January 2011

Volume 20 • Number 1

Smart Card & Identity News

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

www.smartcard.co.uk

Mobile Eavesdropping Made Easy

At the 27th annual Chaos Communication Congress (CCC) in Berlin, German cryptographer Karsten Nohl and team member Sylvain Manaut of the Chaos Computer Club presented their latest exploit - this time against the Global System for Mobile Communications (GSM) network.

Typically, governments tap mobile phones with the co-operation of the mobile phone provider and the call is recorded at a GSM base station. However, a quick internet search reveals that Law enforcement agencies can obtain specialist GSM over-the-air interception hardware for more covert operations!

In August of last year, the GSM association made a statement that they: "strongly suspect the team developing the intercept approach has underestimated its practical complexity. A hacker would need a radio receiver system and the signal processing software necessary to process the raw radio data." Karsten Nohl and team took this as a challenge to create a technique of using inexpensive phones to snoop over-the-air calls.

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, Suparna Sen

Contributors to this Issue –
René Van Ryt, Jeff Hudson,
Tom Tainton, Mickey Boodaei,
Peter Tomlinson

Photographic Images - Nejron -
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.

Our Comments

Patsy Everett

Dear Subscribers

Well it's nearly time for the GSM conference in Barcelona now renamed as the Mobile World Congress. For those of you thinking to attend it's from the 14th to the 17th of February.

I would have to say it has been a particularly interesting month with conversations wandering into the realm of science fiction. It all started with the mobile phone now an essential part of everyday life but which might have been looked on by many as 'sci-fi' back in the 70's or even 80's. In fact I even know a few people who didn't expect it to take off even in the 90's. So we started off imagining what phones would look like in 50 years time, same sort of thing really but with a more modern fashion statement, perhaps some snazzy wrist band and of course speech recognition and all that, there was no need to press buttons or even play around with touch screens.

Now here comes the first run up against biometrics, do we believe that in 50 years time that our electronic gizmos are going to have near perfect speech recognition? I think we do and in my snapshot of family, friends and colleagues this was not seriously in doubt. I would just mention that people have been actively working on this for the last 30 years and in various ways for at least the 20 years before that. So in the last 50 years we haven't got there, so what's going to make it happen in the next 50 years?

It is the advances in technology, we are moving much faster than we have ever moved before and at the end of the day there is no fundamental breach in the law of physics. Starting at home we often have this conversation, if it can happen it will happen and if people realise they need it then it just comes a bit faster. So from the novice side of the counter, will speech recognition be perfect (i.e. without errors) in 50 years time. Well again I think we all agree that it won't be perfect but near it and maybe just 1% error or less. But as my friendly bank manager used to remind me, if you take instructions from 100,000 people in a day that means on average 1000 people are going to have a problem! This was when we wanted to use finger prints for authentication at an ATM.

Now the thing is that this may not matter, in practice the English language has enormous redundancy. There are many examples but here is one,

Aoccdrnig to rscheearch at an Elingsh uinervtisy, it deosn't mttaer in waht oredr the ltteers in a wrod are, olny taht the frist and lsat ltteres are at the rghit pcleas. The rset can be a toatl mses and you can sitll raed it wouthit a porbelm. Tihs is bcuseae we do not raed ervey lteter by ilstef, but the wrod as a wlohe.

And so to our speech recognition, if we can start handling this form of redundancy in spoken context then why not 100% for comprehension and that's all that really matters.

So then we move to identity, a fundamental necessity for payments.

In 50 years time we are not going to have smart cards and the like. It's all going to be in the phone and then we just need identity on the assumption that our money is in some form of a bank account. Now do we believe that will be true in 50 years time? Anyway assuming in the sci-fi world we need to prove our identity in order to get our ration of kwala powder, how do we do it?

Back to biometrics, not speech recognition this time but voice or speaker recognition. This is a totally different problem to the speech recognition that we referred to earlier. I remember once at a seminar hearing the words of wisdom from one of the leading luminaries. I won't name him because he might be embarrassed but anyway he said that biometrics can only ever be a compromise because the human body is dynamic, it is constantly changing and therefore our biometrics are also changing. Unless you can update a person's biometric every hour or so then you are likely to have additional errors to the intrinsic measurement error that you will get whether you like it or not.

In the world of sci-fi you can put your hand or finger on the plate and bingo in you go. I guess it's going to happen in 50 years time, I'm just not sure how?

See you in Barcelona,

Patsy.

Contents

Regular Features

Industry Articles

Events Diary

February 2011

14-17	Mobile World Congress 2011, Barcelona, Spain - www.mobileworldcongress.com
14-16	World Cards and Payments Summit 2011, Dubai, UAE - www.fleminggulf.com/finance/middle-east/world-cards-and-payments-summit-2011
22-23	NFC Congress 2011, Hagenberg, Austria - www.nfc-research.at
22-24	European Card Acquiring Forum 2011, Berlin, Germany - www.europeancardacquiring.com/

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

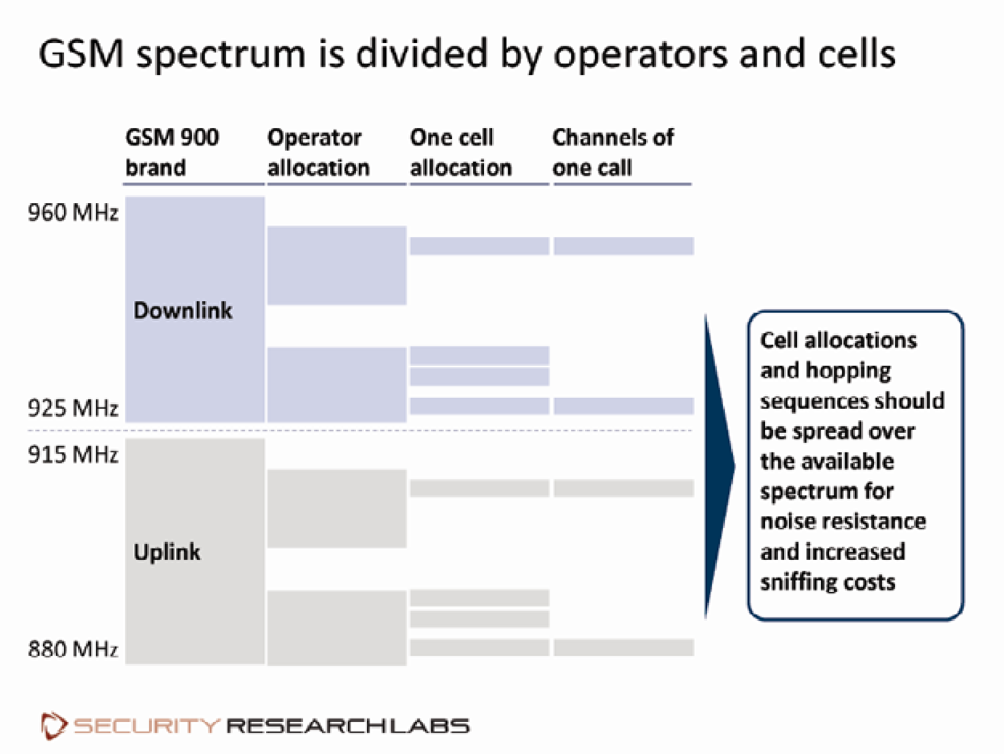
March 2011

8-11	IC Card World 2011, Tokyo, Japan - www.shopbiz.jp/en/ic/
9-11	Payment Trends China 2011, Shanghai - www.paymenttrends.com/
16-17	Cards & Payments Solutions 2011, Earls Court, London, UK – www.retailbusinesstechnologyexpo.com/page.cfm/link=31
21-22	CEE Card Markets Conference 2011, Radisson SAS Beke Hotel, Budapest, Hungary - www.ceecards.com
21-23	Automatic Face and Gesture Recognition 2011, Santa Barbara, California, USA - www.fg2011.org/
21-25	Cards Africa 2011, Johannesburg, South Africa - www.terrapinn.com/2011/cardsza/
23-24	Global Commercial Cards & Payments Summit 2011, Hilton New York, New York, USA - www.commercialpaymentsinternational.com/global-summit-2011.htm
28-29	Cards and Payments Australasia 2011, Hilton Hotel, Sydney, Australia - www.terrapinn.com/2011/cards/
29-31	Cartes in Asia, AsiaWorld-Expo, Hong Kong - www.cartes-asia.com/
29-31	RFID Show, Porte de Versailles, France - www.rfid-show.com/

