, then someone from that security team should be present at every non-trivial design or decision-making meeting. At least that way you stand a chance of shipping a secure product - though it won't help you with operational security.

It's the little things that are the killers: letting a visitor connect his laptop to the company network, neither of you knowing that his machine is actually virus-infected. Transferring sensitive data from one machine to another using a USB key you just leave lying around afterwards. Handing a hard drive full of confidential data over to an infrastructure support staffer, without thinking about whether it's acceptable or legal for him to be in possession of that data. (That last one is a particularly bizarre kind of doublethink, and is worryingly common).

There are a huge number of security products out there. Many different people will tell you that their magic box is better than all the other magic boxes, that it's faster or cheaper or has more magic in it. There's a lot to learn about them all, and while they're often very useful, none of them will completely solve your problem. If, instead, you focus your attention not on the magic boxes that "do security," but on the principles and practices of how to be secure, it's a lot simpler, a lot cheaper, and a lot more effective.





World News In Brief

Visa Account Holders to Pay Each Other for the First Time

Visa Inc. announced that consumers in the U.S. will soon be able to receive and send funds to any eligible Visa credit, debit or prepaid account, anywhere in the world. The breakthrough service extends the utility of Visa's network from enabling payments at the point of sale, to enabling consumers to pay one another.

The new Visa personal payments service, which eliminates the inefficiencies of cash and cheques for payments between individuals, was made possible through technical enhancements to VisaNet, Visa's global payments processing network, and through the introduction of a new Visa transaction type that allows financial institutions to accept incoming funds.

Through the strategic product agreements, CashEdge and Fiserv will have access to VisaNet, enabling them to integrate the Visa personal payment service into their respective person-to-person platforms - Popmoney and ZashPay. This will allow a participating bank's customers to send money directly to a Visa account.

Bank Staff Arrested Over \$10 Million Fraud Conspiracy

US authorities have charged 12 people, including several bank employees, in relation to a \$10 million fraud conspiracy. Members of the network in Minnesota, California and New York are accused of buying and selling stolen identification information which was then used by other members to open fake bank and credit card accounts, apply for loans and get cash. The scam ran from 2006 until this year and saw the defendants obtain, or attempt to, well over \$10 million using thousands of stolen documents.

Among several bank employees charged is a Wells Fargo branch manager who was found with customer account information for several people at her home and in her car when arrested, according to Associated Press.

American Express, Associated Bank, Bank of America, Capital One, Guaranty Bank, JP Morgan Chase Bank, TCF Bank, US Bank, Wachovia Bank, Washington Mutual and Wells Fargo Bank were all hit by the fraud network.

Cord Blood Registry Loses Relevant Data on 300,000 Clients

The Cord Blood Registry (CBR), USA's largest stem cell bank, admitted that it lost unsecured personal data on 300,000 cord bank clients, a breach that could cost it millions to address. The data was contained on LTO4 storage tapes and a Dell E6500 laptop that were stolen from a CBR employee's car parked outside a San Francisco data centre on December 13, 2010, according to a report by Networkworld.

The lost data could have included client names, credit card numbers, driver's licence and social security numbers, according to CBR spokeswoman Kathy Engle. The data were not encrypted, she added.

The letters to clients informing them of the data breach was dated February 14, but some people have not yet received the letters. Explaining the delay, Engle said: "From the time of the incident, it took some time to determine the nature and extent of the data loss. CBR worked diligently to investigate the matter and engaged consultants with specialised expertise to help evaluate the risk to clients and retrace which clients should be contacted. This process did not conclude until late January".

Snapper Instant Payment Smartcard Launched in Auckland

Snapper has commenced an extensive roll out of its leading contactless payments system across the Auckland Super City, bringing New Zealand's fastest way to pay within everyday reach of 1.5 million New Zealanders.

Snapper offers customers integrated ticketing and instant everyday payments. The Snapper system is 99.99% accurate, providing valuable journey data that can be used to plan better transport services for passengers

Snapper CEO Miki Szikszai says, "Snapper is excited to bring the magic way to pay to a third of New Zealand's population". The new contactless payments mode can be used in 1,000 taxis, and over 150 retail points of presence.

