August 2011

Volume 20 • Number 8

Smart Card & Identity News

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

www.smartcard.co.uk

6 • *Contactless paper tickets for global sustainable events*

9 • *De-scoping the contact centre and ecommerce payment environments*

15 • *3-D Secure: Friend or foe?*

18 • **Better by Far...**

The BlackBerry Riots

London and other parts of the UK were ravaged by community protests in August that overnight turned into what can only be viewed as the worst riots in living memory. It is not for us to analyse the cause of these riots but only to look at the technology that many have cited as the catalyst for the extent of these riots. It has been suggested by many that core to this technology is the RIM BlackBerry mobile phones that allow messages between users to be encrypted thereby enabling people to be incited to action in a collective way that cannot be easily monitored by the appropriate authorities. We will ignore for this discussion other technologies such as Twitter and FaceBook that were also clearly used during these riots.

So the question is can people communicate with their Blackberry mobile phones in a way that cannot be monitored by the regulators? There are three concepts we need to understand in order to answer this question,

1) The Blackberry Messenger service (BBM)
2) The Blackberry Internet Service (BIS)
3) The Blackberry Enterprise Service (BES)

Continued on page 4….

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

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

Telephone: +44 (0) 1903 734677

Fax: +44 (0) 1903 734318

Website: www.smartcard.co.uk

Email: info@smartcard.co.uk

Editorial

Researcher– Patsy Everett

Technical Researcher – Dr David Everett

Production Team - John Owen, Lesley Dann.

Contributors to this Issue – Dr.David Everett, Claire Boyer, Robin Adams, Martin Kuschewski, Sascha Breite, Peter Tomlinson.

Photographic Images - Dreamstime.com

Printers – Hastings Printing Company Limited, UK

ISSN – 1755-1021

Disclaimer

Our Comments

Patsy Everett

Dear Subscribers,

Just back from a great holiday in the Scilly Isles and somehow or other we managed to get superb weather which is not usually the case in August. However even on holiday one can't help think about the job and this month it was all about the value of references and identity.

The inquest after the event is always interesting, the hotel was not really as we expected. Doing the reviews on Trip Advisor it came out as number one while we would have put it somewhat lower. But now here's the thing, references are only relevant to people in the same population and the particular population is probably not random but heavily associated with the attributes of the target, in this case the hotel. And you may not realize or be associated with that group.

You are probably wondering what was going on in that hotel but let me put your mind at rest or perhaps engage you in a little disappointment. We were surrounded by a large group of walkers who quite clearly had different expectations to us and as one suspects all the other walkers who have previously given references on the hotel. The sign on the door should have given it away - 'All ye who enter here please take off your walking shoes'. Now it's not that I don't like walking it's just not the priority, exploring to see new things yes but burning up the miles of the coastline for the sake of it no. Our discussion at the dinner table was much more focussed on what we had seen rather than how far we had walked. Although I must confess on occasions we were engaged in discussing some of the strange and not always pleasant things we found on the ground.

Just a little diversion here for my friends, on the Scillies you can hire a golfing cart registered for use on the roads. Oh what excitement is that, careering along narrow country roads at 20 miles an hour with not a care in the world.

But this observation about references led us into thinking even more about what do references mean and of course how does identity fit in with all that.

In some cases it works really well, take Amazon for example, when I read the reviews on a book they are generally a fair reflection of what I find later, on the assumption that I buy the book. This is I believe because the population is in fact a relatively close community because people interested in a particular book are by default related in a common interest. People visiting a hotel are more randomly distributed and can be totally misled by the references, as they say one man's meat is another man's poison.

So the point I'm trying to make is that a reference only has value to people within the same community and you may not be able to readily recognize that community.

Which leads me nicely into identity and whether a persona has to be associated with an individual? So at the hotel we may get to meet new friends and have absolutely no idea of their day to day existence, what we see is what they present to us at that hotel. It could be total fiction, fantasy, whatever and the thing is does it really matter?

When you meet somebody you are by default going to class them as members of some community and then you will score them accordingly. You can see where all this is going, I'm thinking about the internet. Forget the dog but if somebody has good references in a particular community do I actually care about the individual behind it? So take for example the perv who is lurking in chat rooms of young people pretending to be part of that community, would they get good references? Perhaps they would because until they come out of the closet they may well seamlessly blend in and be trusted by the other members of the community.

What this says to me is that a pseudo identity doesn't work, if you are anonymous then you can't be trusted and that an individual has to have a single reference which can be verified. Dear friends I've got to the same place again, a chip in the ear at birth!

Patsy.

Contents

Regular Features

Industry Articles

Events Diary

September 2011

27-29	Biometric Consortium Conference, Tampa, Florida, USA - http://www.biometrics.org/
19-21	NFC World Congress, Sophia Antipolis, France - http://www.nfcworldcongress.com
21-23	Smart Event 2011, Sophia Antipolis, France – http:// www.smart-event.eu
28-30	Cards and Payments Conference, Paris, France - http://www.equens.com/aboutus/events/efma.jsp

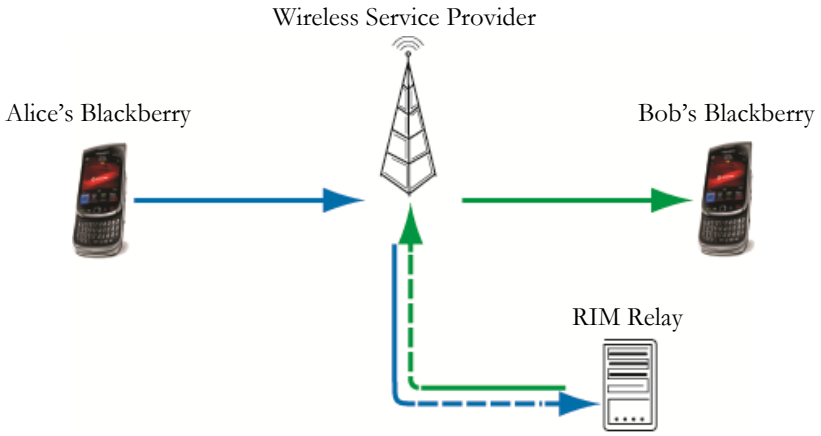
October 2011

11-13	NFC Mobile Payments Forum 2011, Beijing, China - www.nfc-mobilepayments.com
11-13	RSA Conference, London, UK - www.rsaconference.com/2011/europe/about.htm
12-13	Mobile Payments, London, UK - www.smi-online.co.uk/mobilepayments27.asp

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

The BlackBerry Riots …. Continued from page 1

The BlackBerry Messenger Service is something that RIM are very proud of because it provides a flexible instant messaging service to users that does not incur any additional charges like SMS assuming of course that the consumer has a Blackberry data service with their Network Operator. Such data services are usually much cheaper than the full internet services attached to other smart phone contracts such as the iPhone. It is based on the RIM PIN to PIN instant messaging service. Every Blackberry phone has a PIN identifier, this is not a security access device but purely a reference identity for that BlackBerry phone. What this means is that one BlackBerry user can send messages to another if they know the PIN of their correspondent's Blackberry device. Equally the service allows users to set up groups by storing a set of PINs so that they can broadcast messages to the group.