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

Mobile Eavesdropping Made Easy …. Continued from page 1

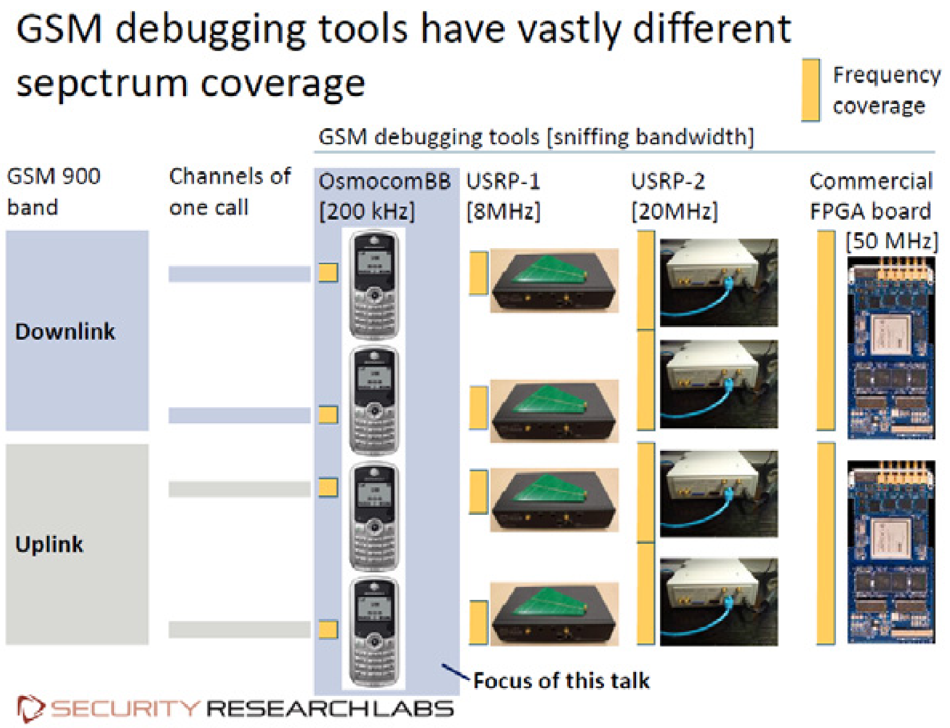
Within the presentation Karsten and Sylvain conducted a live demonstration using inexpensive (10 Euro) mobile phones (Motorola C123's). Karsten Nohl explained how GSM calls hop frequencies: "So you can appreciate that this is a multi-frequency problem, with a moving unpredictable target".


GSM spectrum is divided by operators and cells

Cell allocations and hopping sequences should be spread over the available spectrum for noise resistance and increased sniffing costs

Above: The Operator's cell tower only uses a fraction of the GSM spectrum

The demonstration used four mobiles phones to get the required frequency coverage to listen to the full conversation on the targets phone.



GSM debugging tools have vastly different sepctrum coverage

The phones were connected to a medium-end computer with over 2Terrabytes Bytes of storage capacity. Nohl and his colleague then showed the CCC attendees each step of recording someone else's conversation and text messages. They started with locating a particular phone within the conference room to seizing its unique caller ID, and finally getting hold of data exchanged between a handset and a base station as phone calls are made and messages are sent. After recording the phone calls and text messages, he goes on to use 'Kraken' software to very quickly decrypt the messages and call. In 2010 July's SCN newsletter the article entitled "Kraken Feeds on your Phone Calls" introduces how Karsten Nohl and his team developed the 'Kraken' software.

The team has thus successfully developed a complete toolkit, making it easier for hackers to sniff phone calls anytime, anywhere using open source software and cheap hardware.

The demonstration used Motorola C123 phones, because the phones firmware specification got leaked on the internet enabling opensource advocates 'Osmocom' to create a firmware replacement which enables the phone to record the raw photo call with control data.

Finally let's remember, Karsten's Kraken technology is useful only to crack A5/1 encryption algorithm, not its upgraded version - the A5/3 algorithm. In the presentation Karsten mentions that: "as more iPhones suck up the 3G bandwidth for internet usage, the more phone calls will be pushed down to GSM again. So 3G is no answer to GSM security problems as long as operators operate both as parallel".

Since 1984, CCC has become a platform for world-wide hackers to operate and test the security level in modern network systems. CCC and Karsten Nohl intentions are to make people and companies more aware of weak security.

According to Karsten, mobile phone networks do not provide state-of-the art security for complete, all-round protection. He has repeatedly urged the mobile operators to use the more secured A5/3 algorithm in place of the old A5/1 encryption algorithm, but it seems higher cost of upgrading the equipments has prevented the mobile operators from switching over to A5/3 algorithm.

Suparna Sen, Smartcard & Identity News.

Wideband GSM Sniffing Homepage: http://events.ccc.de/congress/2010/Fahrplan/events/4208.en.html

What Opportunities do Contactless Readers offer Card Manufacturers and the Payment Industry?

By René Van Ryt, Vice President of Cashless Payment, HID Global

René Van Ryt

Historically, it has been difficult for payment and ticketing system manufacturers to offer a single reader solution that simultaneously supports closed-loop payment schemes and open-loop debit/credit card schemes on the same reader platform. With the advent of interoperable, multi-functional contactless reader platforms, however, manufacturers are able to configure solutions that, for instance, can process both a PayPass transaction in Germany and top up an Octopus card in Hong Kong.

These more convenient combination open and closed-loop credit cards are rapidly moving to the top of the user's wallet. They enable converged applications such as a credit card/transit-pass card that can be used with both closed- and open-loop payment schemes, or an ATM card that could be used to add funds to a transit pass using a closed-loop payment system. In addition to enabling both types of payment schemes, today's new reader platforms also support all major contactless smart card technologies and are flexible enough to incorporate new functionality when standards and requirements change.

For card manufacturers as well as automatic fare collection and ticketing systems manufacturers, reliable, fast and secure contactless readers that process both open- and closed-loop payment transactions are essential to future growth. As contactless card technology expands into diverse industries and world regions, and as end-users are introduced to faster, more convenient and secure payment transactions, manufacturers of contactless readers have to stay one step ahead to anticipate new applications and functionality requirements from end-users.

Growth in the prepaid card market helps underscore why contactless reader developers continue to innovate and deliver ever more flexible solutions that process both open- and closed-loop payments.

The Mercator Advisory Group reported that the value of dollars loaded onto prepaid cards in 2009 will have more than doubled, to $672 billion, by 2013. Indeed, the large base of prepaid debit/credit loads has accelerated the transition from closed-loop to open-loop payment schemes. While open-loop schemes have grown by the greatest amount, the closed-loop market still represents a substantial two-thirds of all prepaid dollars. With closed-loop schemes not going away anytime soon, system manufacturers often need readers that will establish a migration path from closed- to open-loop payment and support both payment schemes.

