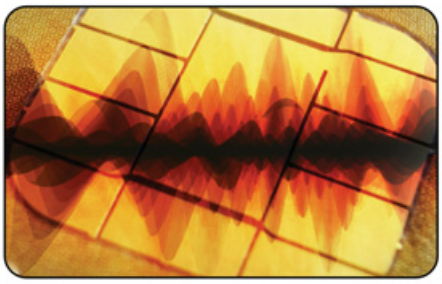
May 2009

Volume 18 • Number 5

Smart Card & Identity News

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

www.smartcard.co.uk



UK ID Cards Open Way for Taxman to View Our Spending

Forget the public furore over fraudulent spending by MPs revealed by the Daily Telegraph this month because the Daily Mail has spotted new Orders that have been laid before parliament to give Commissioners for Revenue and Customs access to the planned National ID card's audit logs.

These logs record every time an ID card is used to verify a person's identity when they make a large value purchase, open a bank account or take out a mortgage. In addition it is proposed that the card should be used for new job applications thereby alerting the taxman as to how many jobs you have compared with what is claimed. You might argue that this invasion into our personal spending habits is all a step too far?

Continued on page 4….

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

Head Office: Smart Card Group, Suite 3, Anchor Springs, Duke Street, Littlehampton, BN17 6BP

Telephone: +44 (0) 1903 734677

Fax: +44 (0) 1903 734318

Website: www.smartcard.co.uk

Email: info@smartcard.co.uk

Editorial

Managing Director – Patsy Everett

Technical Advisor – Dr David Everett

Production Team - John Owen, Rebecca Kimberley, Lesley Dann.

Contributors to this Issue – Tom Tainton, Rebecca Kimberley, Peter Tomlinson, Peter Hawkes, David Everett

Printers – Hastings Printing Company Limited, UK

ISSN – 1755-1021

Disclaimer

Our Comments

Patsy Everett

Dear Subscribers

This month's news is an interesting dichotomy of what appears to be two diametrically opposed security views. On the one hand we have more and more databases appearing which hold our personal and confidential data and which seems to lack the sort of security we might reasonably expect. On the other hand we have the security industry further winding up the security of smart cards (see news about Cryptography Research's new DPA license deal with Mastercard).

It seems to me that the security of smart cards has reached some plateau where they are not going to be easily hacked, we don't even hear much about pay TV smart cards any more. But then in the opposite direction we have (in the UK but also other countries) major moves by Government (see this months lead article) to set up sensitive data bases that nobody believes can be kept secure. Call me old fashioned if you like but aren't smart cards all about identity and authentication and a means to access sensitive data whether financial or personal? Hidden away in the UK Governments security framework documents are requirements for 2-factor authentication for accessing sensitive data that somehow or other never seems to make it down to the practical implementations.

And then of course I worry about making payments on the internet or doing anything else on the internet come to that. People keep on telling me that mobile phones will be the way of the future but will they be any more secure?

The Home Office is now proposing to use chemists, postmasters and photo shops to take your fingerprints for the new ID card scheme. Have I missed something here? Does anybody seriously believe that putting this sort of functionality into the hands of unregulated or unsupervised private companies is going to provide a reliable ID card scheme? To me this is just a bit more misunderstanding of human nature, there is already a concern about the quality of the passport data, this would be a free for all where everybody would have a route for getting an ID card or somebody else's data to suite any nefarious purpose and this might end up being the main reason for acquiring the card in the first place. In fact you can't help but think that the average person will just not bother while there will always be a band of collectors who will just want a card for keepsake, perhaps as a rare antique when the whole scheme gets scrapped.

Apparently the launch area will be Manchester and hang on there not just yet but due to start in the autumn. I always like the use of Seasons because you can stretch the date quite easily, perhaps not to you and I but autumn has been known to extend to December! Jacqui Smith the current Home Secretary (in these turbulent times anything may change) is due to announce this month that she is in discussion with the Post Office, the National Pharmacy Association (which includes Boots the Chemist) and the Photo Marketing Association to provide enrolment centres.

I had another idea, why not include driving licence test centres? There are lots of these dotted around the country and perhaps the government could save a bit of money by combining ID cards with driving licenses?

Patsy.

Contents

Events Diary

June 2009

9 – 10	RFID Smart Labels 09, San Francisco, USA – www.idtechex.com/rfidusa09
15 - 19	Prepaid 09 Conference & Expo, The Brewery, London – http://www.prepaid-conference.com/contact-details
16 – 18	CardExpo Africa 2009, Lasos, Nigeria – http://cardexpoafrica.com
18 – 19	Cards & Payment Europe 2009, Prague – www.cpeurope.com
22 – 24	Contactless Card 2009, London – www.smi-online.co.uk/events/overview
29 – 1	Prepaid Europe, Vienna – www.iirusa.com
30 – 1	EMV User Meeting, Sheraton Arabellapark, Munich, Germany – www.emvco.com/munich

July 2009

6 – 7	The Future of Cards and Payments, Le Méridien Piccadilly, London – www.marketforce.eu.com/cards

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

…. Continued from page 1

There are many things people do (legitimately) that they may not want to get into the public domain and somehow or other past government experience with managing our personal data suggests that it will get published or at least lost on some laptop or memory stick. VIPs should seriously worry here because their spending habits will be a target of all and sundry.

There are of course other spending behaviour patterns that might alert the taxman to new sources of income, perhaps we could use the UK Parliament's Green Book of expenses as an example of where most payments apparently are within the rules no matter how outrageous they might appear at first sight.

Every time a check is made using the ID card it will be logged on the National Identity Register and therefore made available to the taxman. Companies apparently will be charged 60p to check details held on the database (includes prime address, NI number and second homes) for which officials are hoping will account for up to 770 million verifications per year according to the Daily mail. Further details suggest that 44,000 organisations would be accredited to undertake the verification tests including government departments, banks and other financial institutions, mobile phone shops and video rental stores to name a few.

Companies are being told that by using ID verification they can cut millions from their annual fraud bill and can also avoid being prosecuted for employing illegal immigrants. For the Citizen it is clear that an ID card will avoid all the kafuffle of having to present a driving license or passport – or does it?

The trouble with the ID card project is that people are becoming more and more disillusioned as to why they need it, when do I use it, for what purpose? And then once you fail to be convinced of any positive benefit you start to look at the downside and the disadvantages seem to increase the further you look. This latest bit of proposed legislation inviting the taxman and other government departments to monitor our private habits which in most cases are probably perfectly legitimate is just not going to wash. In fact if you were into Machiavellian conspiracies you might imagine it is a deliberate ploy to get enough public support to kill the project. Perhaps the government is not listening very well, they already have enough support to quietly drop it off the books.

So the question is what impact does all this have on the plethora of vendors waiting for a slice of the action in the ID card space?

So far Thales, CSC and IBM have won contracts to supply parts of the scheme. Fujitsu and EDS are also on the shortlist and can bid for further contracts expected to be awarded over the next year.

The Home Office estimates the National Identity Scheme will cost £5.4bn over the next 10 years and argues that 70 per cent of these costs would be needed to support new passport systems regardless.

The smart card suppliers are of course much lower in the value chain and I suspect are not getting too excited about the latest launch of ID cards in Manchester later this year using Post Offices and Chemists. The volumes involved are unlikely to be earth shattering. As for the new passports, well at least they now all include an RFID chip albeit that the security mechanisms don't yet seem to be agreed at the national let alone the international level. Has anybody heard of an international Certification Authority for passports?

Dr David Everett, Smartcard & Identity News.