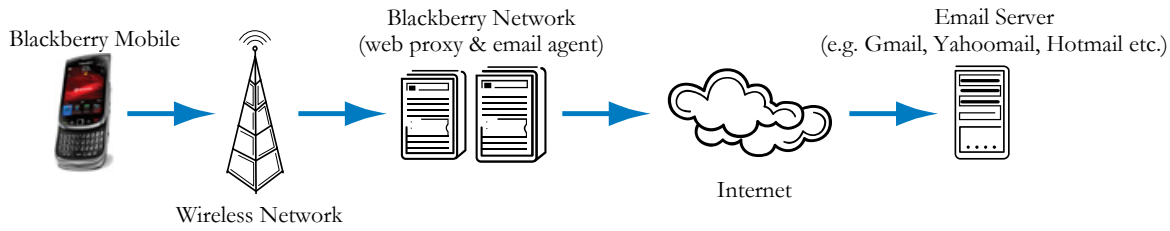
The BBM message goes from the originator's BlackBerry phone through the connected mobile network to the local (or nearest wherever that might be) RIM relay Server. The RIM relay server knows where the BlackBerry phone of the receiver(s) is located and passes the message to the relevant wireless network(s).
These messages are encrypted using Triple DES but with a system wide global key in every phone. RIM does not disguise this fact and tells people that they should look on the security of the BBM service as more akin to scrambling than encryption. I must confess the logic of this terminology escapes me but what we might assume is that one day this global key will become public knowledge and then you might argue that the security property of confidentiality has been breached. However for the moment if the authorities want to decode BBM messages then they can,

1. Use a captured phone that is in the broadcast group of PINs (is this legal?). Please also note that this PIN remains the same for the life of the phone, so if you pass it on the new owner might get some unintended BBM messages.
2. Intercept the relevant BBM message and get a BlackBerry phone to decrypt them (there is no check on the PIN correctness)
3. Issue a legal request to RIM to provide either the Global Key or a copy of the decoded message which has passed through the RIM relay.

The BIS and BES services are the way that eMail messages work on the RIM network. BIS is intended for non corporate users while BES is for the corporate which was the original target for RIM's marketing of the BlackBerry phone.

How BIS works:
On setup, the mobile phone user provides BlackBerry (RIM) with the email addresses, connection details & credentials for each email account he/she would like to receive on their mobile phone. BlackBerry currently allows up to 10 sets of Email credentials.

BlackBerry uses the details provided to login and establish a connection on the user's behalf to their Email server's mailbox. BlackBerry monitors the mailboxes, and when it sees new Email, it retrieves (pulls) a copy and then pushes it to the BlackBerry handheld device over the wireless network.



Encryption is used on data travelling between each entity. The wireless network will typically use one of GSM's family of A5 stream ciphers and if configured, BlackBerry will use a SSL session over the Internet to the E-mail server.

Although Encryption is used, it is under the control of the Network operators. BlackBerry applies compression and optimization making Email little more secure than SMS messaging. BlackBerry's official line is: "Email messages and instant messages that are sent between the BlackBerry Internet Service and your BlackBerry device use the security features of the wireless network. Messages that are sent between your messaging server and the BlackBerry Internet Service are automatically encrypted if the server supports SSL encryption."

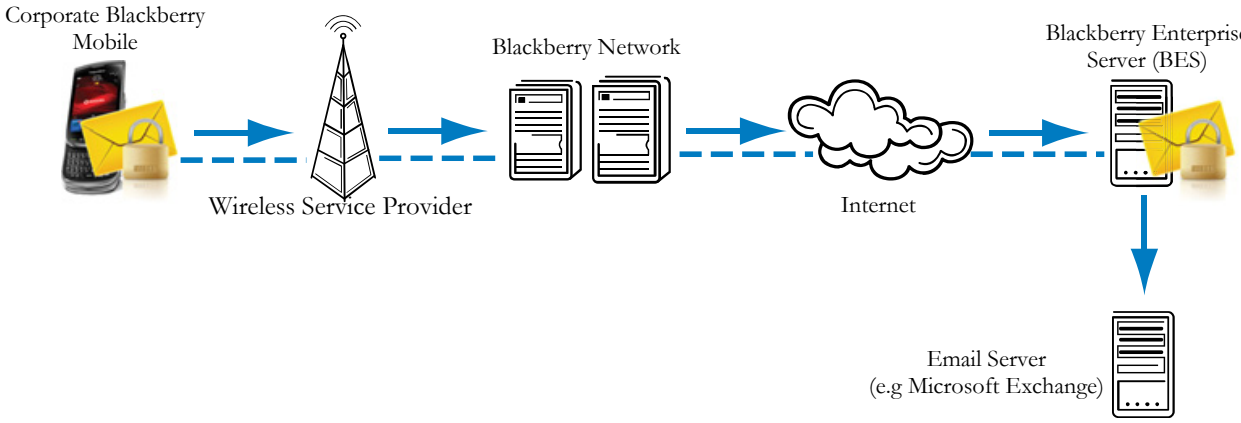
How BES works:

First you must have a BlackBerry phone from the carrier on a business plan. The carrier will often lock-out the BES setup icon from a phone on a personal plan.

In this scenario the BlackBerry mobile phone user will often receive his/her phone from their company. The user is provided an activation password by the companies IT department. The next step is to launch the enterprise activation program on the BlackBerry phone and provide the activation password. The password is used to ensure the phone user is authentic and then the Enterprise Server and BlackBerry device negotiate a device transport key using following the Diffie-Hellman key agreement protocol.

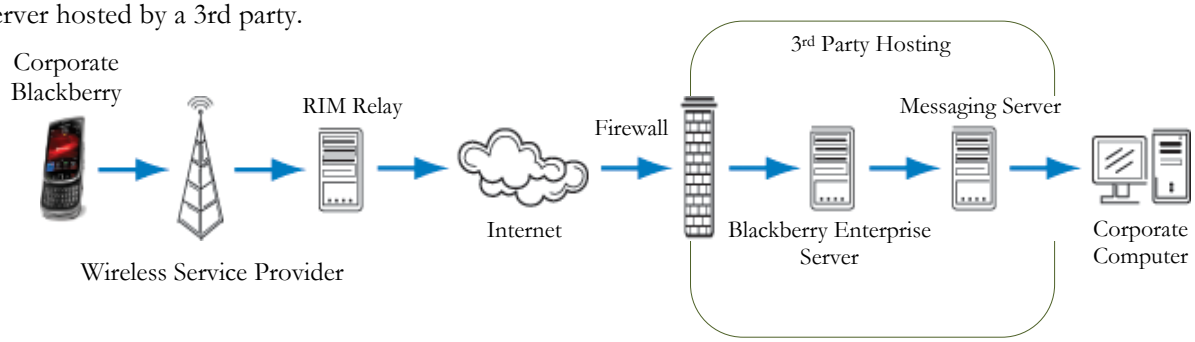
So here we have it,

The RIM BlackBerry Messenger Service is based on the use of a Global key for Triple DES encryption where RIM can easily decode the messages, The BlackBerry Internet Service for eMail is based on the standard encryption algorithms used by the mobile network operators which the Network Operators can easily decode while the Blackberry Enterprise Service for eMail uses AES or Triple DES encryption entirely under the control of the corporate who can decode the messages as required.



The device transport key is held on both the device and server, used to encrypt subsequent communication traffic (Application, Email & Messaging and Voice using additional BlackBerry Mobile Voice Server) using either Triple DES or AES encryption algorithms.

One final note worth mentioning regarding the BES solution is that it is possible to pay to have your BES server hosted by a 3rd party.



Contactless Paper Tickets for Global Sustainable Events: when marketing goes along with security

By Claire Boyer, Corporate Communication manager, ASK

Claire Boyer

When worldwide events have truly become international, they have also turned into the opportunity to showcase high technology to the world, enhance the image of the event's location (country, region, city) and offer new marketing tools to the organizer. Contactless paper tickets are the perfect medium to meet these requirements, secure access and prevent counterfeiting to make organizers and visitors enjoy all contactless technology benefits.

Contactless technology benefits make it all

Contactless technology is now the de facto standard for all mass transit ticketing system and contactless paper tickets are now part of full interoperable and multimodal schemes as well. In events where large gatherings and cash handling are the main two issues, contactless paper tickets are the ideal medium to solve them. Football games, the Olympics, concerts and festivals, international exhibitions are all instances where long queuing time and cash handling are constraints to take into account and RFID is the answer.

