

Smart Card & Identity News

Is published monthly by
Smart Card News Ltd

Head Office: Smart Card Group,
Columbia House, Columbia Drive,
Worthing, BN13 3HD, UK.

Telephone: +44 (0) 1903 691779

Fax: +44 (0) 1903 692616

Website: www.smartcard.co.uk

Email: info@smartcard.co.uk

Editorial

Managing Director – Patsy Everett

Technical Advisor – Dr David Everett

Production Team - Lesley Dann, John Owen

Contributors to this Issue – David Everett, Tim Richards, Tom Tainton, Richard Sanders

Printers – Hastings Printing Company Limited, UK

ISSN – 1755-1021

Disclaimer

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

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

© Smart Card News Ltd

Our Comments

Dear Subscribers



Patsy Everett

Well the summer holidays are nearly over and soon the children will be going back to school. No doubt we shall look back on the summer to reflect our holidays and the unbelievable sequence of events that have resulted in lost data usually by a government department or its agency. The latest reported in this month's newsletter being PA the consultancy firm who lost a computer memory stick containing the personal information of all 84,000 prisoners in England and Wales. The information was apparently taken from the Police National Computer and entrusted by the Home Office to PA Consulting. We understand that the person concerned has been suspended.

Now although PA is getting the blame and they certainly have a lot to answer for you can't help but wonder how these secure data bases are organised. How is it possible for a contractor to obtain a copy of the whole criminal data base and pop it onto a memory stick? Imagine working in a bank and asking to take home a bucket load of money for safe keeping, everybody around would tell you no yet personal data is also worth a lot of money. Organised crime is busy selling our details on the internet.

According to reports the data was encrypted at source but then decrypted by PA staff before being put onto a memory stick. Given that PA are security specialists and are in charge of the National ID card project it seems almost inconceivable that such a lax security approach could be taken. I always used to think that the doom makers throwing mud at the government's handling of personal data were clutching at straws but this year the continual episodes of lost data make these soothsayers look positively conservative.

The thing that is really bothering me is that these are the stories being reported how about all the other events that are kept quiet and I suspect there are more losses never reported than the ones we hear about. Just think of some of the people you know, would they report a lost memory stick? I'll bet you come up with quite a few no's. Dr D has always said that if some of the software programmers he knew were working on the fly by wire then he probably wouldn't want to fly the plane they helped build. The trouble is that we are all human and make mistakes so the system has to protect us. In practice most disasters are not due to just one failure, it's usually a set of failures that results in a catastrophe but not seemingly in the way that the government handles our private data.

What all this makes me do is question why people need to move such valuable data around in such primitive ways, why did the contractor need to have the criminal data base on a memory stick, what was he going to do with it? We really only learn by analysing these mistakes and changing the system. Telling people to encrypt the memory stick may have avoided this problem but its not the real answer what is really required is to re-engineer our information systems so that security sensitive data is not just wandering about.





And yes what does all this have to do with smart cards and identity? Quite basic really and that is all sensitive data should be locked away (logical or physical) and the system should require adequate authentication procedures to get at it, like 2-F authentication using smart cards or tokens.

We had the discussion in the office today about users being required to carry around smart cards or dongles, why not do it in the mobile phone? A small survey I know but the dongles won because they are actually less effort to use and if small enough so that they really do fit on your key ring not a problem to carry around.

Cartes 2008 is drawing ever nearer – any news on those annual railway strikes that always seem to be synchronised to the conference?

Patsy.

Contents

Regular Features

Lead Story – Cryptography Research Clinches \$100m Deal	1
Events Diary	3
World News In Brief	5,9,12,17

Industry Articles

The Real Lessons of the Mifare Classic Card Hack	7
Interview with Michael Trader – President of M2SYS Technology	10
Beyond compliance: Dispute management is a cornerstone to Success .	15
Monitoring the Web: What Information is our ISP Logging?	18

Events Diary

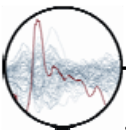
September 2008

- 8 Future of Secure Documents 2008 - Chicago, USA
- 8-10 RFID World - Las Vegas, USA
- 9-12 Cards & Payments 2008 - Paris, France
- 16-19 Smart Event '08. - Sophia-Antipolis, France

October 2008

- 8-9 Printed Electronics Asia - Tokyo, Japan
- 15-16 Storage Expo 2008 - London, UK
- 21-22 Symbian Smart Phone Show - London, UK
- 22-23 Prepaid Cards Summit 2008 - London, UK





.... Continued from page 1

So for the low margin business we might expect over the next 10 years say 1 cent for 500 million chips and for the higher margins perhaps 5 cents for say up to 100 million chips per year which over the 10 year remaining life of the patents would produce up to \$100 million. Pure speculation of course but one suspects it gives a pretty good indication of CRI's aspirations.

But of course apart from Infineon's 30% market share we have,

Samsung	15%
NXP	14%
Atmel	12%
Renesas	12%
ST Microelectronics	7%
Others	10%

So the question is will all the major players sign up? In classic IPR speak are these companies already or likely in the future to infringe a valid patent? Not the right place to have a detailed assessment but what we do know is that all these companies are concerned to get the security of their smart card chips sufficient to achieve the necessary certification processes not only through Common Criteria but also the extra processes applied by both Mastercard and Visa. In all these cases the need to address DPA (Differential Power Analysis), the cornerstone of CRI's work, is well identified. Can you get around it without using the CRI patents? Clearly Infineon think not.