World News In Brief

Companies Warned on Over- reliance of Payment Card Industry's Standard

Corsaire an independent expert in securing information systems has warned businesses against over-confidence that the Payment Card Industry's Data Security Standard (PCI DSS) will keep their customers' data safe. The announcement comes in the wake of several recent security breaches, including those at Heartland Payment Systems and other firms that had successfully passed their PCI DSS assessment.

The PCI DSS is a set of specific requirements for enhancing payment account data security. The standard was developed by the PCI Security Standards Council in order to help facilitate the broad adoption of consistent data security measures. Founding members of the Council include American Express, JCB International, MasterCard, and Visa.

The PCI DSS outlines the regulations that organisations should follow if they expect to process debit and credit card payments. Compliance with these standards covers everything from ensuring that organisations are building and maintaining secure networks, to having an information security policy in place to protect cardholder information.

"First of all, let me say that - if used correctly - the PCI DSS can provide a valuable, base level of data security," says Jane Frankland, Commercial Director, Corsaire "However, the PCI DSS was never meant to be a security programme in itself: it was actually intended to formalise contractual requirements for minimum security within organisations that must interact with the banks and credit card companies. However, the PCI DSS has been often used as form of public seal of approval, to show that an organisation is secure - and that isn't necessarily true."

According to Corsaire, computer 'hackers' will exploit all areas of weakness, and will in fact go to extraordinary lengths to compromise a financial application, as the spoils are just too tempting. Any applications which process financial data, therefore, should have proportionally higher requirements for data confidentiality and transaction integrity.

Frankland adds. "After all, just because somebody has a driver's license, it doesn't necessarily mean that they're a good driver."

Heartland to Contest MasterCard Data Breach Fine

On the 20th January Heartland Payment Systems Inc reported a data breach of more than 100 million credit and debit card account details, the largest data-loss in history(reference: January's SCN Newsletter).

This month, Heartland Payment Systems reported their first quarter results revealing that they have incurred $12.6 million in various expenses and accruals, all of which are attributable to the processing system intrusion in the first quarter.

The majority of these expenses relate to a fine imposed by MasterCard. The fine was imposed due to Heartland allegedly not taking appropriate action subsequent to learning of the possibility of the breach

Robert Carr Heartland CEO says "they will vigorously contest any effort to hold us liable for the MasterCard Fine. We believe we took immediate and extraordinary actions to address the intrusion and cooperate with the card brands investigation of the intrusion, and that we responded appropriately to concerns that were raised leading up to the discovery of the intrusion".

One wonders what the total cost of this breach will cost Heartlands, remember TK Maxx their total cost was over $118 million in fines and court cases.

Toshiba to Reduce Production of Semiconductors

Toshiba Corporation announced continued adjustment of production at its semiconductor plants for the first quarter of FY2009 (April to June, 2009). As a measure to improve the profitability of its semiconductor operation, the company has been implementing working hour adjustments and a leave system for employees in the business since February. For the period April to June, the adjustment will average approximately 6.8 days and it will be applied to some 19,200 employees of Toshiba and its Group companies in Japan.

Toshiba will continue to adjust production volume for NAND flash memory at its Yokkaichi Operations plant in Mie prefecture, Japan during the first quarter of FY2009 (April to June, 2009), and maintain the production level established in January (approximately minus 30%).

NEC Electronics and Renesas to Integrate Business Operations

NEC Electronics Corporation, Renesas Technology Corp., NEC Corporation, Hitachi, Ltd., and Mitsubishi Electric Corporation have agreed to enter into negotiations to integrate business operations at NEC Electronics and Renesas.

NEC Electronics was established in 2002, separating from NEC, and Renesas was established in 2003, integrating semiconductor units at Hitachi and Mitsubishi Electric.

NEC Electronics and Renesas have agreed to explore the possibility of business integration in order to further strengthen their business foundations and technological assets while increasing corporate value through enhanced customer satisfaction.

The new integrated company will have three major product groups, MCUs, SoCs, and discrete products, and will become the world's third-largest semiconductor business. The new company will select and focus on the development of projects covering a diverse range of fields and will expand its comprehensive line-up of globally competitive products.

The preconditions for holding future negotiations are to integrate business operations on April 1, 2010, and to maintain public listing for the new company.

The new company will announce the company name, the location of its headquarters, the corporate representative, the board members, capitalization, total assets, and financial forecasts following the integration.

NEC Electronics and Renesas plan to sign an agreement at the end of July, 2009 to integrate their business operations.

NXP Semiconductors Sales Down 29.4%

NXP Semiconductors announced first quarter sales of USD 673 million, a comparable decrease of 29.4% from the fourth quarter of 2008.

During the period significant progress has been made on execution of the large-scale Redesign Program announced in September 2008. This program is focused on making necessary changes to withstand the significant weakness prevailing in the industry and to optimise the businesses to help deliver NXP's longer-term strategic objectives. The program is now forecast to have restructuring costs of no greater than USD 700 million and is expected to achieve higher annual savings than those initially projected (USD 550 million) by the end of 2010. While the cash expense of the Redesign Program will remain the same in total, the cash-out for the Redesign will increase significantly in the next quarters.

NXP Semiconductors, also announced this month that, Ruediger ('Rudy') Stroh will join NXP as General Manager of the identification business.

Sagem Sécurité to Provide Solution for Biometric Passport in Croatia

Sagem Sécurité (SAFRAN Group) this month announced that its subsidiary Sagem Identification has been selected by the Croatian high-security printing house, the Agencija za komercijalnu djelatnost (AKD), to provide the polycarbonate data page with integrated chip technology for the new Croatian biometric passport. Croatia is moving to a new highly secure electronic passport solution in order to comply with international standards.

Sagem Sécurité has already helped with 7 other European passport implementations. Deliveries will commence as early as of spring 2009. "We are both proud and honoured to earn the trust of the Croatian customer and government," said Anko Blokzijl, Chief Executive Officer of Sagem Identification.

Con-Artists Target Bank Customers By 'Smishing'

Attorney General of the state of Missouri, Chris Koster has been highlighting the essences of a new phishing scam, "smishing".

Much like phishing - and a take-off on its name - the only difference with this scam is the con artists uses a text message to contact would-be victims on their wireless phones. The name uses a combination of phishing and SMS (Short Message Service), which is the technology behind text messaging.

Rockwood Bank customers have been targeted by an onslaught of text messages that appear to be from the bank, telling the customers their accounts have been "locked," and that they need to call a free-phone number to reactivate their accounts. The text messages are bogus, and when customers call the number they are asked to supply sensitive banking information.

"These thieves will use whatever deceptive methods they can to steal people's financial information for their own gain," Koster said. "Consumers must be very careful to protect their sensitive personal information, such as Social Security numbers, bank information and credit card numbers."

Effective spam filters have not yet been developed for cell phone text messages. Very few text messages are blocked by filters or cell phone providers. Whilst e-mail messages that are misspelt and contain broken address links, making it easier to identify spam, determining whether a text message is legitimate may be difficult, as there are no images and the message is usually short.

Internet Data Increases Faster than NASA's Space Rockets

Following the explosion of social networking sites, internet-enabled mobiles and government surveillance, the world's store of digital content is now the equivalent of having one full top-of-the-range iPod for every two people on Earth.

The rapidly expanding digital content, which currently stands at about 487bn Gigabytes (GB), would form a stack of books (if the content was to be printed and bound) that would stretch from Earth to Pluto tenfold. As more people are joining the digital tribe, including through increasing numbers of internet-enabled mobiles, the world's digital output is increasing at such speed that the stacks of books would rise quicker than NASA's fastest space rocket.