Indeed, an RFID chip embedded in a ticket is by far the most secure anti-counterfeit device.

In large international events such as Beijing 2008 Olympic Games and the current 2011 Xi'an International Horticultural exhibition, the chip with a small memory size held a unique serial number with no other private information. If the anti pass-back protocol is activated, it prevents duplicate use of the same ticket for 2 attendees at the same entry point. The solution will detect that access has already occurred and will deny a second access.

As it is a read/write chip, the ticket can be personalized for a specific time period with any useful information and grant access to restricted areas, specific gates or other access points and of course manage VIP access. Customized tickets with various layouts or personalization can be purchased.

While throughput increases at every gate of the event, reducing queues, staffing costs decrease and useful reports can be generated to manage the flow of visitors and streamline future events.

Contactless paper tickets are no doubt the ticket to use for all large events and shows, to improve logistics and security on a whole, convey the image of a modern, high tech organizer and location, whether they be a concert hall, a stadium or an outside exhibition.

In the case of large events, where millions of visitors are expected, sustainable development is of essence for the hosting country and city. The selected ticketing solution must be part of this policy and offer recyclable, eco-friendly products. ASK C.ticket® based on silver ink antennas and paper inlays are environment friendly and manufactured with biodegradable and recycling raw materials.

But the ultimate solution for both the organizer and the visitors is to turn **the** ticket into an artful object and make it a souvenir and reminder of a great moment spent together with family or friends.

A marketing tool for the organizer and a collectible medium for the visitor

Contactless paper tickets have been used for years in mass transit and multi-application. In Firenze, Italy, beautiful ASK special edition tickets have been used for public transport, with various sponsors over the years, including Botticelli artworks during a temporary exhibition. In Torino, ASK C.ticket® was launched during the 2006 Winter Olympics with multi-application tickets, granting access to public transport and museums for a limited period of time.

2008 Beijing Olympics: 1st global event to use RFID on a large scale

On August 08, 2008 were launched the Beijing Olympic games, the 1st global event to use RFID tickets on a large scale.
The country wanted to show the world its willingness to lead an active environmental policy making the Games "green Olympics". Therefore, the 14 million ASK C.ticket® had to fit the Beijing Organizing Committee for the Games (BOCOG) policy. The tickets, customized with visual security features by the Bank of China, have been designed in 6 different layouts for the Olympics and Para-Olympics. The red opening ceremony tickets feature the symbolic Bird's Nest Beijing National stadium.

Entertainment tickets delivered for large one shot events are limited edition tickets and become even more valuable when designed for a special day within the event (opening ceremony, preview admission etc.). Manufactured by millions they remain unique and a strong symbol of attending a Once-in-a-Lifetime event for most attendees. Therefore, they are both a technology showcase and a powerful marketing tool, enhancing the high tech image of the country's or city's hosting and usually boosting the local economy during and after the event.

2011 International Horticultural exhibition: technology and creativity at work

The International Horticultural Exhibition started on April 28th and will close on October 22nd, 2011. It is being held in Xi'an, in the Chan-Ba Ecological District. The city of Xi'an is well-known for its collection of terracotta sculptures depicting the armies of Qin Shi Huang, the first Emperor of China and will now be remembered as a hosting city for this beautiful exhibition.

ASK 7.5 million tickets have been personalized by the Bank of China with specific security features (microtext, UV, embossing, specific color patterns…) turning the tickets into a real technology showcase. If the RFID chip is no doubt the most secure anti-counterfeit device of the ticket, attendees recognize visual security printing features they are used to observing on their banknotes, credit cards or check books. This increases the intrinsic value of the ticket, giving a feeling of enhanced security and aesthetics so that visitors will eventually keep it as a souvenir and will not throw it away as it is usually done with regular bland paper tickets.

The Chang'an Tower, an observation tower, is the symbol of the exhibition and is printed on the various layouts of the tickets. It is a reflection of both the essence of Chinese architectural culture and modern, trendy urban features. The peak-day ticket holds the most colorful artwork and is to be used for 22 special days during the whole duration of the Xi'an expo.

So during your summer, if you want to enjoy art and high technology at the same time and pay a tribute to the 418 hectares of worldwide gardens, waterfalls and flowers, go to Xi'an!

Event ticketing is a different business case from mass transit ticketing. It allows for more expansive tickets since they will ultimately be sold with a higher purchase price to visitors and attendants. Contactless paper tickets can turn into powerful marketing devices thanks to highly sophisticated printing features usually meant for the banking sector. Different artworks and chip personalization can target specific groups of visitors. ASK, the inventor of contactless paper tickets, have delivered over 120 million C.ticket® for mass transit and event ticketing worldwide. So if you or your client wants to enhance the event through your ticketing system and make cost savings thanks to anti-counterfeit media, seamless traffic, optimized staffing, go for contactless paper tickets!

World News In Brief

NXP Consolidates No. 1 Position in Worldwide ID Market

NXP Semiconductors N.V. has extended its lead in the global Identification market, after eight quarters of consecutive growth in total sales across all market segments using Identification technologies.

In 2010, NXP's Identification business unit posted global revenues of $589 million across its three product lines Secure Transactions, Secure Identity, and Tagging & Authentication, attaining the No.1 position in the worldwide ID market. In H1 2011, NXP reported revenues of $383 million in Identification, firmly establishing its No. 1 position with recently announced Q2 revenues of $194 million.

"ABI Research believes NXP is uniquely positioned and differentiated from its peers in that the company supports the full range of RFID frequencies from LF to HF to UHF," said Mike Liard, research director for RFID at ABI Research. "Primary applications supported by NXP's transponder ICs are broad and far-reaching, including automobile immobilizers, security/access control, contactless payment, ticketing, NFC, government ID, asset management, item-level tracking, authentication and many others.

Global EPOS Market on Path to Recovery

The global EPOS (electronic point of sale) market is recovering from the recessionary environment of 2008 and 2009, according to new research by London-based strategic research and consulting firm RBR. The number of programmable EPOS terminals shipped worldwide increased by 11% in 2010 to 1.38 million, and the total installed base of terminals reached 10 million.

Despite a pick-up in EPOS shipments in 2010, the challenging economic climate is leading some retailers and hospitality operators to operate their EPOS terminals for longer than usual before replacement. Furthermore, new installation activity remains generally subdued.

RBR forecasts that global EPOS shipments will increase by 14% in 2011 and 12% in 2012, as retailers and hospitality operators resume replacement and new installation activity. Growth will then continue at a slower rate until 2015 and 2016, when the market downturn of 2008-2010 will cause a fall in shipments, as fewer machines will need replacement.

First Fingerprint-enabled NFC Payment Transaction Completed in the U.S.

NXP Semiconductors, AuthenTec and DeviceFidelity, Inc., announce they are jointly developing reference designs that enable highly secure mobile payments via Android-based phones through the use of fingerprint biometrics and near field communication (NFC) technology.

The companies recently collaborated to complete the first biometrically-enabled NFC mobile payment transaction in the U.S. The successful transaction was made possible via a Motorola ATRIX 4G smartphone equipped with AuthenTec's AES1750 smart fingerprint sensor and DeviceFidelity's In2Pay microSD card based on NXP's secure NFC solution. The mobile payment was conducted when the demonstrator swiped a finger over the Smartphone's fingerprint sensor, authenticating him as the pre-enrolled account owner and launching a credit card app. Following authentication the user simply tapped the ATRIX smartphone against a payment terminal to complete the first fingerprint-enabled, secure NFC transaction in the U.S.

VeriFone Completes Acquisition of Hypercom Corporation

VeriFone Systems, Inc. announced this month the completion of its acquisition of Hypercom Corporation. In connection with the closing, VeriFone and Hypercom reached a settlement with the U.S. Department of Justice, following which Hypercom divested its U.S. payment systems business to The Gores Group, LLC.