There is more for card manufacturers to focus on beyond how to support evolving payment schemes. The payment industry is also very rapidly moving from legacy magnetic stripe (mag stripe) to 13.56 MHz contactless technologies that significantly improve security, performance and data integrity. This also delivers the advantages of enabling multiple applications in a single credential. In the transit industry in particular, contactless technology has trumped mag stripe as contactless cards and readers have become the preferred choice for new automatic fare collection projects worldwide. This has positive implications for card manufacturers and system integrators, who now have the opportunity to help transportation authorities improve efficiency to cut cost as well as assist them in partnering with banks and retailers to create a transit card that becomes the payment card of choice for their riders. This enables passengers to benefit from an easy-to-use system that speeds transactions and shortens queues.

To support these trends, the card industry must ensure that today's payment systems incorporate all popular high-frequency contactless card technologies including MIFARE, DESFire and iCLASS, plus a broad range of protocols and payment schemes including FeliCa, EMVCo, Calypso, MasterCard PayPass, Visa payWave and American Express expresspay. In addition, integrators must be knowledgeable on how to comply with national/international standards as well as certifications that are fundamental to the integration of payment and public transport ticketing systems. While developing universally compliant systems can be challenging, today's reader solution developers can turn to manufacturers like HID Global to support them in this task.

The latest generation of multi-technology contactless solutions can be used for diverse applications -- from cashless payment with integrated loyalty programs that boost repeat business while enhancing the customer experience, to vending solutions that deliver higher levels of service and satisfaction while increasing revenue and profitability. These systems help retailers to achieve better revenues as their consumers spend more per transaction and make purchases more frequently.

A card that has multiple uses provides added value and convenience which will create the desired "top of wallet" position with consumers. Logically, if customers use a payment card to travel on the train in the morning, they are far more likely to automatically turn to the same card, if it is easy to use, for small purchases on their way to work. It is no surprise that the major credit card companies and open payment card associations are excited about the increased revenue opportunities presented by these combination cards. With multi-functional, contactless reader platforms that support open- and closed-looped schemes along with the increasing popularity of contactless technology and global standards fuelling interoperability, the industry is rapidly evolving to meet the demand for payment systems that deliver increased functionality, convenience and revenue.

World News In Brief

Oberthur Raising Finance for De La Rue Bid?

Privately owned Oberthur Technologies are thought to have approached buyout firms to help finance their bid for De La Rue, in return for a stake in its acquisition.

Earlier this month the UK takeover regulator gave Oberthur until the 7th February to make clear its intensions under a 'Put Up or Shut Up Deadline'. If Oberthur does not make a bid by the deadline it will be unable to do so for another for six months.

In December Oberthur's offer 896 million-pound offer was swiftly rejected by De La Rue.

Now Vancouver's Transit System to Accept Smartcards

TransLink has a signed a contract with IBM Canada and Cubic Transportation Systems to bring smartcard-based fare payment system to Vancouver's transit system, according to The Cloverdale Reporter.

Slated for a 2013 launch, the new system will allow passengers on Metro Vancouver public transportation, including the rapid transit SkyTrain, to pay for trips with a single smartcard.

According to The Cloverdale Reporter, the project boasts a $171 million budget, of which $84 million will go to Cubic for the operating system, fare gates, smart card vending machines, readers and other equipment. Most of the remaining budget will go toward upgrading SkyTrain stations with new turnstiles.

SoftBank Selects Gemalto for Mobile Contactless Payment Trial

Gemalto announced its selection by SoftBank Mobile for the latest mobile contactless payment trial in Japan. SoftBank Mobile is a leading mobile operator in Japan with 21 million subscribers. The program is the first in Asia to enable secure mobile Near Field Communication (NFC) transactions from a choice of different credit card accounts. The pilot is expected to roll out in the first quarter of 2011.

SoftBank Mobile customers will be able to use their mobile phone for contactless payments in convenience stores, fast-food restaurants and theatres. The program also enables users perform NFC transactions from 2 credit card issuers - Orient Corporation, the largest service provider of MasterCard PayPass in Japan, and Credit Saison another Japanese leading financial institution. This is made possible by embedding multiple MasterCard PayPass applications in the secure UICC.

For the program, Gemalto will provide a turnkey NFC solution comprised of its Allynis Trusted Services Management operated services, UICC cards and N-Flex devices. The N-Flex let users to turn a conventional handset into an NFC-enabled mobile phone without any change to the device.

Phisher's Robbed China of $3 Billion

In 2010, new phishing websites went up 10 times in China and skyrocketed to 1.75 million. According to a Beijing Rising International Software Co. report, there were more than 44 million phishing cheating cases in 2010, which amounted to a total loss of more than $3 billion USD.

The phisher's mainly attacked online gamers and online banking clients. In addition, the rise of e-commerce in China (increased 22% compared to 2009) is also a key reason to explain the high number of phishing frauds. It was reported that China's largest online retailer, Taobao.com doubled its users from 176 million in 2009 to 370 million last year.

To tackle the growing phishing problem, Alibaba.com Ltd, owner of Taobao.com, signed an agreement with Intertek, a London-based internet security to improve online security.

McDonalds Plan Massive Contactless Rollout in UK

McDonalds has confirmed the rollout of contactless payment technology in all 1,200 of its UK restaurants. According to The Mirror, the fast-food giant is introducing special contactless readers that will allow customers to pay for orders of GBP 15 or less with contactless credit or debit cards. The 1.5million-pound initiative is set for launch this summer.

Google Manufacturing Cream

Google is building a mobile wallet nicknamed "Cream," which it plans to integrate with Android NFC phones that consumers could tap to pay in stores. Already U.S-based Citigroup has shown interest in the new mobile wallet.

According to news sources, MasterCard Worldwide and Visa Inc. have also been in talks with Google about possible participation in the search giant's plans to launch the wallet and enable a mobile-payment and advertising service on NFC smartphones. Among those phones to have Cream is Google's own Nexus S.

If the parties go ahead with the plans, an announcement of a launch could come early this year, with some sources predicting it could happen in a matter of weeks.

MBNA to Roll out Contactless Cards

UK's largest credit card provider, MBNA, has announced the start of its two-year programme that will see its 6 million customer base moved over to contactless cards by January 1, 2012.

To achieve this, MBNA will issue a new contactless credit card each time a new or replacement card request is made by a customer. MBNA estimates that most of its card-holders will have the ability to pay without a PIN by the start of 2012.

Contactless payment is a relatively new option at the checkout and is currently limited to GBP 15 per transaction, but the card provider can see the benefit to customers of this easier and faster payment mode.

Ian O'Doherty, Europe Card executive for Bank of America, which operates the MBNA brand, said: "With this two-year roll out of new and replacement contactless enabled cards we are reinforcing our support for the evolution of contactless technology in the UK.

New MorphoIDent in North America

MorphoTrak (Safran group) has released MorphoIDent at the Colorado Sheriffs' Winter Conference. Designed for law enforcement officers in the field, MorphoIDent mobile devices provide on-the-spot identity checks in real-time.

Palm-sized MorphoIDent weighs about 5 oz, and includes functional features such as an intuitive interface, folder management, vibration alert for noisy environments and an easy-to-use keypad. Fingerprints are captured with an FBI certified optical PIV sensor, including real-time automated quality check, and searched against an on-device watch-list or local, state and federal automated fingerprint identification (AFIS) databases.

Search results shown on the device's large colour LCD display provide officers fast access to critical crime solving information. MorphoIDent can be easily integrated into an existing IT architecture without incurring additional infrastructure costs.

ICO Welcomes Scottish Government's New Privacy Principles

The Scottish Government has published the Identity Management and Privacy Principles for public service organisations. The new guidance is designed to help organisations achieve privacy-friendly public services, encouraging good practice and ensuring personal data is always handled with respect. They have been devised by an expert group, including Ken Macdonald, ICO's Assistant Information Commissioner for Scotland and Registrar General, and subject to full public consultation.