70% of the information held is created by individuals and include phone calls, photos, emails, online banking and social networking postings. Rapid increases in machine-to-machine communications, such as the Oyster Card, have also contributed greatly to this quantity.

The Digital Universe report shows the world's digital content was 161bn GB in 2007. Now this is likely to double over the next 18 months, according to research from technology consultancy IDC and IT firm EMC.

Britain's Cashless Society Unlikely

A report this month has suggested that Britain will never evolve into a cashless society. The study carried out for ATM operator Bank Machine shows that the long term impact of the current financial crisis will take affect on people relying on the tangibility of notes and coins, to which we count on for local newsagents, caf?s, fund-raisers, collection tins and pocket money.

The report,"Paying in cash: more than the strange pastime of a few," was analysed by James Woudhuysen, Professor of Forecasting and Innovation at De Montfort University, Leicester. It argues that a society with exclusively electronic payments would cause activities like these to disappear from our lives, as the electronic payment methods would be too costly to install and not financially viable.

At the same time the resistance to change from an ageing population, concerns about a surveillance society, retailer resistance and Britons' attachment to sterling will all ensure cash continues to be widely used. The report added that the removal of notes and coins from our lives would also have a knock-on effect on many activities as it would not be commercially viable to install contactless payment systems for these events.

G&D Prototype Self-service Machine

Giesecke & Devrient (G&D) presented the first functioning prototype of its new Instant Issuance Kiosk for payment cards at the Visa Europe Member Days in Berlin. The exhibited product is a self-service machine for private customers, who can use it to issue their own prepaid cards.

The machines can be installed - at train stations, airports, shopping centres, football stadiums, or in the self-service area of a branch bank. This solution enables banks to significantly expand their service offering and improve customer loyalty, while also tapping new business segments and target groups. G&D presented the prototype in collaboration with Visa Europe, Wirecard Bank AG and the issuing processor Cetrel S.A.

Customers will be able to acquire a ready-to-use prepaid, debit, credit or contactless card any time, any place, and use it to shop in retail stores and online. This solution will also enable bank customers to quickly and conveniently replace lost or stolen cards whenever they need to.

Reflections on the Security Document World Conference

By Peter Hawkes, Smartcard & Identity News

Peter Hawkes, BSI Biometrics Committee Member

This was the third in the annual series organised by Mark Lockie and his team at Science Media Partners. It took place on March 26 and 27. The venue was the QE2 Conference centre in Westminster, London. The associated Exhibition was sold out with 60 stands. For the Conference Mark had assembled a cast of 43 speakers and 10 session chairmen. They were drawn from governments and their suppliers from across the world. Two presentation tracks ran in parallel for most of the two days. Inevitably this meant that I missed nearly half the talks.

Hopefully I shall be able to comment on these when I receive the CD of the proceedings promised by the organisers. The delegate manual contained no written papers and few synopses.

This lack of pre-prints seems unavoidable these days. The Speakers present their latest thoughts as slides. Consequently a Delegate has little opportunity to reflect on the material presented before posing any query. This makes for limited discussion after a talk.
There are of course further opportunities for discussions in the coffee and lunch breaks. But these must be cut short to make time to visit the Exhibition stands. The event was well attended. About 2000 visitors came to the exhibition. There were 270 conference delegates.

Highlights of the Conference

1/ Open-ness

Governments were remarkably open about the possible vulnerabilities to forgery and counterfeiting of their Security Documents and associated systems. Suppliers were equally open about at least some the Countermeasures they are deploying to detect and deter criminal activities.

2/ Limitations of e-Documents

Most suppliers of e-passports and like security documents conforming to ICAO's Mandate remain wedded to new and improved Physical security features. One reason for this is that the ICAO Logical security features in the document chip such as time limited digital certificates are vulnerable to poor administration by the passport issuing State. If certificates are not renewed in time Receiving States must rely on Physical Security Features to establish passport validity.

Another reason is that chip stored data in e-passports and like documents is normally only readable by Government Readers. Readers belonging to Non-Governmental organisations cannot read the chip-stored data. Inter alia this restriction helps protect the personal privacy of the Authorised document holder. A side effect is that non-governmental organisations checking Government e-documents must rely on the available (physical) means for the detection of forged or counterfeit e-Documents.

Hopefully this limitation on "private sector" Readers while be overcome in the medium term.
One way to do it would be to have two logically separate data storage areas in the chip of e-documents. One area would be for use by Governments. The other would be for use by commercial organisations. The design of the latter would incorporate relevant safeguards for the maintenance of personal data protection. For example it might be good enough for the commercial area to contain an appropriate digital certificate and no personal data whatsoever. This would not indicate the status of a document that had been revoked. However this could be checked on-line.

3/ Significant points made by Session Chairmen and Speakers

(a) "Identity is Relationships"- Aside by a Session Chairman
(b) "Biometrics is about Interoperability and (sample) Image Quality."-aside by another Session Chairman
Point (a) is quite profound.

Point (b) was recognised in the earliest activities of the ISO committee on Biometrics- SC37. Working Group 3 of SC37 has already developed 9 published ISO standards in the series ISO 19794-X "Biometric Data interchange formats". These common file formats for biometric images are essential for Interoperability. They cover the commoner types of biometrics. More are in the development pipeline. See Reference 1 below.

Sample image data quality must be maintained or performance will deteriorate. Again SC 37 is developing relevant standards.

(c) "IPS is committed to on-going R&D activities. This is not least because the war between us and the criminals will continue indefinitely" – Duncan Hine, Director of Integrity & Security, IPS in his talk "Biometric Enrolment and the National Identity Scheme".
This serves as a timely reminder that whatever security features are adopted for ID cards and passports the criminals will sooner or later find ways to subvert them.

(d) Bob Carter of IPS gave us an update of his talk last year on Extended Access Control (EAC), "EAC is here now - the vision becomes reality". EAC was devised by BSI in Germany. It is based on time limited digital certificates stored in Government Readers and e-passports. There is mutual authentication of Reader and e-passport chip. Accordingly it meets ICAO's recommendation for an international e-passport system which safeguards the personal data held in the chips of e-passports and like e-documents. The first UK documents to operate under EAC will be UK ID cards issued to foreign residents. UK e-passports will become EAC based in 2012.

What was not well covered in the Conference

It was disappointing to hear little about the personal privacy issues associated with Security Documents including ID cards and passports.

Highlight of the Exhibition

Bearing in mind the Privacy issue just mentioned my choice for this highlighting was the stand of Priv-ID B.V. of Eindhoven. Their Web site is www.priv-id.com
I managed to talk to the founder, Dr Tom Kevenaar. Whilst working in Philips Research Division he and his team devised and patented their ideas for a new form of "Revocable Biometrics"- sometimes called "Traceless biometrics" or "Biometric (key) encryption". Revocable biometrics is not a new concept. However Priv-ID's approach seems novel and promises much.

The company has been spun off from Philips as a separate entity with Philips retaining a small share stake.
As the company name implies the privacy of personal identity data is safeguarded. This is achieved by the use of a one-way function to form a template from biometric image data such as a digitised fingerprint. Comparison between a sample live-scan fingerprint and the template allows 1-to-1 authentication of an ID card-holder. However "1 to many" searching of the sample against images in a fingerprint database is said to be "impossible". In technical terms the transforming function used is "non-invertible".