"This strategic acquisition complements VeriFone's position as a trusted, worldwide leader of the electronic payment industry," said VeriFone CEO Douglas G. Bergeron.

VeriFone expects the acquired Hypercom business to contribute in fiscal year 2012 non-GAAP revenue of $350 million.

De-scoping the Contact Centre and eCommerce Payment Environments

By Robin Adams, Director of Security, Fraud and Risk Management at The Logic Group

Robin Adams

Merchants are discovering new ways to cut costs and risk in card transactions by taking their payment environment, particularly contact centres and web servers, out of scope for PCI DSS.

Introduction

The cost of keeping cardholder data secure is steadily increasing. IT research firm Gartner reported that merchant spending to protect cardholder data and become PCI DSS (Payment Card Industry Data Security Standard) compliant increased by almost five times during the previous 18 months.

Researchers found that Level 1 retailers (those with more than 6 million transactions per year) spent an average of £1.8m, excluding the costs of PCI assessment services. Even Level 3 merchants (20,000-1m transactions per year) spent an average of £103,000, excluding security assessment.

Costs are set to increase further for many with the announcement that MasterCard now requires all Level 2 merchants to have either an external audit through a qualified QSA (Qualified Security Advisor), or that their internal auditors pass PCI Internal Security Assessor (ISA) training and maintain their accreditation annually, before completing the Self Assessment Questionnaire (SAQ).

The rising cost of PCI compliance means that merchants are increasingly finding it more cost-effective to eliminate customer card data from their infrastructure altogether, thereby reducing the scope of PCI DSS.

Recent innovations in the areas of ecommerce and call centres have been successful in leading this scope reduction. In the area of contact centres, it is key that efforts are centred on securing voice transactions so that a de-scoping strategy can be applied to contact centres and phone orders.

There's a range of ecommerce payment solutions available that include de-scoping a merchant's web server from scope. By removing all card data from these environments there's no risk of internal card fraud and its potential damage to brand reputation.

PCI DSS guidelines

PCI DSS is a worldwide information security standard defined by the Payment Card Industry Security Standards Council. It was created to help prevent card fraud and applies to all organisations that store, process or transmit cardholder information, from any card branded with the logo of one of the member card schemes (Visa, MasterCard, American Express, Discover and JCB).

Within the PCI DSS annual assessments there are five Validation Types that dictate which SAQ the merchant has to complete. Each SAQ has a set number of controls which the merchant is obliged to meet.

Organisations are expected to meet a variety of security criteria depending on the size and complexity of their systems. Call centres may be subject to as many as 222 separate control criteria, but using a hosted, PCI compliant secure payments solution can dramatically reduce the amount of controls they're required to fulfil, and so cut costs and administration.

By reducing the scope of the PCI audit from an SAQ Validation Type 5 (SAQ D) to Type 4 (SAQ C) it is possible to reduce the PCI compliance and audit costs by more than 75 per cent. For merchants with no customer-facing transactions that can de-scope to an SAQ Validation Type 1 (SAQ A), the reduction in cost is closer to 90 per cent.

Substituting card data

It is rare that cardholder data can be totally eliminated as it is required for refunds, loyalty programmes etc, so merchants focus on substituting their stored card data or rendering it useless. The two most common methods of doing this are:

- Point-to-point encryption – data is securely encrypted between two end points
- Tokenization – substitution of non-sensitive data which can be used as an identifier

These systems can be used on their own or together, often with just the last four digits of the credit card number (which doesn't require encryption) visible. However, the nature of contact centres introduces some additional problems for compliance.

Contact centres

Shops can use chip and PIN machines, online transactions can use secure, fully automated systems, but the presence of an agent speaking to a customer by phone in a contact centre means additional security challenges requiring that the contact centre is physically secure, and that calls have to be recorded.

Securing the physical environment of the contact centre can mean drastic measures such as controlling writing materials and access to email, banning mobile phones and limiting personal effects, all of which can lead to a difficult working atmosphere.

The fact that calls have to be recorded poses another problem, since the cardholder data within the recordings needs to be rendered useless. This is often done by agents physically stopping the recording at key moments, a system that is prone to human error and can lead to organisations falling foul of regulations if the wrong parts of the call are erased. And since agents typically input cardholder data into a computer system, their actual machines also fall within scope of PCI DSS compliance.

Because of the cost and complexity of making contact centres secure, many firms are now finding it is more cost-effective, with less potential risk, to take their contact centres out of scope for PCI DSS wherever possible.

One method for taking cardholder data out of scope for PCI DSS is a software-based solution, which shields all credit card data from agents, call recordings and screen recordings. Agents do not hear or see the cardholder's data, call recordings do not capture it, and screen recordings only capture asterisks and the last four digits of the credit card number.

Agents don't ask cardholders to speak their card details, they ask them to use their telephone keypad to enter the numbers. Crucially, the system will mask the DTMF (Dual Tone Multi-Frequency) tones from the cardholder's telephone and replaces them with a flat tone so that they cannot be identified. While this is happening, voice communications remain intact between the agent and the cardholder, maintaining the 'personal touch'.

The agent can then call up the "pay page" of a Payment Service Provider (PSP) and pass across the cardholder name, transaction reference, amount and any other payment details required for payment authorization. The agent will only see masked data on their computer screen as the cardholder enters their card data.

Once the transaction details have been collected, the agent requests the transaction authorization and the details from the online payment page are combined with the masked payment card numbers.

The PSP then returns the results of the authorization including the authorization code and the transaction token, which can be displayed by the Semafone hosted page or can be posted back to the agent application.

The solution is compatible with virtually any existing computer and phone systems and can be installed with very little disruption. The simplicity of the system also makes it extremely easy for staff to use and it can often cut down on the time spent processing transactions.

Through capturing or routing card data, the solution will now be in scope for PCI DSS, but by segregating the contact centre by firewalls, the contact centre environment may be de-scoped. Compliance levels can be further reduced by deploying a secure payments solution within the telephony cloud of the merchant's network provider rather than within the enterprise itself, in which case the merchant is deemed to have outsourced its voice based payment processing for PCI DSS purposes.

This solution, providing secure telephone call recording functionality, has been integrated into The Logic Group's next generation secure payment platform. This provides hosted payment pages as well as direct integration technologies for contact centre environments for secure payment processing.

At the point of taking a payment, the payment technology will automatically block the dial tones from both the agent and call recording system, passing the payment details directly to the PSP. Combined with a tokenisation capability, merchants can eliminate the risk of fraud to their organisation and to the end customer, as payment information is neither heard by the agent nor stored by the business.

Conclusion

As the cost of PCI DSS compliance continues to rise, merchants are increasingly looking for ways to avoid managing cardholder data internally. Merging secure voice and data transactions together for card payments permits the merchant to achieve this for contact centres and ecommerce.

By taking these environments out of scope for PCI DSS, these solutions will dramatically ease the compliance burden for merchants, whatever their size, and help them to cut costs, meet their compliance objectives and reduce the risk of potential fraud.

World News In Brief

UnionPay overtakes Visa to Become World's Largest Card Scheme

The results of Retail Banking Research's (RBR) latest global payment cards research provide remarkable reading. Several findings stand out, including surpassing a phenomenal eight billion cards worldwide, a fall in the number of cards in North America and more than 10% growth in the prepaid and debit card sectors. The most startling finding however is that China's UnionPay is now the largest payment card scheme in the world, its brand appearing on three in every ten cards worldwide.

Executives at Visa, the scheme that has been usurped at the top of the rankings, can console themselves with the news that cards with their branding are still well ahead in terms of usage and spending, and the fact that most UnionPay cards are found in China.

The new RBR research shows that there is still plenty to play for, with 20% of cards worldwide belonging to domestic bank card or private label schemes. This share is falling however, so competition for these cards plus efforts to persuade large issuers to change their scheme allegiances will only intensify.