The full guidance of Identity Management and Privacy Principles can be viewed at: www.scotland.gov.uk/Publications/2010/12/PrivacyPrinciples

2,500 More Ukash POS Terminals in Belgium

Following its launch in Belgium in 2008, Ukash, the Global eMoney Network, has significantly increased its foothold in the country, by now making available Bancontact/Mr.Cash system at an additional 2,500 points of sale across Belgium.

Bancontact/Mr.Cash system will provide greater access to consumers who wish to deposit, spend or send cash online. Ukash will be available in more than 2,500 independent convenience stores and petrol stations across the country from Trendycash terminals in increments of 10, 20, 50 and 100 Euros.

Weaponised Malware - how criminals are using digital certificates to cripple your organisation

By Jeff Hudson, Chief Executive Officer, Venafi

Jeff Hudson

The recent cyber attack on an Iranian nuclear facility using the Stuxnet virus should worry all of us - not just those in close proximity who were in danger of being blown into the next world by the actions of a computer virus.

The headlines around the story of the Stuxnet attack on an Iranian nuclear facility were familiar: "New malware attack". Digital security threats and sometimes the hype surrounding them have become commonplace in our interconnected and IT-dependent world. However, this was no ordinary attack. Apparently malware was introduced into the Iranian nuclear facilities local area network. It entered between the internet and the internal network. The other possibility was a trusted insider who was an agent of the organisation which carried out the attack.

As researchers later discovered, the attack used four different Zero Day exploits on Windows platforms. In addition to the Zero Day attacks, the 'payload' included a stolen digital certificate that was issued by Verisign. The virus was self-propagating and spread to numerous machines. The mission of this virus was to auto-propagate in the wild (there was no back channel to a command and control host as this was an isolated network). It was then to locate and operate a valve or control module that was a critical part of the nuclear facility's infrastructure, with the intent of disabling or damaging the facility. In other words: to act as a weapon. This is a significant step forward in the development of malware.

The traditional, malicious approach to damaging the facility would have been to use a conventional weapon (i.e. a bomb). The astonishing difference is that this malware was attempting to do mechanical damage to the facility without supplying the destructive mechanical force on its own. In other words, this was malware designed specifically to accomplish the work of a weapon. It has therefore earned the dubious classification as weaponised malware.

This particular malware is estimated to have taken 10 man years of effort to develop. It is sophisticated. The tools used in development, the timestamps on the binaries, and the number of modules with different coding styles suggest multiple development teams. The origin of the malware has not been verified but the most popular theory is that it was developed by a nation state or states that were attempting to disrupt the Iranian nuclear program.

Iran has the largest percentage of known instances of the Stuxnet virus. However it has also been found on systems in many other countries. Experts predict that numerous, undetected instances are still active.

It is a well-established fact that many weapons developed by national military programs become available to non-nation state entities, such as terrorists, rogue nation states and criminal organisations. It is just a matter of time. Examples are; night-vision goggles, GPS systems, airborne drones, fully automatic rifles, Kevlar body armour and shoulder launched missiles, to name just a few.

The questions are, A) when will Weaponised Malware and its derivatives be used to destroy, disable or steal valuable assets and information from other nations, utilities, banks, or telecommunication companies, and B) what can we do about it?

The Stuxnet weaponised malware utilised multiple zero day vulnerabilities to infect, and employed a signed digital certificate to authenticate itself in the environment. The certificate allowed the malware to act as a trusted application and communicate with other devices. This is the first reported incident of the utilisation of a digital certificate in this type of attack, and is a very ominous and worrying development. The level of threat has moved from downtime and a damaged reputation because your certificate has expired to do physical damage to you and your employees if the virus successfully makes a manufacturing or utility process go critical.

The use of four zero day vulnerabilities and a stolen digital certificate signals the beginning of a new era of cyber warfare and cyber crime. The implications are enormous. This is not the first occurrence of this species. The Aurora virus was a first generation variant and Stuxnet represents a significant evolutionary leap in complexity and sophistication. Additionally the potential costs to the targeted organisation in the event of a successful attack are higher than ever.

Zero day vulnerabilities are by definition impossible to defend against. The use of unauthorised digital certificates by weaponised malware in a networked environment is another matter. There are steps organisations can take to significantly reduce the risk of a successful attack.

The first consideration is the knowledge of digital certificates that are active in a network. Most organisations do not know how many they have, where they are installed, who installed them, their validity, and the expiration date of the digital certificates in their network. Here's a parallel analogy in the world of physical security. This is exactly the same as not knowing which people in a secure building are authorised to be on the premises and which ones are unauthorised. Imagine a bank where no one knew which people in the building were authorised to be there or not. This is not an exaggeration. This is an unacceptable situation to anyone who takes security seriously. This is an unquantified risk. The only acceptable practice is to continually and actively discover certificates on the network.

Additionally those certificates must be validated that they are functioning as intended and that they are monitored throughout their lifecycle so that they can be expired and replaced as dictated by the security policies of the organisation. Most organisations are deficient in this regard. This is an unmanaged risk and can be easily brought under management. A failure to manage this kind of risk exposes organisations to increased vulnerabilities like the Stuxnet attack. This is not scaremongering – it is a real threat which will affect an organisation sometime soon.

Why are organisations exposing themselves to this unquantified and unmanaged risk? The reason is simple enough to understand. Before Stuxnet, the lackadaisical knowledge and management of digital certificates was viewed as acceptable. Additionally many board - level executives are not familiar with digital certificates, how they work, their role in security, and the management practices and policies. This has to change. There is not one board - level executive that misunderstands or underestimates the importance of ensuring that only authorised individuals can enter a secure building. Those same executives naively allow unauthorised or unknown certificates to enter and operate on their networks.

In summary there is unquantified and unmanaged risk that allows Stuxnet to propagate and operate on a network. This represents bad management practice of a critical part of a layered security model. Digital certificates are widely used to authenticate and identify entities in a network. Poor management practices render digital certificates ineffective for their intended purpose. In fact poor management in some cases creates an exploitation opportunity.

The Stuxnet Weaponised Malware is a very loud wakeup call as it has exploited the poor management practices of digital certificates that exist in many firms today. Implementing practices and policies for the management of digital certificates is an important and necessary component of a broad and wide security strategy. It is the one strategy that can detect the appearance of malware that utilizes digital certificates for authentication. Weaponised Malware has or will be aimed at every company in the Global 2000. The responsibility is to act before the weapon strikes.

World News In Brief

iPhone Hacker Publishes Secret Sony PlayStation 3 Key

The PlayStation 3's security has been broken by hackers, potentially allowing anyone to run any software, including pirated games, on the console. A group of hackers recently showed off a method that could force the system to reveal secret keys used to load software on to the machine.

A US hacker George Hotz, who gained notoriety for unlocking Apple's iPhone, has now used a similar technique to crack PS3's master key, and then published it on his blog. Sony has submitted a filing at the Northern District Court of California against the hackers.

Record Fraudulent iTunes Accounts for Sale on a Chinese Website

Around 50,000 accounts linked to stolen credit cards are listed on auction site TaoBao, China's equivalent of eBay. Buyers are promised temporary access to unlimited downloads from the service for as little as 1 Yuan (10p) a time. Apple, which recently stepped up iTunes' security after a series of break-ins, declined to comment. However, Apple had earlier warned users to safeguard their personal details.

Listings seen by the BBC tell buyers they can "go after anything they like" including "software, games, movies, music and so on". Several listings tell prospective buyers they can only use the accounts for 12 hours before it is likely to be shut down.

While it is not clear whether the accounts themselves were stolen, or whether they were set up with fraudulently obtained information, it is against the terms and conditions of iTunes to resell user identities.