The sample units on the Priv-ID stand showed the system working with fingerprints. The template per fingerprint or other biometric image is quite compact- a few hundred bytes. So it can be stored as a printed 2-D bar code or in a low cost RFID tag. Such tokens are disposable and can be anonymous. This opens up possibilities for "disposable" uses such as for Boarding passes or in one-time pads.
It was not clear to me how proprietary technology like Priv-ID's and similar from it's Competitors can be used in future ISO standards and ICAO mandates. No doubt ways will be found.

Conclusion

Last January Mark Lockie wrote to prospective delegates about this conference. In his letter he promised that SDW 2009 will help interested people to find answers to questions such as "Do you understand how secure documentation and exchange of data will be crucial to combating organised crime, terrorism and human trafficking?"

In my opinion he and his team achieved what they promised. When one "opened the tin" the content was every bit as good as the picture on the label. That is pretty rare in today's world of marketing hyperbole.

References

- The British Standards Institute now has a Biometrics Web site for the activities of it's Biometrics Committee IST 44. See:-
  www.bsigroup.com/en/Standards-and-publications/Industry-Sectors/biometrics/
  Note that IST 44 is the UK's mirror committee of ISO's SC37 "Biometrics" committee.
- For details of next year's repeat of the Security Document World Conference see:-
  www.sciencemediapartners.com

World News In Brief

NXP and G&D Launch Contactless Fast Pay Solution

NXP and Giesecke & Devrient (G&D) have announced the introduction of NXP's new Fast Pay contactless security chip and a new line of G&D contactless payment devices based on this IC. Fast Pay-based devices have been specifically designed to provide consumers in the USA and Canada with a convenient and swift contactless payment solution.

In 2008 alone, over 70 million contactless smart cards were issued in the USA and this annual number is expected to rise to 100 million over the next 3 years. The new chip will be widely used for contactless payment applications, such as in G&D's Visa payWave and MasterCard PayPass cards. The EMVCo approved chip offers a Data Encryption Standard (DES) hardware co-processor.

Commonwealth Bank of Australia set to Push Contactless Payments

The Commonwealth Bank of Australia (CBA) is set to install 5000 contactless payments readers across the country this year, following a successful trial.

The trial enabled participants to make contactless payments of up to $35 AUD. Retailers participating in the trial included McDonalds, restaurants and cafés.

The CBA is now looking to roll out thousands of terminals, which will work with credit cards using the MasterCard or Visa contactless technology. The transaction limit may also be raised to $100.

US Missile Launch Data on eBay Hard Drive

Credant Technologies say that revelations about a hard drive purchased on eBay - which reportedly contained the launch procedures for a US military air defence system - is extremely worrying.

"This is obviously a serious lapse of security procedures for the agency concerned, but the worrying aspect about the incident is that it may not be a one-off. US government agencies - and, indeed, all government agencies worldwide - should have a policy of crushing hard drives once they have been removed from office PCs," said Michael Callahan, Credant's senior vice president.

"But this isn't a one-off situation - if we go back to April 2006, there was the well-publicised incident of a flash drive with US spy data being sold in an Afghan bazaar for just $40. The ensuing investigation into that incident revealed the fact that the data had been downloaded from an unencrypted hard drive," he added.

And the lack of encryption - rather than a lack of enforced policies on disposal of old drives - is the root cause of this latest security incident, he says.

If the data on the PC used in Afghanistan in 2006 had been encrypted, as had the data on the drive reportedly sold on eBay, then the ensuing press embarrassment for the US military would not have happened.

"I suspect that the investigation by BT's security research centre and a number of international universities will reveal other serious security failures with hard drives," he said.

Nokia Release its 3rd NFC Phone

Nokia announces its third fully integrated Near Field Communication (NFC) device, the Nokia 6216 classic. The new arrival is Nokia's first SIM-based NFC device which enables operators to build NFC services on to the SIM card. With NFC consumers will benefit from greater ease of use, more

convenient sharing of content - such as images, web links, audio files or contact data - as well as secure payment and ticketing transactions, all with just one tap of the device. The Nokia 6216 classic is expected to start shipping in the third quarter of 2009 in select markets.

"The Nokia 6216 classic will be amongst the first commercial devices in the market complying with operator requirements using the SIM card in connection to secure transactions with Near Field Communications," says Jeremy Belostock, head of near field communications at Nokia. "With the Nokia 6216 classic in your pocket and the ticketing applications on the SIM you can replace the multitude of cards in your wallet. Having the applications on the SIM consumers can bring their secure applications to their next Nokia NFC enabled phone."

Fraud Trends Increase Dramatically

The analysis of fraud trends during the first quarter of 2009 by CIFAS - The UK's Fraud Prevention Service - reveals some particularly alarming patterns.

During this quarter, a staggering 75% increase in facility takeover (also known as account takeover) frauds - where the fraudster gains access to, and plunders the legitimately obtained accounts of innocent victims - continued the steep upward trend seen throughout 2008. This type of fraud is particularly traumatic for the victim, as the impact goes far deeper than any financial losses. The sense of uncertainty inflicted upon victims often undermines their sense of security and well-being as fraudsters leech off of their accounts.

A 40% increase in the number of people being impersonated indicates that the flat trend seen in 2008 (where identity fraud increased by only 0.06% from 2007) was exceptional. While last year's figures were a surprise, the sudden and significant increase in the first quarter of 2009 heralds an unwelcome return of identity fraud as the fraudsters' method of choice; as fraudsters assume creditworthy identities in order to swindle individuals and companies alike: stealing funds, goods and services at someone else's expense.

Richard Hurley, CIFAS Communications Manager, explains: "It is a commonly held view that fraud rises to the surface during times of economic recession, and these figures substantiate that. With the alarming rise in identity fraud, we are faced with the possibility of a 'chicken or egg' situation: are these increases caused by - or uncovered by - the recession, as lenders and other businesses look even more closely at their existing books?

TSSI raises concern over UK ID card scheme launch

Identity specialist TSSI has branded the new government-led ID card scheme to launch in Manchester as premature. Home Secretary Jacqui Smith has stated that anyone over 16 in the city with a UK passport will be able to apply for a card from the Home Office from Autumn 2009. "The scheme works on the assumption that people will apply on a voluntary basis although it is not entirely clear what the immediate real benefits to members of the public are," said John Barker, TSSI Systems Ltd.

"It is estimated that the ID cards will cost between £30 and £60 each to produce at a time when the government is focused on curbing public spending. Advocates of the scheme point to the benefits of personalised public services, but this relies on the appropriate supporting systems being in place which could take up to five years to develop."

"The estimated cost of the project to the Home Office is about £5bn, but Dr Whitley of the London School of Economics estimates that the last four years has already seen astronomical costs of between £10 and £20bn. With spiralling costs it seems that the government has already bitten off more than it can chew."

"One of the arguments for the introduction of ID cards is that they can help combat impersonation, ID theft and fraud. However, the Government's proposed ID card scheme does not go far enough to address this issue. Stronger verification technology needs to be in place. Biometric technology alone does not suffice to prevent fraud. For example, the Dutch biometric passports were cracked soon after launching, despite strong encryption. Unfortunately, there is no such thing as a 100% secure solution – and saying you've got one is an open invitation to hackers! All you can do is minimise the risk as far as possible."

"What's needed if the ID card scheme is to work is a belt and braces approach. Storing the data as an algorithmic encryption makes it impossible for even the most sophisticated fraudster to read or substitute. Even authorised personnel – and therefore any successful hackers - would only be able to view binary code, and not the finger, iris or facial data itself. They would also be unable to replicate the algorithm to clone the card. However, this method of encryption goes beyond the scope of the ID cards currently proposed."