One in Three Gamers Has Used "Real World" Money to Purchase Virtual Content

U.S. Gamers, whose online purchases of digital goods were once paid for largely by credits earned from advertiser offers, now say they are migrating to "real world" payment for digital goods using debit, credit and prepaid cards, according to a new study of online gamer behaviour commissioned by PlaySpan, and undertaken by research firm VGMarket.

According to the study, nearly one-third (31 percent) of the general gamer population has used real world money to purchase virtual content. Of those gamers who use real world money, 57 percent said they make purchases of virtual items using real world money at least once every month. Console games with online play account for the majority (51 percent) of virtual purchases using real world money, with social networking games (30 percent) and Massively Multiplayer Online Games (MMOs) coming in at second and third respectively.

Overall, 72 percent of respondents indicated they expect to spend the same or more money on games in 2011 as they did in 2010. 67 percent of those who intend to spend more said they were playing more online games than last year, with 42 percent saying they have more money to spend. 32 percent claimed ease of purchase as the main reason, while greater in-game rewards (30 percent) were the fourth most popular reason.

The survey data was compiled in July 2011 from over 1000 gamers drawn from a VGMarket database.

HTC Radar: Mango Detected

HTC is expanding its range to incorporate the long-awaited software update from Microsoft. The HTC Radar is one of the company's first to showcase the new Windows Phone 7 operating system

The chassis of the Radar is typical of HTC; the unibody design that we first encountered on the original HD Windows efforts is back, meaning there's only a small panel on the bottom of the rear that's removable and no microSD slot.

It's fair to say that the Windows operating system was never as well received as Microsoft would have hoped, and despite churning out iteration after iteration, the platform always languished behind the likes of Android and iOS. At least until Windows Phone 7 arrived.

Microsoft has brought a raft of improvements to the software including better multitasking, an improved Hub system and Internet Explorer 9. The IE9 update brings hardware accelerated graphics and HTML5 support and has also undergone various superficial changes, one of which sees the address bar move to the foot of the screen which makes one-handed web surfing far easier.

In a bid to keep the Windows experience as pure as possible Microsoft has banned manufacturers from including their own skin. HTC has attempted to get round this by including the best bits from its Sense UI in something called the HTC Hub – behind this tile lies regular Sense features such as news, stocks and weather.

The HTC Radar comes with a Qualcomm MSM 8255 1GHz single-core CPU.

Safeguarding the Integrity Lifetime of ID Documents

By Martin Kuschewski, Smartrac Technolgy Group

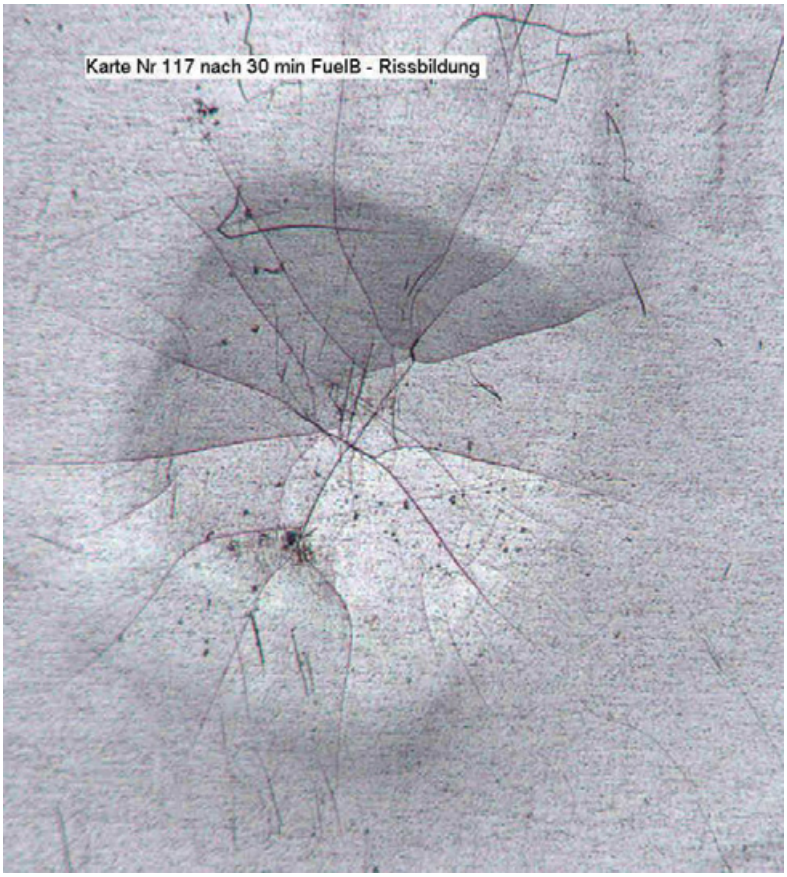
Martin Kuschewski

Assuring that a person in fact is the one he or she claims to be has engaged people and authorities for centuries. Issuance of identity documents can be traced back to the Middle Ages. Over the years, security printers have gained in-depth knowledge and have developed ever sophisticated mechanisms to protect identity documents. Watermarks, special paper, security ink, and optical security features safeguard documents from tampering, forgery, and counterfeiting, especially when used in combination.

The next evolutionary step was the combination of physical security mechanisms with electronic security features. Introduction of electronic passports started some ten years ago combining the paper document with electronic data stored on a chip. Today, governments around the globe upgrade more and more identity documents to the state-of-the-art standard which is a plastic-based smartcard in ID-1 format with an integrated chip.

RFID-based identity cards combine several advantages. One of the key benefits for governments and citizens alike is the fact that contactless identity cards can be seamlessly integrated into the existing e-passport infrastructure thereby reducing the necessary investment to a minimum and paying off for all parties involved. Due to their robustness and resistibility, they are much less prone to environmental conditions like humidity and dirt. Usage of contactless technology therefore enables a longer lifetime and trouble-free functionality of identity documents compared with their pure paper-based predecessors. Manufactured without contact area for data transmission, the latest generation of e-ID Cards also offers more space for the printing of personal information or visual security features including watermarks, photos and the like. In addition, contactless chips have made steady progress over the last years in terms of functionality and security and are today able to process all necessary security requirements including authentication, sophisticated encryption, and Public Key Infrastructure (PKI) operations.

RFID-based identity cards today are typically made of polycarbonate (PC). The material is widely used and has proven its durability in other application fields since several years. Manufacturing electronic identity cards based on polycarbonate however reveals a weakness of the material: Continuous mechanical stress can cause so called “micro cracks” around the chip module inside of the card body. As a result, the structure of the card body might break up in the course of time. This weakness is not only suited to cause temporary dysfunction, it might also lead to the fact that ID documents have to be replaced resulting in additional costs and annoyance for the citizen.



As this circumstance has been realized at an early stage of the introduction of RFID-based identity cards, smartcard manufacturers are able to address the material weakness with suitable contactless card inlays. RFID transponder manufacturers like SMARTRAC support card manufacturers with both consulting services and specific products to avoid failure of PC-based contactless identity documents in the field. SMARTRAC has invented a PC card inlay which is equipped with a so called "anti-crack-feature", the so called SMART-AC. Specific methods during the card inlay manufacturing process prevent that micro cracks are able to spread inside the card body. Various tests with finished contactless smartcards according to very strict criteria have shown that this specific technological approach shows significant differences to conventionally manufactured contactless card inlays. The result is a product which combines mechanical robustness with the benefits of polycarbonate-based contactless smartcards.

Based on today's technical capabilities and steady progress of technologies to manufacture high-quality and highly secure identity documents which are comprised of various "layers" of security, namely physical, logical, and digital functionalities, citizens today have identity documents on hand which are highly reliable, durable, and accepted as proof of identity worldwide.