Italy ID Cards to Use LaserCard's Optical Security

LaserCard Corporation has received an order to supply additional credentials for Italy's Citizen ID Card program - Carta d'Identita Elettronica or CIE. The highly secure, multi-technology ID cards, based on LaserCard's optical security media platform, will be used by citizens for identification and travel. The order is valued at approximately $540,000 and is expected to be delivered by March 31, 2011.

Through Italy's Citizen ID Card, security and law enforcement authorities will verify the identity of citizens while preventing the counterfeiting and fraudulent use of vital documents. The program includes special-language ID cards that are issued to citizens living in border regions where languages other than Italian are predominant. A small proportion of the cards from this order will be printed in Slovenian.

Vital Scottish Court Records Dumped at Recycling Bank

The Scottish Court Service breached the Data Protection Act by failing to take sufficient steps to prevent court documents containing sensitive personal details being accidentally disposed of at a local recycling bank in Glasgow, according to the Information Commissioner's Office (ICO) report.

The ICO was first made aware of the breach when a Scottish newspaper published details of the discovery of files containing appeal documents on 25 September 2010. Subsequent checks by the ICO uncovered that the papers had been lost by the editor of a series of law reports and that the court service had failed to check how this individual intended to keep the information secure.

The court service has now tightened its procedures around the handling of sensitive information by its staff and other people involved in the court process. The editor of the law reports has also agreed to improve the way in which court documents that include sensitive personal details are handled.

Brighton is UK's Card Fraud Capital

The annual Card Fraud Index released yesterday from life assistance company CPP has named Brighton as the card fraud capital of the country.

The top five card fraud hotspots in the UK are Brighton (38%), London (34%), Manchester (33%), Bristol and Leeds at joint fourth place (32%) and Edinburgh (31%).

The Card Fraud Index also reveals the methods criminals are using, with most victims (20 per cent) having the magnetic stripe on their card cloned at an ATM or via a Chip and PIN machine. This is a three per cent increase on 2009. One in five victims has been defrauded online with criminals using the internet to obtain card details.

New MegaMatcher from Neurotechnology

Neurotechnology announced the release of MegaMatcher 4.0, a multi-biometric software development kit (SDK) that integrates fingerprint, iris, facial and palm-print biometrics in a single, high-performance SDK that requires no add-ons.

In MegaMatcher 4.0, Neurotechnology has incorporated palm-print technology along with the latest versions of their popular VeriFinger (fingerprint), VeriEye (iris) and VeriLook (facial) biometric SDKs, all of which are now built on a common architecture and feature a common programming interface. This tight integration enables developers and integrators to more quickly and easily develop systems that use any of the different biometric components singularly or in combination for increased flexibility and reliability.

DeviceFidelity to Release New Add-On for Mobile Phones

U.S-based technology company DeviceFidelity will announce a new add-on for mobile phones, which will ensure a consistent experience for consumers tapping certain handsets to pay, including the popular Samsung Galaxy S, said NFC Times.

The add-on-a sticker containing an extra antenna or coil is needed to extend the range of the company's In2Pay microSD cards, which will carry a Visa payWave application.

Consumers would be asked to affix the sticker - Range Extender label to the inside back cover of their cell phones, giving the device an increased range of 2 to 4 centimetres, and allowing consumers to tap the back of the phones every time to pay.

Virtual Piggy going all the way to the bank

By Tom Tainton, Smartcard & Identity News

Tom Tainton

In the past five years, the social media craze has tightened its grip on the way the world interacts and stays connected. Today, individuals are socialszing online at a much earlier age, resulting in the growing participation of children in social gaming and the online market.

There are, of course, concerns about the protection of children in the virtual world. Whereas there are hundreds of laws and measures in place to provide protection in the physical world, virtual reality is distinctly lacking with regards to providing a defence against the sinister underbelly of the cyber world. But, Moggle Incorporated, an innovative technology company based in the U.S, has developed a solution that could give parents peace of mind. Started in 2008, Moggle delivers a security platform targeting children under the age of 18, enabling them to transact with online merchants, play games, and use social networks while under parent supervision.

The company's technology is designed to function in alongside the Children's Online Privacy Protection Act (COPPA) and other international child privacy laws. In 2009, $26 billion was spent by children on online purchases. This year the figure is expected to rocket to over $43 billion. Addressing a near untapped market, Moggle is growing rapidly. Its first patent-pending product is Virtual Piggy.

Virtual Piggy is a unique concept. Developed in response to an increasing number of online products aimed at children, the application provides an online payment profile that allows parents to set up, monitor and control their offspring's financial transactions online. And, not only does Virtual Piggy track all spending, parents can receive alerts and reports about when and where their funds are being spent. Guardians can determine how much a child can spend at one time, and control the merchants with which they can communicate. The beauty of the product is its potential. It could easily attract the likes of Facebook and online gaming sites to follow suit and do more to protect their younger users.

Moggle's Chairman, Dr. Jo Webber, said: "Moggle is at the forefront of developing platform architectures that create a safer environment for children online." It's a well-known fact that management is a key to a company's success, and Webber already has quite a pedigree. She served as CEO of Energy Solutions and InnoPhase Corporation, both of which were snapped up by larger players for huge amounts. Already, in the first round of financing from the private sector, Webber is rumoured to have raised over $2 million. The real question is: can she replicate the success long-term with Moggle?

The company's made a positive start, that's for sure. It was invited to present on the subject of Digital Monetization Strategies alongside luminaries from Hasbro, Disney, Foursquare and other leading digital media companies. Moggle also recently announced that it had reached a deal to use Chase Paymentech's Orbital Payment Gateway for the Virtual Piggy technology. The certification enables Virtual Piggy to support credit card transactions on the Chase payment processing platform, which supports all major cards. In addition, Moggle plans to extend the payment processing ability in the future to facilitate gateways such as PayPal and First Data.

Alongside Virtual Piggy, Moggle has developed several other applications: ParentMatch, ParentPlayback, and Age Check. ParentMatch and ParentPlayback are web services that provide guardians with an increased level of control. ParentMatch allows parents to set up web-filtering programs for their children, while ParentPlayback offers parents a video transcript of their child's online session. Moggle's Age Check is a software system that provides a rapid secure checking mechanism to determine the age of an individual.

It seems that Moggle is well-placed to take advantage of this market growth, and, with increased media exposure, could well become a recognisable name in the global online community.

World News In Brief

UK Finally Ends Controversial ID Card Scheme

Great Britain has scrapped a controversial identity card scheme whose introduction by the previous Labour government as part of anti-terrorism plans had outraged civil rights activists. The scrapping of the scheme has been approved after the David Cameron government's first Home Office bill, the Identity Documents Bill, received royal assent. The Office of the Identity Commissioner was also been closed.

The Identity Documents Bill invalidates the identity card, meaning that within a month, holders will no longer be able to use the cards to prove their identity or as a travel document in Europe. The Identity Card Scheme and associated work around biometrics has already cost the taxpayer 292 million pounds. The government will now stop planned future investment in the scheme of 835 million pounds.

All existing cardholders will be notified in writing and the Identity and Passport Service will now inform international border agencies, travel operators and customers of the change in law.

IBM Forecasts Holograms in Mobile Phones for 2015

IBM has released its 5th annual “Five in Five” forecasts, where the company states that in the next 5 years, people will see mobile phones with built-in holographic projectors that will enable users to get a 3D view of the people with whom they are speaking.

The two-way, 3D holographic-based communication technology will begin appearing in a wide variety of communications devices such as cell phones, enabling new levels of communications between people and in workplace collaboration.