"With the UK in the midst of a recession and projected cost of the scheme seemingly escalating as well as potential gaps in the security of the technology, is this really the right time to be launching an ID card scheme?

SCN IAAC Workshop – Power to the People: Information Assurance

By Peter Tomlinson, Iosis Associates

Peter Tomlinson

The afternoon of Wednesday 12th May was spent at a Workshop run by the Information Assurance Advisory Council (IAAC). The subject was People-Centric Information Assurance, the place was the BCS London office, and this was the second session. We operated under the Chatham House Rule – we can report what was said but not who said it.

Information Assurance (IA) in ICT systems and services is the name for a Cabinet Office policy, created in the early days of this century. Those were the days of the eEurope Initiative, the UK's eEnvoy, and the National Smart Card Project. IA is a mix of Information Security and Service Quality, intended to underpin all eServices operated by or for the public sector, perhaps also for all those private sector eServices regulated by government. Its visible manifestation is intended to build on a behind-the-scenes implementation across internal government ICT services, and indeed a great deal of background work has been done under the CSIA banner. Despite two recent conferences (IA 07 and IA 08), so far there has been very little obvious impact on citizen services, and the visions from around 2002 are still just visions. Those conferences, we heard, asked for more regulation of eServices to the public – that looks like the topic to be taken forward, and indeed the call for more and independent regulation (instead of micro-management by Whitehall) is being widely heard, not just for eServices but also in many other areas of citizen and business services.

Information Assurance Advisory Council

IAAC

IAAC: www.iaac.org.uk
"IAAC's aim is to work for the creation of a safe and secure Information Society. It is a unique, not for profit body with high level support from government and industry backed by world class research expertise."

The first Workshop session, last November, had started with a clean sheet. The subjects were divided into the problem space in our increasingly digital society (people, their lives, expectations, understanding, and the risks that they face) and the solution space for internet based personal services. Personally, having seen the concentration on the internet in the IA 07 papers, I am with others who commented at the time: ICT penetrates far more into our lives than just internet delivered services, and that penetration will increase – think mobile phones, NFC, smart cards just for starters, think of the internet of things communicating as and when they will. That 2007 reaction was a warning for the frustrating, tunnel vision experience to come last week as we started to look for solutions that deliver IA. It was towards the end of the afternoon when we finally divined that the view from the centre is still characterised by the binary model of 'us' (the government) and 'them' (the public). Government IA wonks in the UK, and the IAAC, still have a long path to tread before they understand how to build and operate a layered model of legislature, executive, regulator, and service provider, with competence at every layer.

MasterCard Caves in to Cryptography Research Inc

By David Everett, Smartcard & Identity News

David Everett

It may seem a long time ago that Paul Kocher and his team at Cryptography Research Inc (CRI) came up with Differential Power Analysis (DPA), a smart way of breaking the cryptography of smart cards by analysing the power signal feeding the smart card chip.

It all happened back in 1998 when Paul Kocher, Joshua Jaffe and Benjamin Jun published their findings whilst taking out some patents on techniques for mitigating this DPA vulnerability. CRI have been selling licences ever since. Well not quite, nothing much happened until last year when Infineon rapidly followed by Renesas and NXP (representing three of the top smart card chip manufacturers but note that ST Microelectronics is missing from the list) signed up for a licence deal with CRI. You can read more about the Infineon licensing deal in August 2008's Smartcard & Identity News Letter (SCN).

But it's not just at the chip end there have also been disputes with Visa and Mastercard. Visa settled in September last year and now MasterCard has followed suite but with a totally different form of agreement with CRI.

In 2004 CRI filed a complaint in California claiming that Visa used its pull in the credit card industry to exclude CRI's solution to a smart card security defect in order to avoid paying licensing fees. Visa originally had a licensing agreement with CRI see SCN November 2006, but terminated that agreement and allegedly conspired with MasterCard, creating a buyer's monopoly in order to eliminate standards that integrated CRI's solution to the security defect.

According to Darren Donnelly a patent Attorney for Fenwick & West who were pursuing the CRI patents "The manufacturers who provide the smart cards have to have standards of security protection approved, EMV Co. used to have this standard, but when we protected our patents, [Visa] pulled it out of the standard in favour of something that didn't have this countermeasure,"

On September 23, 2008, CRI and Visa settled their differences and announced that they have signed a definitive agreement under which Visa will become a licensee of Cryptography Research's patent portfolio covering countermeasures to Differential Power Analysis (DPA). The license fee and other settlement terms are confidential per the agreement. What we do know is that there was a substantial down payment and one also suspects an additional license fee per chip which is CRI's normal licensing arrangement.

What this means is that when a bank buys a smart card for use as a Visa branded card the DPA licence fee is paid for by Visa. Neither the card manufacturer nor the chip manufacturer is liable for the fee. In the case of Infineon, Renesas and NXP they would be absolved from the license fee payment under their separate agreement with CRI.

The MasterCard agreement is however very different. Under the agreement, MasterCard will require that vendors of smart cards and other cryptographic products that utilize DPA countermeasures be licensed from Cryptography Research in order to be used on MasterCard's payment networks.

Mastercard have financially compensated CRI for this agreement which seems to be far more about resolving the past disputes than any agreement for Mastercard to take on the licensing position for the banks when using DPA protected chips for MasterCard branded cards. It is a recognition that the CRI patents on DPA protection are valid and should not be infringed. By implication of the statement in the press release they are also all encompassing, what happens if ST Microelectronics believes that their chips are resistant to DPA without employing any of the CRI patented countermeasures?

Many congratulations to CRI, they have fought a long and hard battle and most of the major players have succumbed albeit in strangely different ways.

Smart Cards Are Fundamentally Broken

By Rebecca Kimberley, Smartcard & Identity News

Jeremy Thorp, CEO of software conditional access(CA) specialists Latens, believes that smart cards for usage in set-top boxes are outmoded. This was the message Thorp brought to the latest 'Rapid TV News' Round Table on the cable TV industry.

The markets are increasingly receptive to software-based (and card-less) conditional access. "We've been pushing software conditional access for six years saying that this is the way the market's going to go and I think we've gradually seen that tipping over as we've demonstrated that we can do it successfully." said Thorp. "The traditional security model with a smart card is fundamentally broken with what's going on from a technology point of view."

Some Cable providers are already in the late stages of using card-less/security chip-less set-top boxes, with plans to deploy these over the next 2-3 years.

Pay TV cards are being increasingly hacked as people are trying to gain access to satellite television for free. USA Today, New York, released figures revealing that as many as 3 million households in the US get virtually every channel, including premium networks, sports and all pay-per-view services, for free and illegally.

Renowned hacker Chris Tarnovsky, former NDS employee (set-top box manufacturer for Sky TV), gave an interview with WIRED magazine at the end of last year revealing that Pirate dealers can claim $400,000 over a weekend selling Pirate Cards at around US$250, as well as demonstrating how to hack Smart Cards for Free Satellite TV, through fooling satellites into thinking that the Pirate Cards are genuine TV smart cards.

Pirate Cards are in abundance over the internet. After investigating on the internet, I have managed to easily find sites and forums that discuss Pirate TV cards. Forums reveal Satellite experts giving out website addresses and even inviting people into private messaging chat rooms and arranging payments through PayPal. To top that you can even purchase the Pirate Smartcard operating systems installer software to become a pirate card merchant yourself.