World News In Brief

Level Four Software supports ATM updates mandated by American Disability Act

Level Four Software today confirms that by January 2012, its BRIDGE:test product will enable financial institutions and ATM deployers, to conduct fully automated end to end testing of new voice guidance functionality at the ATM. This critical step will help banks to ensure their ATM network meets new legal requirements from the American Disability Act (ADA) which come into force in March 2012.

After conducting extensive research and development immediately following the government ruling, Level Four is now creating the required updates to its Regression Test Manager product in BRIDGE:test.

Last month the U.S. Department of Justice issued a final ruling on new accessibility standards under the Americans with Disabilities Act (ADA). This ruling imposes new standards around ATM accessibility. It includes requirements on voice guidance, height and reach, layout and touch of keypad, screen visibility and Braille instructions.

All ATMs in the United States must become speech-enabled by March 15th 2012 in order to provide visually-impaired individuals with access to all services offered at the ATM.

Ian Kerr, CEO of Level Four, said: "The ADA ruling is a significant challenge for ATM deployers. To meet this deadline, updates to ATM terminals and software will be required. Especially in the case of voice guidance, these updates will need extensive testing so that errors and glitches between screen flows and voice commands do not occur. Left untested, such errors are not only costly to repair but can leave the bank open to non-conformity issues with the standards and also cause reputation damage when a customer encounters an ATM that is unusable."

Raytheon seeks 500 Million-Pounds in Compensation after being Dropped from UK e-Boarders Programme

In a letter to the Chairman of the Home Affairs Committee Raytheon is demanding 500 million-pounds compensation after the government terminated its contract in July 2010 over poor performance.

In the letter Robert Delorge Raytheon's UK CEO states "We maintain that the purported termination was unlawful and that Raytheon are entitled to recover substantial damages for the wrongful termination. We have made counterclaims in the arbitration in excess of 500 million in respect of these matters."

Immigration minister Damian Green told MPs at the time of the contract termination "Elements had not arrived on time, the next critical parts were running 12 months late, with the risk of further delays, and there is no confidence in the current prime supplier to be able to address this situation,"

Raytheon was awarded the 650 million-pound contact after beating a rival bid from BT Group PLC's 'BT Emblem' group in November 2007.

Diebold Unveils Prototype for World's First Virtualized ATM

Diebold has developed a virtualized ATM prototype in collaboration with VMware. Virtualization of the self-service channel removes the onboard computer from the ATM, tying each terminal in a fleet to a centralised computing resource. In this scenario, the physical components of a single server provide resources to many "virtual" ATMs. The result is not only the consolidation and sharing of resources throughout a self-service network, but also across delivery channels, opening the door for more effective channel orchestration.

M6 Toll Becomes the UK's First Contactless Payment Toll Road

M6 Toll operator, Midland Expressway, has partnered with CreditCall and Barclaycard, becoming the first toll road in the UK to enable drivers pay for their journeys by tapping their contactless cards on new readers installed at the Toll lanes.

With MasterCard and Visa concentrating on increasing usage of contactless technology countrywide, the joint effort between Barclaycard, M6 Toll and CreditCall is not only the UK's first contactless project within transportation but also the biggest outside London.

CreditCall is providing on-site transaction servers connecting with the contactless card readers at each of the toll lanes over a secure network, sending transactions back to the CreditCall network for settlement. The whole process will operate within the scope of PCI DSS (Payment Card Industry Data Security Standard).

Contactless payments will initially be trialled from autumn 2011, rolling the technology out across all M6 card-accepting toll booths in the first quarter of 2012 ahead of time for the London 2012 Olympics. The new contactless technology will allow convenient and quick payments to be made by M6Toll customers, at the toll booths.

Oberthur Smart Card Sell Off Takes a Step Nearer

Oberthur is in the final stages of an auction to sell large chunks of its business to private equity bidders, in a move that analysts said would provide the French group with fire power to eventually re-launch its bid for troubled UK banknote printer De La Rue according to a report in the Financial Times.

In December last year Oberthur made an 896 million-pound cash offer ($1.4 billion) for De La Rue, which was rejected. In January De La Rue asked the regulator to impose a deadline (February 7th) for Oberthur to make its intentions clear, under a so-called 'Put up or shut up deadline'. After this date Oberthur would be unable to make another attempt to buy the printer for a further 6 months under U.K. takeover rules.

This month Advent International and One Equity Partners, the two major competitors submitted their final offer to Rothschild.

De La Rue to Close Two UK Sites

De La Rue announced this month that it is relocating two of its UK sites - Dunstable and Basingstoke. The workforce was told at lunchtime that the sites would close and production would be transferred to Gateshead in the north east and Westhoughton in the north west.

In May revenue fell by 17% compared with 2010 and Nicholas Brookes, De La Rue Chairman, commented: "The 2010/11 financial year has undoubtedly been a difficult one for De La Rue, our employees, customers and shareholders. We have dealt with a number of challenges including paper production issues; lower than expected banknote print volumes, changes in senior management and a takeover approach.

"The Improvement Plan has a target to achieve an operating profit in excess of 100 million-pound within three years by both restoring revenue growth and delivering significant cost reduction. The Board is confident that this plan can be delivered and its decision to maintain the dividend reflects that confidence, and the strong fundamentals of the business."

92,000 Customers Details Stolen from Citi Cards Japan

Citi Cards Japan (CCJ) has confirmed that the personal information of 92,408 customers has been stolen and sold to a third party illegally. The information that has been compromised includes account numbers, names, addresses, phone numbers, date of birth, gender and the date the account was opened, and only affects CCJ cardholders.

Card security information, including Personal Identification Numbers (PINs) and Card Security Code (CVVs) have not been compromised. CCJ immediately reported the inappropriate sale to the relevant authorities and the police, and has been cooperating fully with the investigation. So far no reports of fraudulent transactions have occurred.

3-D Secure: Friend or Foe?

By Sascha Breite, SIX Card Solutions

Sascha Breite

The latest series of cyber attacks on high profile companies such as Sony Playstation, Nintendo and CitiBank has put card not present (CNP) fraud firmly back in the spotlight. The theft of millions of customers' personal details, including credit card information in some instances, means that both consumers and banks need to be wary of the threat of criminals using these details for fraudulent means and thus take the necessary measures to prevent this. One simple solution is for consumers and businesses to sign up to the 3-D Secure scheme which combats online fraud by requiring the customer to enter a unique password that is only known by the issuing bank and genuine cardholder to complete a transaction.

Three Domain Secure, otherwise known as 3-D Secure, was first developed and introduced by Visa in 2001 to improve the security of online payments. Their branded 3-D Secure programme is commonly known as 'Verified By VISA'. MasterCard soon followed suit and introduced its payer authentication programme called 'SecureCode'. Along with increasing consumer confidence about making purchases over the internet, the overriding objective of 3-D Secure is to provide Issuers with the ability to actually authenticate cardholders during an online purchase. Up until its introduction, there was no way of proving that the person performing the payment transaction was the actual cardholder. For example, the Issuer could not obtain and validate a customer's signature as can occur during a face-to-face transaction. As a result, if a transaction was brought into question, the merchant would lose out on the sale as well as the goods or services. With the advent of 3-D Secure however the liability for a fraudulent transaction shifted from the merchant to the issuing bank and thus reduced the number of chargeback fees due to unauthorised transactions.

Where the problem arises today is that while Verified by Visa and MasterCard SecureCode are powerful tools in the fight against fraud, not all card issuing banks have enrolled their card holders to 3-D Secure. For example, in France only 14-15% of cardholders are registered to use 3-D Secure when making a payment online. This is because in those countries the main banking groups act as both the issuer and acquirer and so the liability lies with them regardless of whether 3-D Secure has been adopted during the transaction or not. Therefore the business case for these banks to invest in 3-D Secure and to market the technology becomes nullified.