Million Ingenico Terminals Delivered to Latin America in 2010

Ingenico has reached the historic milestone of delivering 1 million terminals in Latin America in 2010. The payment terminals, which include POS and PIN Pads were equipped with secure magnetic stripe. The smart cards readers were delivered to major banks and acquirers in the region over the past 12 months, thereby enhancing security of customers. The markets which showed greatest demand were Brazil, Mexico, Argentina, Colombia, Venezuela, Chile and Peru.

ViVOtech Released World’s First Customer-Facing Payment Acceptance and Promotion Device

ViVOtech released its new breed of customer-facing payment acceptance devices for merchants - ViVOpay 8800e

Featuring EMV chip, PCI 2.1 certification and built-in contactless NFC technology, the new ViVOpay 8800e device is equipped with a 16 million colour HD display and tactile keypad enabling merchants around the world to accept EMV smart cards, contactless and magnetic-stripe cards, and handset-based NFC mobile payments. The same system also allows merchants to deliver personalised NFC mobile loyalty and marketing programs to their customers’ mobile devices.

Using ViVOpay 8800e, customers can redeem mobile coupons and promotions electronically with contactless or mag-stripe cards, contactless sticker-attached to existing phones or NFC-enabled mobile phones. As a result, customers enjoy a high-value shopping and payment experience with personalised and location-based services and offers delivered to them while they are shopping in merchant stores.

World’s Fastest Card Printer Launched

Japan’s Toppan Printing Co. has announced the development of its new CP500 printer, which it claims to be the “world’s fastest printer for ID cards, student cards and admission cards”. The CP500’s compact 340x320x435mm size is roughly a third of Toppan’s previous models, but it can handle items ranging from magnetic cards to contactless cards and contact IC cards with “improved printing speed,” according to Toppan.

Additionally, the CP500 is capable of printing with a resolution of 600dpi and features the company’s anti-counterfeit pigment ink technology. Toppan hopes to launch the printer in August 2011.

Trident Appoints Interim CEO

Trident Microsystems announced that Sylvia Summers Couder has resigned as CEO and as a director to pursue other opportunities.

Philippe Geyres has been appointed as interim CEO with immediate effect.

11.7 Million Affected by Identity Theft in U.S

About 11.7 million Americans were victimised by identity theft over a two-year period, with more than half affected by the unauthorised use or attempted use of a credit card, according to the Bureau of Justice Statistics study. The Bureau surveyed 56,000 people in 2007 and 2008. People affected are around 5% of people age 16 and above.

Only about a quarter of victims nationwide suffered an out-of-pocket financial loss, and half of them experienced a loss of $200 or less, according to the report. The average out-of-pocket loss was $1,870, and the bureau estimated the total cost of identity theft over the course of the study was $17 billion.

The national study did not include figures for individual states or cities, but recent Federal Trade Commission data show the types of identity theft are more evenly spread in Oklahoma.

Intel Pays $1.5 Billion to Nvidia

The world's biggest micro-chip maker Intel has agreed to pay its smaller rival Nvidia $1.5 billion (GBP 965.2 million) to use its technology. The move brings to an end to a long legal dispute that began in 2009.

Intel had sued Nvidia, a graphics chip maker, over the right to keep making an Intel designed chip. Nvidia then counter-sued. Intel now has the right to use Nvidia technology at a time when graphics processing is increasingly important.

New iSC2xx Terminals Meet PCI SSC's Stringent PIN Transaction Security Device Requirements

Ingenico announced that its iSC2xx series signature capture devices have received approval for being in compliance with PCI Security Standards Council's (PCI SSC) PIN Transaction security standards.

The iSC2xx can be used for signature capture payment solutions and security. Built on Ingenico's new Telium 2 platform, it also offers retailers unmatched transaction speed and the full range of payment choices. The Ingenico iSC2xx devices will go for sale in Q1 2011.

Christopher Justice, President of Ingenico, North America said “Building on our solid base of innovative technology and security expertise, the new Telium 2 platform reduces our customers' exposure to fraud by protecting their brand and keeping their investments secure.”

Starbucks Rolls Out M-Payments across US

Following trials in California and New York, coffee chain Starbucks is rolling out its mobile payments service to nearly 6800 stores across USA.

The chain introduced its Starbucks Card Mobile App for iPhones, iPods and select BlackBerrys in 16 California outlets in 2009, later expanding the trial to 1000 Starbucks in US Target stores and another 300 New York locations.

AKAI Unveils India's First Trio

AKAI Mobiles announced the launch of its first triple SIM phone in India - ‘Trio’. It is a triple standby (GSM+GSM +GSM) phone with multimedia features.

Trio is a stylish phone with 5.1 cm (2”) TFT screen and including 1.3 megapixel camera with digital zoom, dual language support and audio player with equaliser. The handset hosts an in-built sound recorder and video player with video recording capability. Other basic features available in the phone include FM Radio, Bluetooth (A2DP), USB, E-book and gaming.

Trio has an expandable memory of 8 GB and the phone is GPRS and WAP enabled, which makes web browsing easier for consumers.

MasterCard Hired Orange Boss

MasterCard hired Mung-Ki Woo, the ex-Vice President of Mobile Payments of Orange, one of Europe's largest operators. Mung-Ki Woo will lead MasterCard's newly formed mobile unit.

Woo has worked at Orange since 2005, and is credited of hosting some of the first trials of near field communication (NFC) technology. He also coordinated a huge NFC push that's due to take place in France this year.

HID Global Achieves Worldwide ISO Certification

HID Global announced its worldwide certification of compliance with the International Organisation for Standardization (ISO)-9001:2008 specifications.

ISO 9001: 2008 certification of all HID Global facilities worldwide validates that all product design, develop, manufacturing, and delivery services adhere to process specifications and continuous improvement practices that produce consistent product quality and delivery performance.

The Criminal In Your Browser Is Real

He Wants Your Data and He's Not Going to Stop Till He Gets It. So, Are You Going To Let Him Have It?

By Mickey Boodaei, CEO Trusteer

Mickey Boodaei

Evidence is everywhere that cyber criminals exist, and they're able to make a substantial living from their illegal activities. While it is true that many are focusing their efforts on individuals, others have their sights set much higher. They are targeting enterprises to steal their highly prized intellectual property, log-in credentials, financial data and other sensitive information that resides within the once safe confines of the corporate network or in web applications. Numerous articles have written on why you need to protect this data. So, instead we're going to focus on the business at hand – the 'Man in the Browser'. How is he getting into enterprise networks and applications and, more importantly, how you can stop him?

The browser has emerged as the weakest link in an enterprise's security infrastructure. It is being successfully exploited by malware authors and criminals who use this method to steal logon credentials and inject Trojans that crack IT systems wide open, often undetected. With these browser sessions often containing the logon details for email systems, VPN's, cloud services – such as cloud CRM, it is a critical area to secure and lock down without impacting performance.

However, the growing demand for mobility makes this easier said than done. Once upon a time, remote access to enterprise resources was the privilege of a chosen few employees, who used standard computers owned and managed by the enterprise, making security a big, yet ultimately manageable, task. Today such access capabilities have exploded to allow virtually any employee, contractor and partner to gain entry. The problem is further compounded as these 'trusted users' are allowed to choose their laptop and smartphone, as well as utilise their home PC for work purposes and generally control their own IT environment. With more resources for them to access, and in the majority of cases not contained within a protected server farm – they're literally out there in the wild.

It is this adoption of unmanaged home-and-work laptops and personal PCs that has lead, in many cases, to malware infestations.

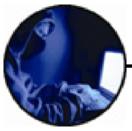
It's not safe out there

With more than 57,000 new malicious sites created each week, most of which mimic prominent web sites[1], it's hard not to stumble upon a spoof site and get infected. As users innocently browse these 'respectable' sites, they could inadvertently fall victim to drive-by-infections. However these attacks aren't just on spoof/phishing sites they also reside on legitimate websites that have been infected with malware, and the criminals use search engine optimisation (SEO) techniques to raise them to top of search engines to maximise the number of people infected. In fact, increasingly engineered attacks, such as the recent LinkedIn email phishing campaign, and SEO techniques are being used to ambush individuals and install sophisticated malware such as Zeus, Bugat, and Clampi (to name just a few) on unmanaged computers that operate outside corporate networks.