I, myself was offered a Pirate Card over an internet forum, for £150 plus £5 postage. The Australian eBay has also been spotted selling these pirate cards at 150 Euros and 10 Euros Shipping.

Cable businesses have fought back, attempts have been made to to block sensitive internet content and even look into the reason's behind large blank card sales to prevent card pirates. DirectTV fought back in January 2001, sending electronic signals from its satellites, destroying thousands of hacked cards being used on their services.

Raids are also being carried out on a large scale, with the main target being Australia, as the main stream of Pay-TV piracy seems to suggest. Criminal rings are being found to have set-top decoders, several computers and boxes of the fake pay TV encryption cards. The Brisbane Times reported last April that the Australian Federal Police made raids on 10 properties in Queensland, New South Wales and Victoria, seizing set-top decoders, AUD$169,000 in cash, and 18 boxes of illegal pay TV cards.

"The hackers now completely have the dominant hand there," Thorp added. "They've done it successfully once and I think that means that they'll be willing to drive to do it again with more of this sort of technology and that's going to earn them lots of money.

Hacking is one reason why subscription media providers are looking at alternative methods of security, but also as Thorp explained is that cable operators wish to offer services to more devices, not only the set-top box, the consumer in an environment full of devices wants the content to run across all the devices seamlessly. Thorp believes that the "card-based model will break down," with solutions being costly for the operators, who "just settle with being hacked for a very long time" and accepting the consequences.

A word of warning on using pirate cards- because pirate cards are mostly cloned cards, cables operators know they are in use. They are able to detect the use of hacked cards through duplicate identification numbers/keys

and could press charges for Satellite Fraud on those whom are found to be in possession.

Is software conditional access secure and the way forward?

Well, the security involved is a bit out of my scope to answer. However, whilst reading a student's Master's Thesis on "White-box Cryptography for Digital Content Protection," the author, Marjanne Plasmans mentions 'node locking,' to ensure that the software can only be used on particular hardware. Therefore hardware is still a factor in preventing copying and cloning, so could be problematic when upgrading/replacing a set-top box.

Links/Sources:

- Wired Online -Chris Tarnovsky - http://www.wired.com/politics/security/news/2008/05/tarnovsky
- Rapid TV News' Round Table - http://www.rapidtvnews.com/index.php/200905193881/latens-says-smart-card-ca-is-finished.html
- Brisbane Times - http://www.brisbanetimes.com.au/articles/2008/04/16/1208025271569.html
- USA Today - http://www.usatoday.com/news/acovmon.htm

World News In Brief

Databac Counters ID Theft with Contactless Card and Passport Shields

Databac Group this month released a range of products designed to help stop identity theft. The FIPS201-approved product family from US developer Identity Stronghold is designed to block unauthorised RFID reading of contactless cards, passports and driving licences.

Secure Sleeve and Secure Badgeholder products create an RFID shield by blocking the electromagnetic energy necessary to power and communicate with contactless smart cards, passports, driving licences and travel cards. While encased in the holder, the card or passport cannot be read or copied. It is only extracted when required, putting the user in control of where and when the card or passport is read.

"It is frighteningly easy to steal data from contactless cards," said Databac managing director Charles Balcomb. "Secure Sleeve and Secure Badgeholder are essential protection for any business serious about ID security."

Credit card readers can be easily purchased that will read the credit account number, expiration date and even the name off an RFID-enabled credit card. These readers can be concealed so that someone could walk through a crowd, ride on a train, lift or other crowded area and steal nearby credit card information without the cardholder ever knowing it happened.

While most contactless smart card systems implement industry-standard security mechanisms, readers can be modified to access information without authorisation, making the electromagnetic ally opaque shields essential to achieve total security.

Briton's Identities Bagged by Fraudsters

New research released earlier this week reveals that women who carry trendy oversized handbags are walking targets for fraudsters. The average size of handbags have doubled in the last 10 years and new findings from CPP, providers of card, mobile and identity protection, reveal that women are increasingly using these handbags to hoard valuable documents such as passports, bank statements and pay-slips.

With bag theft on the increase, the 'maxi-bag' has significantly increased women's exposure to fraud, with over 700,000 cases in 2008. Experts have warned about the dangers of overloading handbags with too much personal information, with more than 75% of women admitting that their bags contain papers with names, dates of births and addresses (83%) and 53% unaware what information a fraudster would need to steal an identity. Men are also targeted, with 1 in 10 carrying a 'man bag' and over 62% admitting to having sensitive personal documentation in their bags.

Top locations for bag theft include pubs and public transport, which both places stand at 29%, while 1 in 10 have been targeted in night clubs or shopping centres. Many people make it simple for fraudsters to steal bags, by leaving them unattended or on the back of a chair.

Last year, APACS, the UK payments association, card fraud totalled £609.9million up 14% on 2007 and CIFAS, The UK's Fraud Prevention Service, said there were over 62,000 victims of impersonation for the purpose of identity fraud.

Smart Card Vulnerabilities

By David Everett, Smartcard & Identity News

David Everett

This month is a special addition on smart card security vulnerabilities reflecting the significant advances that have been made in the last 10 years or so in the design of smart card chips for which the latest designs are truly ingenious. Many of these advances are also in a large way credit to Paul Kocher and his team who really exposed some major weaknesses and in particular timing attacks and of course Differential Power Analysis (DPA).

The story starts with TEMPEST (Transient Electromagnetic Pulse Emanation Standard) a U.S government code word that defines a classified set of standards for limiting electric or electromagnetic radiation emanations from electronic equipment. Microprocessors, computers, VDU's in fact all electronic devices emanate radiation through the ether or through electrical conductors. In the early 50's the U.S government became concerned that such radiation patterns may be collected and analyzed by an enemy. The use of cryptography could effectively be thwarted if the appropriate information could be successfully reconstructed. Research in the laboratory showed that such signals could be collected at some considerable distance from the source of the emanations and accordingly the Tempest program was started.

Although the subject of Tempest was well known in the defense world it entered the wider public domain with the publication of a land mark paper in 1985 entitled 'Electronic Radiation from Video Display Units: An eavesdropping Risk' by Win van Eck of the Netherland's PTT Research Laboratories. His paper showed the successful reconstruction of the image displayed on the target VDU captured at some distance away, even outside the building. It is the use of square wave signals and high switching frequencies in digital equipment that leads to the radiation of electromagnetic fields with frequency components extending into hundreds of megahertz. It is important to note here that although the spectral power of these signals decreases with increasing frequency, that the radiation effectiveness increases with increasing frequency.

The solution to this problem is equally well known and relates to the screening of the equipment by creating an effective Faraday Cage and the filtering of the signal and power cables to reduce their radiating capability. The levels required for such screening and filtering are part of the classified Tempest standard. In this particular case the designer of equipment receives expert advice on the level of protection required. The designer of cryptographic equipment needs similar advice from experts on the appropriate algorithms and the necessary key lengths.

In the world of cryptographic security another seminal paper was published in 1996 by Paul Kocher entitled 'Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS and other Systems'. In this paper he was able to show that by measuring the amount of time required to perform private key operations, that attackers could, in principle, find the key exponents and thereby potentially break the cryptographic system. Although such attacks are in practice somewhat difficult and adequate defenses are conceptually fairly straightforward, the issues raised have none the less much wider implications.