As a result of the fragmented roll-out of 3-D Secure, especially across Europe, significant challenges are created for those businesses looking to expand internationally. What tends to happen is that a merchant that is growing cross-border will often come up against customers who are unfamiliar with 3-D Secure, like in France for example. In these scenarios where a customer is not registered with a 3-D scheme, they are often prompted to sign up during the purchase process. This will typically take them to a form, usually in a pop-up window, in which they are expected to confirm their identity by answering security questions which should be known to their card issuer. Cardholders who are unwilling to take the risk of registering their card during a purchase can therefore be deterred from completing a purchase due to this unknown feature. Even for cardholders enrolled with 3-D Secure, the problem can be in determining if the pop-up window in which the pre-agreed password must be entered is really from their bank, when it could be from a fraudulent website attempting to harvest the cardholder's details. In these instances the 3-D Secure schemes can be mistaken by users as phishing scams and again purchases are not completed as a result.

As a consequence, merchants are increasingly making the decision to disable 3-D Secure on their websites so as to increase the order rate in these countries. This is a risky approach in that it not only increases the merchant's exposure to fraud but it also shifts the liability back to them and raises chargeback rates. However, with 40-60 per cent of orders reportedly unfulfilled due to the issues thrown up by 3-D Secure for customers, it is a risk that many merchants are becoming prepared to take.

The solution would obviously be to ensure all cardholders are registered to a 3-D Secure scheme. However, although acquirers can force merchants to invest in 3-D Secure in order for them to obtain an acquiring contract – under the PCI-DSS standards – the same does not apply on the issuing side where 3-D Secure is an opt-in service for cardholders. To resolve this imbalance, both Visa and MasterCard are applying pressure on issuing banks to encourage more take-up of 3-D Secure among their customers. Yet without any regulation to compel them to do so, the onus remains very much on individual banks to educate their customers.

So while 3-D Secure has yet to be universally rolled out, it is clear that online merchants need to have appropriate tools and risk management applications in place to not only better protect themselves from fraud but also to help determine in which instances 3-D Secure should be used. For example, when a card comes into a merchant's payment system, there is software that can identify whether it has been issued by a bank with a good track record in enrolling customers to a 3-D Secure scheme. Subsequently it can recommend when to deactivate 3-D Secure to ensure an order is completed rather than disable the protocol altogether. As merchants need to be able to keep costs down and business fluid, such tools allow them to achieve the fine balance between higher revenue and fewer charge backs. Furthermore, it enables them to effectively fight CNP fraud and avoid unnecessary losses. Only then, can 3-D Secure be a true friend.

World News In Brief

Southern Railway Trials Smartcard Technology

Southern is to trial new smartcard technology - an alternative to paper tickets - making it easier and quicker for passengers to buy and use tickets.

Called 'the key', the new smartcard is reusable and can be recharged again and again with various types of ticket including seasons, singles and returns.

The trial will be at all stations on the line from Brighton to Seaford where work has started on installing the equipment required to support the smartcard system. 100 passengers will take part, reporting back on their experience of the system so that Southern can refine it before rolling it out elsewhere. The trial is due to start in September.

Southern's Development Director Alex Foulds said: "This is just the start. The key smartcard will evolve over time with many possibilities for the future. For example in time we will be able to tailor ticket products such as 'early bird' season tickets for those who travel earlier than the morning rush hour, or perhaps a carnet-style season ticket for less frequent travellers. There will also be opportunities for integrated travel tickets such as rail-bus tickets."

BlackBerry Smart Card Reader Achieves Advanced Security Certification for U.S. Federal Government

Research In Motion (RIM) announced today that the BlackBerry Smart Card Reader has achieved FIPS 140-2 certification level 3 - the highest certification achieved by any wireless smart card reader on the market. Smart cards support security programs like the U.S. Department of Defence's Common Access Card (CAC) program and the Homeland Security Presidential Directive 12 (HSPD-12) which calls for a mandatory, government-wide standard for secure and reliable forms of identification issued by the federal government to its employees and to the employees of federal contractors. FIPS (Federal Information Processing Standard) certifications are assigned by the National Institute of Standards and Technology (NIST), an agency of the U.S. Department of Commerce.

"Our customers value the robust security provided with BlackBerry products and services and smart card readers are particularly important within the government sector," said Scott Totzke, Senior Vice President, BlackBerry Security at Research In Motion. "This advanced certification of the BlackBerry Smart Card Reader for the U.S. Federal Government demonstrates our ongoing commitment to meet and exceed the expectations of our government customers."

The BlackBerry Smart Card Reader is designed to work with personal identification cards issued by government organisations or other high-security organisations. Users insert a smart card into this lightweight reader and wear it on a lanyard as a two-factor authentication device for secure access to BlackBerry smartphones, desktop computers and facilities. BlackBerry smartphones and desktop computers automatically lock when the user's smart card is not in proximity.

FIPS 140-2 level 3 certification of the BlackBerry Smart Card Reader also verifies advanced security features of the smart card reader itself, such as tamper evidence and self destruction of critical security parameters upon device breach.

South Korean iPhone owners to Sue Apple

Apple has faced much criticism after it was revealed that the iPhone and iPad stores their locations which could be used to track users' movements.Apple is facing a law suit from 27,000 South Koreans for privacy violations relating to the collection of user location information. Each is seeking One-million KRW (GBP 568).

In April a pair of security researchers found a hidden file on the iPhone which records the devices latitude-longitude coordinates along with a timestamp, although not one hundred percent exact they are very well detailed. Apple have denied that they have used the information to track a users location, saying the handsets were recording information about mobile phone masts and wi-fi hotspots.

Hackers Bypass Google Security to Execute 80,000 Daily Queries for Cyber Reconnaissance

Imperva's Hacker Intelligence Initiative (HII) today revealed that hackers are leveraging the power of search engines to successfully carry out attacks - and it's risk free. Hackers, armed with a browser and specially crafted search queries ("Dorks"), are using botnets to generate more than 80,000 daily queries, identify potential attack targets and build an accurate picture of the resources within that server that are potentially exposed. Automating the query and result parsing enables the attacker to issue a large number of queries, examine all the returned results and get a filtered list of potentially exploitable sites in a very short time and with minimal effort. As searches are conducted using botnets, and not the hacker's IP address, the attacker's identity remains concealed.

"Hackers have become experts at using Google to create a map of hackable targets on the Web. This cyber reconnaissance allows hackers to be more productive when it comes to targeting attacks which may lead to contaminated web sites, data theft, data modification, or even a compromise of company servers" explained Imperva's CTO, Amachai Shulman. "These attacks highlight that search engine providers are need to do more to prevent attackers from taking advantage of their platforms."

During May and June its Application Defense Centre (ADC) observed a specific botnet attack on a popular search engine. For each unique search query, the botnet examined dozens and even hundreds of returned results using paging parameters in the query.

The volume of attack traffic was huge: nearly 550,000 queries (up to 81,000 daily queries, and 22,000 daily queries on average) were requested during the observation period. The attacker was able to take advantage of the bandwidth available to the dozens of controlled hosts in the botnet to seek and examine vulnerable applications.

Google Acquires Motorola Mobility

Google Inc. and Motorola Mobility Holdings, Inc. this month announced that they have entered into a definitive agreement under which Google will acquire Motorola Mobility for $40.00 per share in cash, or a total of about $12.5 billion, a premium of 63% to the closing price of Motorola Mobility shares on Friday, August 12, 2011. The transaction was unanimously approved by the boards of directors of both companies.

The acquisition of Motorola Mobility, a dedicated Android partner, will enable Google to supercharge the Android ecosystem and will enhance competition in mobile computing. Motorola Mobility will remain a licensee of Android and Android will remain open. Google will run Motorola Mobility as a separate business.

Larry Page, CEO of Google, said, "Motorola Mobility's total commitment to Android has created a natural fit for our two companies. Together, we will create amazing user experiences that supercharge the entire Android ecosystem for the benefit of consumers, partners and developers. I look forward to welcoming Motorolans to our family of Googlers."