This modern malware is designed to slip under the radar of traditional anti-virus solutions and to bypass strong authentication technologies like tokens or Network Access Control (NAC) systems. When an infected unmanaged computer accesses enterprise resources via VPN connections and web portals, the malware is able to elude perimeter security mechanisms. The malware captures all data processed by that browser - including logon credentials and large quantities of sensitive corporate information, and transmits it back to the criminals. All this can be achieved without infecting a single computer within the physical boundaries of the enterprise or setting off alarms.

As attack opportunities continue to multiply, so does malware sophistication. An example of such ingenuity was witnessed in early 2010. The Aurora attack - targeting Google, Adobe and another 32 companies, demonstrated unprecedented malware sophistication. It used multiple coordinated malware packages, several layers of encryption and various browser and Operating System vulnerabilities demonstrating the power of today's malware. The fact that the entire attack went completely under the victims' radar makes this even more serious. Advanced Persistent Threats, coordinated long-term attack activity targeted at specific enterprises, is not uncommon in today's IT environment.

[1] *http://www.internetnews.com/security/article.php/3903046/Weekly+Tally+of+Malicious+Sites+Grows+to+57000.htm*



Proof of such attacks already targeting the enterprise is already being seen. We recently decrypted an attack on the popular Citrix Access Gateway where Zeus was instructed to take a screenshot every time the mouse is left clicked while the URL includes the term "/citrix/". This attack defeats Citrix' virtual keyboard solution which was created to bypass key-loggers by replacing keystrokes with mouse clicks. It proves that the criminals, such as those behind Zeus, are specifically targeting remote access connections into secure networks and going after intellectual property and other sensitive data contained within company IT networks and applications.

With modern malware efficiently written by professionals and designed to be robust, organisations need to think outside the box if they're to stand a chance of shielding their assets.

Don't trust the device, trust the session

Enterprises need to acknowledge and counteract the point of attack - the browser - if they're to stand a chance of protecting confidential enterprise data. A solution that can effectively secure access to enterprise networks from potentially insecure endpoint devices is needed.

Such a solution would comprise of technology that creates a virtual firewall of sorts inside the user's computer. Intuitively activated when the user connects to enterprise networks and applications, this potential technology would separate enterprise related sessions from any others taking place on the machine. Malware and exploitable vulnerabilities would be prevented from bypassing this virtual firewall and influencing protected web sessions with the enterprise. When a malware infected machine tries to communicate with the enterprise, it should be identified and the malware should automatically be removed before authenticating the device to all the enterprise systems.

Such technology should include keystroke encryption to evade key-loggers, communication protection to guard against unauthorised modifications, browser process and add-on protection as well as API blockage to prevent unauthorised access.

The enterprise is increasingly becoming a target of sophisticated, stealthy new malware that uses the enterprise's own employees, partners and contractors as weapons. With five percent of endpoint devices estimated to be infected by botnets and other sophisticated malware, can you afford to leave the door to the enterprise unguarded? The Man in the browser is out there, waiting to be invited in so make sure you slam the door in his face.

World News In Brief

PenFed CU Customer Data Exposed by Malware-Infected Laptop

The Pentagon Federal Credit Union (PenFed CU) confirmed that a laptop infected with malware has left the personal and financial information of some members exposed. The letter to the New Hampshire Attorney General Office revealed credit union discovered the exposure in mid-December 2010. Around 514 New Hampshire residents are affected by the breach but the credit union says it has no evidence that the information has been misused so far.

The malware permitted access to a database containing names, addresses, social security numbers, account numbers and credit and debit card numbers of PenFed members, joint owners, ex-members, staff and beneficiaries. PenFed has taken appropriate steps to prevent this from recurring, says the letter.

Micropross Releases New Contactless/NFC Protocol Analyser

Micropross has released a new protocol analyser for contactless applications - MP300 ACL1. The aim of this tool is to spy any exchanges that occur between contactless objects that operate at 13.56MHz.

The MP300 ACL1 is capable of spying all major protocols, including ISO 14443 A/B, ISO 15693, Mifare, FeliCa, NFC-Forum, NFC-IP1 and -IP2.

The MP300 ACL1's hardware is compatible with the very high baudrates protocols (both ASK and PSK modulations), and its embedded oscilloscope offers an analogue display of the communication, allowing the user to monitor the real signal without any additional hardware.

Vodafone Australia Customer Details Sold to Criminals

Vodafone Australia may face a class action for breach of privacy after it confirmed that its customers' details may have been sold to criminals. Apparently, the company change user passwords only once a month with many people accessing the customer database.

Vodafone Hutchison Australia said that all customer information was stored on Vodafone's internal systems and accessed through a secure web portal. It was accessible to authorised employees and dealers via a secure log-in and password.

Responding to the allegation, a Vodafone Group spokesman said "early indications suggested that this was an isolated incident". To him, Vodafone Group password policy complies with the international security standard ISO 27001.

However, according to the Information Security Forum's Standard of Good Practice, all users should be authenticated using user IDs and passwords or by strong authentication mechanisms (for example, smartcards or biometric devices, etc) before they can access target systems. But the company is silent on how often passwords should be updated.

On third-party access to corporate information, the ISF guide says the company should balance third-party control in order to protect the interests of the organisation in relation to ownership of information and systems, copyright of information and other issues, as well as limit the liabilities of the organisation to third parties.

Citigroup to Trail New Thank You Prestige 2G Card

International financial services firm Citigroup is set to trial a new multi-purpose smartcard - Thank You Prestige 2G Card, which will allow users to choose whether to pay for goods with credit or loyalty points. The company has teamed up with credit card producer Dynamics Inc to launch the Thank You Prestige 2G Card.

The card runs on Dynamics' Card 2.0 technology and features 2 buttons - Regular Credit and Request Rewards, which light up upon selection. Dynamics' Card 2.0 technology was awarded the Best of Innovations Winner for Personal Electronics at the 2011 International Consumer Electronics Show.

O2 Plans NFC Rollout in Second Half of 2011

A second major UK mobile operator will commercially launch NFC with Telefonica O2 UK during the second half of 2011. O2 joins the Orange UK-T-Mobile UK joint venture, Everything Everywhere, in making known its plans to roll out NFC. Everything Everywhere, which is partnering with Barclays bank's credit card unit, Barclaycard, for its launch, is likely to launch before O2.

O2 sees NFC as a major opportunity to build its financial services arm, O2 Money. A spokeswoman confirmed to NFC Times that the company is recruiting 14 new staff for the unit. O2 Money launched a pair of prepaid payment cards in 2009, which O2 has touted as the "most successful UK card launch".

Ingenico and Merchant Link Partner on Point-to-Point Encryption and Tokenisation Solution

Ingenico and Merchant Link announced a joint solution to offer Merchant Link's TransactionVault tokenisation technology with Ingenico On-Guard point-to-point encryption (P2PE) to merchants in U.S.A. Ingenico On-Guard with TransactionVault is a comprehensive data security solution that is primarily geared toward integrated multi-lane merchants.

The Ingenico On-Guard with TransactionVault solution helps merchants reduce their business risks and liabilities associated with potential data breaches by eliminating the transmission and storage of plain-text cardholder data from the merchant's environment, rendering card data unreadable and unusable to cyber criminals. This comprehensive payment processing and hosted tokenisation solution will also help merchants reduce their PCI DSS compliance footprint.