Also in 1996 Dan Boneh and colleagues from Bellcore highlighted the vulnerability of Smart Card cryptographic implementations to Differential Fault Analysis (DFA). They showed in their paper ('On the Importance of Checking Calculations') how you could take advantage of induced random hardware faults. In particular they showed how you could theoretically break the Chinese Reminder Theorem by such techniques. Again the idea of inducing faults is not new but what they showed is how vulnerable classical cryptographic algorithms can be to such attacks. In this particular example it is of course the implementation of the algorithm that is vulnerable and which at a high level can be blocked by applying suitable cross checks during the execution of the algorithm.

The main point about all these attacks is that the principles are well known. The difficulty for the designer is to ensure that adequate controls are applied to the particular implementation, to ensure that his system is not vulnerable to a low work function attack. Protection controls by their very nature are an overhead and perfect security can never be achieved. It may be observed here that you cannot prevent an invasive attack on the

functionality of an integrated circuit if you have access to the chip. You can only try to limit the impact. It is in this area that modern day chips are most vulnerable although the architecture of Infineon's SLE 88 is particularly interesting in that it offers real time execution integrity checks by comparing dual processing paths.

Security is a pervasive subject where one is not only concerned about the strengths of the front door but also whether there is an unattended back door. In particular for example has some new tool been invented that can effortlessly bore a hole in the door.

And then we come to 'Introduction to Differential Power Analysis and Related Attacks' by Paul Kocher, Joshua Jaffe and Benjamin Jun from the U.S consultancy company Cryptography Research. This paper describes a class of attacks against Smart Cards and secure cryptographic tokens based on the analysis of the device's power signal. This involves the use of advanced statistical techniques to reconstruct the processor tasks thereby determining the secret information such as cryptographic keys and PINs stored in the card.

As we have already discussed, the concept of information leakage is not new, it is the success that Paul Kocher and his colleagues have demonstrated in applying their new tools to break existing Smart Card implementation that has raised concern.

The monitoring of power consumption to identify cryptographic operation in Smart Cards was first reported by Ernst Bovenlander of TNO at the 1997 Eurocrypt Conference, where he was able to identify the regular structure of the DES cryptographic algorithm. The work of Kocher, Jaffe and Jun takes this much further by being able to determine the actual keys used in the cryptographic algorithms. They show that the operation of the transistors within the Smart Card chip produces observable electronic behavior. Because the operation of the logic is regularly being synchronized to a deterministic clock pattern, it is possible to identify macro characteristics of the microprocessor operation just by simple monitoring of the power consumption.

So just how practical are these attacks? In their paper Kocher et al first define the concept of simple power analysis (SPA – see following briefing by Kocher et al for a more detailed description). Here they discuss the monitoring of the power signal using, say an oscilloscope, where they point out that it may be possible, for instance, to visually observe the difference between the squaring and multiply operations commonly used in the implementation of the RSA (or other public key) algorithm. As they point out it is not particularly difficult to protect against this type of attack.

The thrust of their paper is aimed at Differential Power Analysis (DPA) where they use statistical analysis and error correction techniques to extract information correlated to secret keys. The attack requires two phases, the collection of power signal data followed by the data analysis.

In their paper they give an example of a DPA attack on the DES algorithm. As they point out such techniques require a detailed knowledge of the target algorithm and its likely implementation. In the example quoted 1000 samples of the DES operation are stored for analysis where each sample consists of 100,000 data points. The attacker is also assumed to have the relevant 1000 ciphertexts.

A third analysis tool is described as High-Order Differential Power Analysis (HO-DPA). This is described as an extension of the DPA technique where sample data is collected from multiple cryptographic suboperations. Here it may be data from multiple sources (e.g. different Smart Cards doing the same operation), correlated signals stored using different measurement techniques (e.g. power signal and EMR signal) or signals with different temporal offsets. Clearly such analysis requires an even deeper understanding of the underlying mechanisms. As the authors point out they are not aware of any actual systems that are vulnerable to HO-DPA that are not also vulnerable to DPA.

Cryptography Research has now successfully licensed their technology to three of the major smart card chip manufacturers Infineon, Renesas and NXP. Whilst it is possible to modify the hardware of the processor to help mask these unwanted signals it is clear that the actual implementation of the cryptographic algorithms is fundamental to an adequate protection profile. Cryptography Research should be complimented for the success of their research and for bringing it into the public domain because it helps focus the designers of such systems to ensure that adequate protection mechanisms are employed.

As history shows the battle will continue but there seems every reason to believe that the seesaw is tipped to the advantage of the designer. New attack methods will always appear but good security designs continuously employ change to ensure that the economics of an attack remain with the defenders. Well implemented Smart Card devices present a formidable tamper resistant barrier; with what should we compare them? Is it possible to remove the need for physical barriers, white box cryptography where even visibility of the execution of a cryptographic algorithm is not sufficient to reveal the protected information? Oh… let's leave that one for another day.

An Introduction to Power Analysis – A Extract from "Differential Power Analysis" by Paul Kocher, Joshua Jaffe, and Benjamin Jun - Cryptography Research, Inc."

Most modern cryptographic devices are implemented using semiconductor logic gates, which are constructed out of transistors. Electrons flow across the silicon substrate when charge is applied to (or removed from) a transistor's gate, consuming power and producing electromagnetic radiation.

To measure a circuit's power consumption, a small (e.g., 50 ohm) resistor is inserted in series with the power or ground input. The voltage difference across the resistor divided by the resistance yields the current. Well-equipped electronics labs have equipment that can digitally sample voltage differences at extraordinarily high rates (over 1GHz) with excellent accuracy (less than 1% error). Devices capable of sampling at 20MHz or faster and transferring the data to a PC can be bought for less than $400.

Simple Power Analysis (SPA) is a technique that involves directly interpreting power consumption measurements collected during cryptographic operations. SPA can yield information about a device's operation as well as key material.

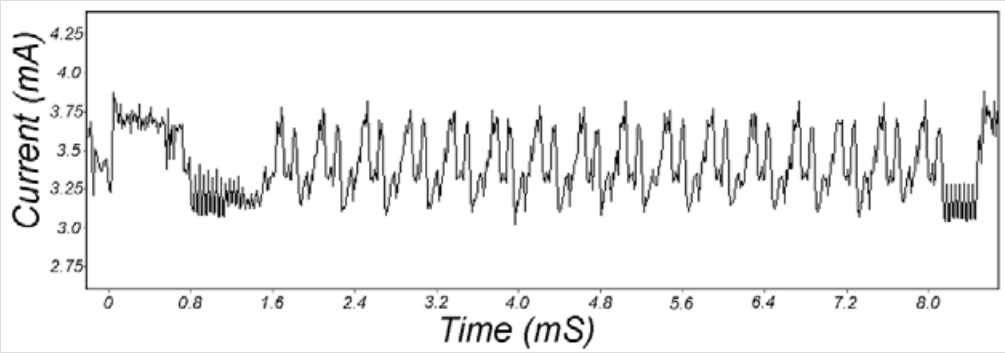


Figure 1: SPA trace showing an entire DES operation.

A trace refers to a set of power consumption measurements taken across a cryptographic operation. For example, a 1 millisecond operation sampled at 5 MHz yields a trace containing 5000 points. Figure 1 shows an SPA trace from a typical smart card as it performs a DES operation. Note that the 16 DES rounds are clearly visible.