The transaction is subject to customary closing conditions, including the receipt of regulatory approvals in the US, the European Union and other jurisdictions, and the approval of Motorola Mobility's stockholders. The transaction is expected to close by the end of 2011 or early 2012.

iPhone Users Most Keen to Bank via Their Mobile

Intelligent Environments, a digital banking provider, reveals that one in five (21%) Brits would pay their bills through a mobile phone if they had the choice. A quarter (25%) of GB adults would transfer funds using a mobile phone while 36 per cent would be keen to check their balances via the device.

iPhone users emerged as the most eager to access banking services via their phones: 69 per cent would check their balance, 46 per cent would pay their bills and 62 per cent don't mind transferring funds, all through their mobiles.

Better by Far...

By Peter Tomlinson, Smartcard & Identity News

Peter Tomlinson

The Wurzels enjoyed considerable popularity in some music circles, but before then it was something more substantial: Adge Cutler and the Wurzels. Very sadly, one night in 1974 after a gig, Adge drove down towards the M4 from Chepstow and failed to make it round the Motorway junction roundabout. I never met him or listened to him live (although I did buy a cassette tape from his widow), but my Uncle who lived in Pill would sometimes encounter Adge in the local Working Mens' Club. Late at night Adge would turn up, play the piano, and they would all sing 'Pill, Pill' . The song features the Pill Ferry across the Avon to Shirehampton, on a stormy night, and has the line: "Better by far in the Duke or the Star than on the old Pill Ferry tonight".

The April article was about eID, and then at the end introduced another topic: Information Assurance (IA) , which describes a set of quality disciplines applicable to the ICT environment of connected systems and users (and equally applies to non-ICT schemes). In applying IA to ICT, the aim is to guide organisations towards understanding the nature of that environment: computers are deterministic - the old 'garbage in, garbage out' rule applies - and weaknesses are there to be exploited. Parodying Adge, better by far to be secure in the knowledge that an online system has been professionally developed according to IA principles and professional standards, thoroughly tested and carefully served (sorry - I was thinking about the Somerset cider again - meant to write regularly reviewed and tested). Better than being brought down by attackers that can penetrate every crevice in your design, better too than having a scheme that frustrates the users.

But, when developing online methods, I submit that we also need to do something else beyond applying IA-related technical methodologies, because the stark definitions of Information Assurance miss out taking into account user psychology - practitioners will do well to add that into their armoury. The term 'users' there encompasses not just the external service user, it also includes those who use the formal framework within which IA principles are applied to design and operation of an ICT driven scheme.

Nowhere is the problem of motivating those who develop and run a scheme more obvious than in large sections of our public administration, and it was in that context that the 30th March session of the House of Commons Public Administration Select Committee included the following exchange :

> Q557 Lindsay Roy MP: What you are telling us is that one of the key changes is that IT considerations will be viewed in a similar way to financial or legal implications, and treated in the same way during their development process. Would that be an accurate reflection?
>
> Ian Watmore (Cabinet Office COO): I absolutely think that delivery of the policy, in all its guises, should be thought about right at the beginning when you are making policy, and delivery includes technology, organisational change, people and the other things as well. I absolutely agree.
>
> Francis Maude MP, Cabinet Office Minister: As we move towards public services being delivered much more online, following Martha Lane Fox's excellent report, what has happened in the past is that not very good processes that have been designed to deliver complicated policy tend to get automated, which leads to a lot of complexity in the technology. The key insight Martha Lane Fox had in her report was that you need to use automation and the move to online delivery to force redesign of the process from the outside in. The Chief Executive of one Government agency said to me a few months ago, "Of course, we need to educate the public to use our service properly." I said, "I think you have that the wrong way around actually. I think we need to educate ourselves to provide our service in a way that the public do not need to be educated about it." Amazon did not get where they were by saying, "We have to educate the public to use our service." They did it by having an offering that was irresistible, irresistibly easy to use and then constantly developing it. We have to change our own mindsets and behaviours.

When the rain down pours, the thunder roars, the lightning flashes bright,
I'd be better by far in the Duke or the Star than on the old Pill Ferry tonight.

1. *The song is included in Adge Cutler Live at the Royal Oak Nailsea (Nov 1966)*
2. *http://en.wikipedia.org/wiki/Information_assurance*
3. *http://www.publications.parliament.uk/pa/cm201011/cmselect/cmpubadm/uc715-v/uc71501.htm*

World News In Brief

Visa Plans to Accelerate Chip Migration and Adoption of Mobile Payments in USA

Visa Inc. announces plans to accelerate the migration to EMV contact and contactless chip technology in the United States. The adoption of dual-interface chip technology will help prepare the U.S. payment infrastructure for the arrival of NFC-based mobile payments by building the necessary infrastructure to accept and process chip transactions that support either a signature or PIN at the point of sale.

"By encouraging investments in EMV contact and contactless chip technology, we will speed up the adoption of mobile payments as well as improve international interoperability and security," said Jim McCarthy, global head of product, Visa Inc.

Not only will chip technology accelerate mobile innovations, it is also expected to secure payments into the future through the use of dynamic authentication. Chip technology greatly reduces a criminal's ability to use stolen payment card data by introducing dynamic values for each transaction. Even if payment card data is compromised, a counterfeit card would be unusable at the point of sale without the presence of the card's unique elements. By reducing static authentication, we diminish the value of stolen cardholder data, benefiting all stakeholders.

VeriFone Completes Acquisition of Hypercom Corporation

VeriFone Systems, Inc. announced this month the completion of its acquisition of Hypercom Corporation. In connection with the closing, VeriFone and Hypercom reached a settlement with the U.S. Department of Justice, following which Hypercom divested its U.S. payment systems business to The Gores Group, LLC.

"This strategic acquisition complements VeriFone's position as a trusted, worldwide leader of the electronic payment industry," said VeriFone CEO Douglas G. Bergeron. "VeriFone plans to grow and enhance all major product lines that existed prior to completing this acquisition, bolstered with the strong VeriFone brand identity."

VeriFone expects the acquired Hypercom business to contribute in fiscal year 2012 non-GAAP revenue of $350 million and non-GAAP fully diluted EPS accretion of 20 to 25 cents.

NHS e-Records Unworkable say UK MP's

The Commons Public Accounts Committee publishes a report this month on the workability of the National Programme for IT in the NHS. The report is based on evidence from the Department of Health (The Department) and its contractors BT and Computer Sciences Corporation (CSC).

The Department has been unable to demonstrate what benefits have been delivered from the 2.7 billion-pound spent on the project so far.

It should now urgently review whether it is worth continuing with the remaining elements of the care records system. The 4.3 billion-pound which the Department expects to spend might be better used to buy systems that are proven to work, that are good value for money and which deliver demonstrable benefits to the NHS.

Margaret Hodge MP, Chair of the Committee of Public Accounts, said: "The Department of Health is not going to achieve its original aim of a fully integrated care records system across the NHS. Trying to create a one-size-fits-all system in the NHS was a massive risk and has proven to be unworkable.

The original objective was to ensure every NHS patient had an individual electronic care record which could be rapidly transmitted between different parts of the NHS, in order to make accurate patient records available to NHS staff at all times.

Lieberman Software Calls for Companies to go Wired-only

As a new wireless network sniffing app for Android - reportedly with attack, man-in-the-middle and remote trojan facilities - is about to be released, Lieberman Software is warning companies that wireless connections should no longer be considered the best option for network deployments.

According to Philip Lieberman, President and Chief Executive Officer, the development of dark apps such as the Android Network Toolkit means that anyone armed with an Android smartphone or tablet computer can now become a wireless network hacker.

"All it takes is one wireless configuration error, and Android-equipped hackers can gain access to the corporate network - and then all hell can break loose." he added.