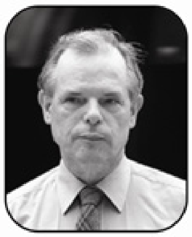
Qualcomm to Buy Atheros for $3.2Billion

Qualcomm Inc, the world's largest mobile phone chipmaker, agreed to buy Atheros Communications Inc for about $3.2 billion in cash, expanding its line up of Wi-Fi networking technology.

Qualcomm will use Atheros's chips in its base-band processors for mobile phones. Both the companies aim in making devices seamlessly pass calls from cellular to Wi-Fi networks.

So why do we not do eID?

By Peter Tomlinson - Smartcard & Identity News



Peter Tomlinson

The Porvoo Conferences are named after the Finnish city because that is where they started - in 2002. As their web site[1] states: "The International Porvoo Group supports the deployment of electronic identity in Europe" – universal secure eID, with digital certificates, secure tokens held in smart cards or maybe in mobile devices, verification service, etc. The win-win is obvious: lower costs with safe and better services. So far these are national programmes across Europe, not stitched together into an EU wide method, and definitely not joined into any emerging global programme. The Porvoo Conference programme is for two gatherings per year, each time in a different country. Thus the 14th Conference was held in Cardiff in October 2008, courtesy of DVLA. There Meg Hillier MP, then Home Office Minister for ID cards, was asked "Why do we not do eID?" Quickly her response was: "We have to walk before we can run".

Fast forward two years and an article in last October's SCN asked basically the same question about eID. At the same time a letter on the topic went to Ian Watmore in Cabinet Office, triggering a response that suggested "message received and understood". The SCN article included pointers to two eID programme, both started last summer. First to the Westminster based UK public sector G-Digital programme for a privately supplied method to deliver safe online services on behalf of the UK public sector: again looking for the win-win of lower costs with safe and better services - but only public sector services. It soon became clear that, despite all the global work done in this Millennium and earlier on universal eID methods applicable to both public and private services, the team behind G-Digital are still not running in the global sprint for the universal eID method to deliver the win-win. The second eID programme featured in October was also started last summer. It is the USA government sponsored programme to create a universal method by which all service providers and all users, public and private, can be safe online, a programme now known as the National Strategy for Trusted Identities in Cyberspace (NSTIC). The Americans see the benefit of doing something for everyone. Over here, the Directgov people in Cabinet Office are apparently going to be doing something to us rather than for us, and it is something that is only for the public sector. But, in the Big Society, the 'us' are all citizens, all service providers and the wider technology that support service supply chain. So where is the Big Society involved in G-Digital? Where is innovation encouraged?

As last October, a coda. First, it became obvious that the UK G-Digital programme is in two parts: service provision (initially through Directgov, later perhaps from the wider public sector) and Identity Assurance. Now we see on the G-Digital home page that G-Digital is "within the G-Cloud programme[2]" for government computing a consultation with the potential industry suppliers of the tools for the G-Digital job took place, then all was quiet, and expected further material did not appear in November. Two months later the G-Digital Market Investigation Findings have been published[3], and "The Identity Assurance Service Description is being finalised[4]". Studying the Findings suggests, not Ms Hillier's style of caution from inside the tent, but instead industry's concerns from out there in the big wide world:

- Consensus that a very clear set of operating standards are required
- Common agreement that customisation of a service must be strongly resisted
- SMEs need greater representation and emphasised the need for transparency in establishing markets
- Defining the standards (technical and other) for the G-Digital service 'eco-system'

In the USA, the federal move is for supporting universal standards and methods[5], after which the market will provide secure tools for both public and private services. Their pro-active standards organisation NIST is involved[6], they have taken the topic to the monthly meetings of their Government Smart Card Interagency Advisory Board (IAB), and their Commerce Dept is to host a National Program Office in support of NSTIC[7] - but there is also some concern that this may take a long time[8]. There is a flurry of activity to build the 'eco-system' so that the flowers can bloom.

[1] *http://www.fineid.fi/vrk/fineid/home.nsf/pages/6F4EF70B48806C41C225708B004A2BE5*

[2] *http://gdigital.direct.gov.uk/*

[3] *http://gdigital.direct.gov.uk/findings/*

[4] *http://gdigital.direct.gov.uk/identity-assurance/*

[5] *The root policy document, dated June 2010, is on the Dept of Homeland Security web site: http://www.dhs.gov/xlibrary/assets/ns_tic.pdf*

[6] *http://www.nist.gov/nstic*

[7] *http://www.computerworld.com/s/article/9204078/White_House_officials_push_online_trusted_IDs*

[8] *http://www.networkworld.com/news/2011/011411-experts-govt-trusted-internet-identities.html*

World News In Brief

G&D Signed International Payments Contract with UniCredit

Giesecke & Devrient (G&D) has been awarded an international three-year contract by the UniCredit Group for supplying electronic payment system solutions. The contract has been effective as on January 1, 2011.

G&D will be a UniCredit group-wide strategic partner for providing the full spectrum of modern payment cards, including dual-interface cards and comprehensive payment services. The UniCredit Group is an internationally active financial institution and one of Europe's biggest banks, with 160,000 employees.

Besides supplying state-of-the-art debit and credit cards to UniCredit, G&D will also provide technical consultancy and card personalisation services.

FIME First to Offer New EMV Test Plan

FIME, worldwide supplier of test solutions for smartcards, RFID and NFC, is the world's first organisation to obtain a full EMVCo qualification for the implementation of the EMV 4.2c test plan.

The EMV 4.2c library is now available for the EVAL tool. With the latest addition, EVAL enables laboratories to offer EMV 4.2c Type Approval testing and terminal manufacturers to test the compliance of their products.

EMV specifications ensure the worldwide interoperability of terminals and smartcards, mobile payment and contactless payment applications.

The EMVCo test process is divided into two levels: Level 1 testing which is required for the physical, electrical and protocol layers of a terminal and Level 2 testing which is obligatory for terminal applications.

L-1 Identity Launched New Set of Biometric Access Control Devices

L-1 Identity Solutions, Inc. announced a new set of high quality, low cost access control products - 4G V-Flex Lite, 4G CR-Pass and 4G SecureControl, designed to increase efficiency and lower the cost of access control installations.

4G V-Flex Lite is an access control device that uses fingerprint recognition or fingerprint and card-based authentication for identification in multi-door enterprise systems or stand-alone door access control deployments. The product includes multiple authentication options, template storage capacity of 5,000 in 1: N or 25,000 in 1:1 and a 500 DPI optical sensor.

The 4G CR-Pass is a card reader that can be used in environments with biometric and card reader-only devices, all of which can be managed on the same platform for significant time and cost savings.

4G SecureControl is a door control module placed on the secure side of the door to provide added security for single door access locations.

All these new reader products are IP 65 rated allowing for indoor or outdoor use, and include biometric capabilities and option to use card-only access for installations that require a mix of biometric and non-biometric devices.

White House to Issue Internet ID's

The US Department of Commerce has plans to introduce universal internet ID's through the National Strategy for Trusted Identities in Cyberspace law.

It will be the first time any government has sought to provide a single form of digital identification for internet users, coded to provide a form of filtered identity information, giving out only as much information as needed depending on the type of online transaction.

For example, whether buy a bottle of wine or voting online, the digital ID would verify that you are over the legal drinking age or have the right to vote.

One of the advantages of the ID's is that users would no longer have to remember myriad passwords for different transactions. Websites that use the strategy to authenticate identity would carry a small icon on their pages, similar to retail and banking sites which announce they use encryption software to safeguard transmitted information. The internet ID also aims to put a brake on cyber crimes such as identity theft and online fraud.

White House Cybersecurity Coordinator Howard Schmidt told CNET.com there's no chance "a centralized database will emerge" and stresses that anonymity will remain on the Internet.