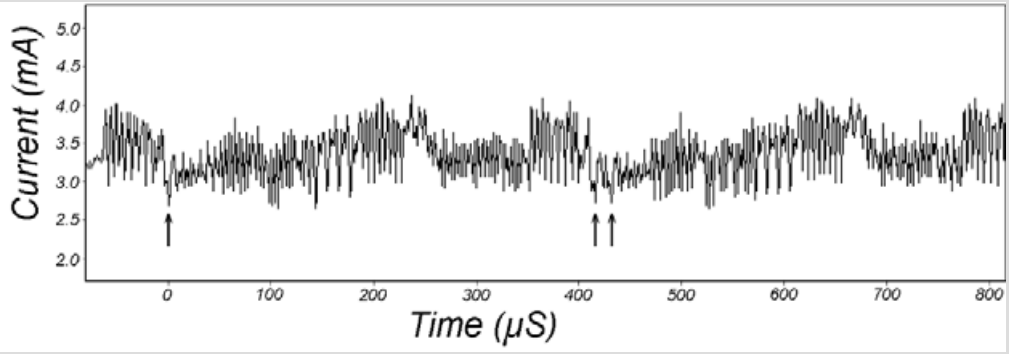


Figure 2: SPA trace showing DES rounds 2 and 3.

Figure 2 is a more detailed view of the same trace showing the second and third rounds of a DES

encryption operation. Many details of the DES operation are now visible. For example, the 28-bit DES key registers C and D are rotated once in round 2 (left arrow) and twice in round 3 (right arrows). In Figure 2, small variations between the rounds just can be perceived. Many of these discernable features are SPA weaknesses caused by conditional jumps based on key bits and computational intermediates.

Figure 3 shows even higher resolution views of the trace showing power consumption through two regions, each of seven clock cycles at 3.5714 MHz. The visible variations between clock cycles result primarily from differences in the power consumption of different microprocessor instructions. The upper trace in Figure 3 shows the execution path through an SPA feature where a jump instruction is performed, and the lower trace shows a case where the jump is not taken. The point of divergence is at clock cycle 6 and is clearly visible.

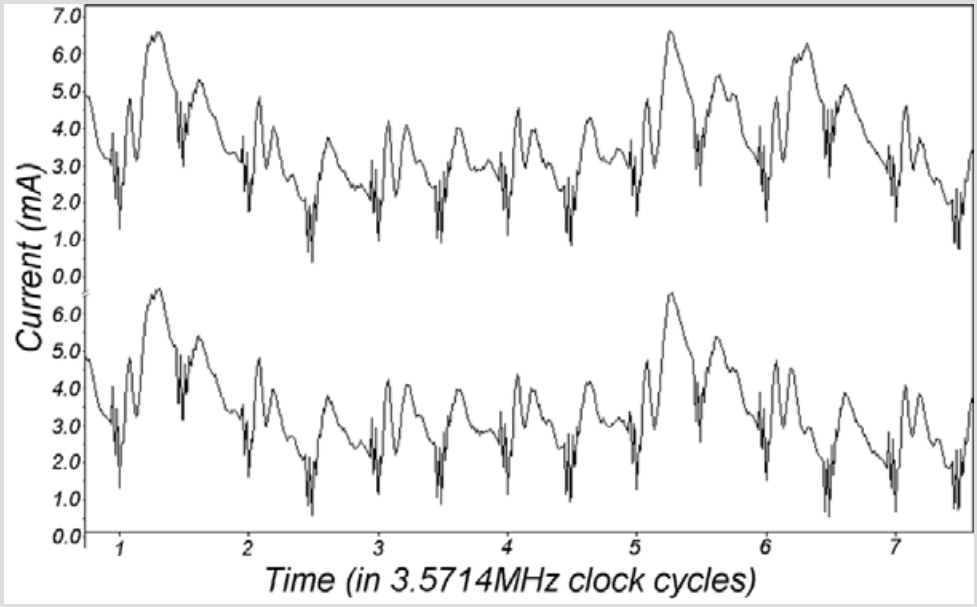


Figure 3: SPA trace showing individual clock cycles.

Because SPA can reveal the sequence of instructions executed, it can be used to break cryptographic implementations in which the execution path depends on the data being processed. For example:

DES key schedule:
The DES key schedule computation involves rotating 28-bit key registers. A conditional branch is commonly used to check the bit shifted off the end so that '1' bits can be wrapped around. The resulting power consumption traces for a '1' bit and a '0' bit will contain different SPA features if the execution paths take different branches for each.

DES permutations:
DES implementations perform a variety of bit permutations.
Conditional branching in software or microcode can cause significant power consumption differences for '0' and '1' bits.

Comparisons:
String or memory comparison operations typically perform a conditional branch when a mismatch is found. This conditional branching causes large SPA (and sometimes timing) characteristics.

Multipliers:
Modular multiplication circuits tend to leak a great deal of information about the data they process. The leakage functions depend on the multiplier design, but are often strongly correlated to operand values and Hamming weights.

Exponentiators:
A simple modular exponentiation function scans across the exponent, performing a squaring operation in every iteration with an additional multiplication operation for each exponent bit that is equal to '1'. The exponent can be compromised if squaring and multiplication operations have different power consumption characteristics, take different amounts of time, or are separated by different code. Modular exponentiation functions that operate on two or more exponent bits at a time may have more complex leakage functions.

EU Issues Smart Chip Privacy Guidelines

By Tom Tainton, Smartcard & Identity News

Tom Tainton

This month the European Commission adopted a set of recommendations to ensure that players in the smartcard industry respects the individual's fundamental right to privacy – an entitlement set out in the European Union charter of fundamental rights. The decision will be welcomed by consumers across Europe who will now be able to have control over their smart chips, a global market set to skyrocket 500% in the next decade. Already there are over 6 billion microelectronic devices that can be integrated into everyday objects such as travel cards, passports and payment cards. The majority of these smart chips use Radio Frequency Identification (RFID) technology, a process which uses a 'reader' to pick up a radio signal and exchange data automatically. The worldwide market value for RFID tags is estimated at around £4 billion, and that figure is predicted to increase to £20 billion by 2018.

The recommendation by the European Commission is by no means a snap decision. As early as 2006, officials launched a public consultation on the development and use of smart chips. Based on these findings the Commission announced that further action was expected by the public in terms of privacy and data protection. The latest announcement on May 12 responded to these expectations. After taking advice from suppliers and users, standardization bodies, consumer organizations and trade unions, the new proposal seeks to create a level-playing field for the European industry while maintaining respect for the individual's right to privacy.

Viviane Reding, EU Commissioner for Information Society and Media was positive about the changes saying, "Europeans must never be taken unawares by the new technology. This is why the Commission issued strong recommendations to the industry today. European consumers must be confident that if and when their personal data is involved, their privacy will be impregnable also in a changing technological environment. The Commission therefore wants RFID technology to empower consumers to control their data security, which is the best way to make sure it is an economic success."

The European industry had better brace itself for some changes. The commission laid out the following principles for protecting privacy and data protection. Retailers should automatically disable tags, free-of-charge, at the point of purchase unless specifically asked otherwise. The same retailers should also promote consumer awareness through a recognizable European sign on products containing a smart chip. Private firms and government departments that employ smart chips, such as the passport and identity agencies, should tell consumers exactly what data they collect, the purpose and how that data will be used. The Commission also advised that card readers be clearly labelled and an information contact point be provided for citizens.

Viviane Reding suggested companies and organizations should "conduct privacy and data protection impact assessments before using smart chips". The assessments, which would be reviewed by national data protection authorities, would make sure personal data was secure. However, some experts are still concerned with the risks of skimming and identity fraud that RFID technology carries but any claims of security flaws were strongly rebuffed by the Smartcard Association. EU member states now have two years to inform the Commission on the steps they intend to take to meet the objectives of the Recommendation. Within three years, the Commission will report on the success of the implementation, including an analysis of its impact on companies, public authorities, and citizens.