So where does the work of CRI lay in the world of the smart card chip? The silicon manufacturers have always recognised the importance of security to their chips but they have gone through a number of development phases that also involve the software developers, including the chip kernel software.

Phase 1: Basic Application Software Vulnerabilities (- 1990)

In the early 90's and before many software developers made basic mistakes in their core application. This was in two categories, errors that allowed an attacker to break through the application perhaps by leaving undocumented development commands or vulnerabilities to buffer overflows for example. The second category was to leave vulnerabilities in the actual implementation of basic functions that could be exploited by an attacker. One well known example was the software used to check PIN entry. If the software checks the PIN before decrementing the allowed incorrect PIN attempt counter then an attacker may monitor this operation guessing each PIN in turn (often only 4 digits) and if the program doesn't accept the PIN (determined by a number of monitoring techniques based on time (say) then he can turn off the power to prevent the counter from being decremented. Early chips that had an external EEPROM memory high voltage connection were vulnerable to this attack by simply removing this wire on the connector which would stop any write (e.g. the PIN attempt counter) from being implemented. Today this high voltage is generated internally within the chip.

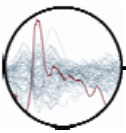
Phase 2: Chip Test Mode (- 1994)

Again in the early 90's chips were often vulnerable to attacks on their test mode. If an attacker could re-invoke the test mode then it would be possible to effectively read any of the chip memories including the mask ROM and the EEPROM memory where the secret cryptographic keys are most likely to be stored. Silicon manufacturers have developed this area of their chips to a level at which this would today be practically impossible to achieve.

Phase 3: Timing Attacks (1996)

Perhaps the first seminal paper by Paul Kocher on the concepts of determining the secret keys of cryptographic algorithms as a function of their (inadequate) implementation. Subsequent to the publication of this paper several researchers have proven the concepts in a real practical environment. Further details can be obtained from his paper.





Paul C. Kocher: Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. CRYPTO 1996: 104–113

Today programmers ensure that all cryptographic functions are either constant or random time regardless of the key or data processed.

Phase 4: Power Analysis Attacks (and Electro-Magnetic Radiation) (1998)

In the smart card world it is this paper that has attracted the most attention over the last 10 years. The reader is referred to the paper for full details but in essence what is shown is the vulnerability of cryptographic algorithms to their implementation in a chip where the CPU operations can be viewed, recorded and analysed by measuring the power consumed by the chip. In a naïve mode (called Simple Power Analysis by the authors) it is possible to actually view for example the execution of an exponentiation function (used by RSA and other asymmetric algorithms) and to visually be able to read the secret cryptographic key.

Paul Kocher, Joshua Jaffe, Benjamin Jun, "Introduction to Differential Power Analysis and Related Attacks (1998)

This is of course the area that is covered by the CRI patents and one of the key concepts is to use blinding techniques so that an attacker cannot correlate the measured power signal data with the secret cryptographic keys.

Because it is a fundamental part of any smart card chip evaluation both the silicon manufacturer and the software programmers are concerned to ensure their implementations are not vulnerable to such attacks. Modern chips produced by Infineon and others may incorporate techniques in the hardware implementation of the chip perhaps by creating random current noise or by balancing the power consumption so that it is not possible to correlate the power signals with the underlying cryptographic processes. It should also be noted that smart card chips are similarly vulnerable to monitoring of their electro-magnetic emissions which needs to be equally addressed.

Phase 5: Induced Fault Analysis (1996)

Although this attack was published before the paper on differential power analysis (originally in 1996) I have classed the vulnerability as Phase 5 because it remains the most difficult weakness in the chip to address. The basic ideas were presented in the paper referenced below,

On the importance of checking cryptographic protocols for faults (1997)
by Dan Boneh, Richard A. Demillo, Richard J. Lipton (Bellcore)

But these concepts have been considerably developed since that time. The only comment I would want to add here is that such attacks require sophisticated resources to implement in a well constructed smart card chip platform in terms of both hardware and software. This is no longer a back bedroom attack.

Dr David Everett

World News In Brief

Smart Cards To Surpass The World's Population

By the end of next year, there will be more smart cards than people occupying this planet. IMS Research's latest report on the smart card market projects that the installed base of smart cards is forecast to surpass the world's population during 2009, meaning that on average each person on the planet will be in possession of more than one smart card.

From relatively humble beginnings in 1983, it has taken 25 years for the smart card installed base to approach the level where, on average, everyone has at least one. By the end of 2009 the installed base is projected to have passed the 7 billion level, a level the global population won't reach until 2011. Furthermore, whereas previously smart card use was concentrated in specific markets and countries, the growing breadth of applications the market now addresses means that the use of smart cards is more widespread geographically than ever before.



So what are we using all these cards for? "By far, for most of us, the most likely reason we own a smart card is for use within our cellular handsets, in the form of a SIM card. Not all handsets require them, but an estimated 2.7 billion did at the end of last year" stated Alex Green, the author of IMS Research's annual Smart Card and Semiconductors in Smart Cards report.

Along with retail loyalty cards, pay TV conditional access, payphone cards, transportation and physical access cards the next big mile stone of 10 billion is in fact less than five years away!

KeyCorp Signs Deal For The Sale Of Its Smartcard Business

Keycorp Limited, a supplier of secure electronic transaction solutions, announced the sale for cash of its Smartcards division to Gemalto. In January this year Keycorp had said that it remained "committed" to the smartcard business.

Gemalto is paying 25.7 million Australian dollars (approximately 15 million Euros, or 22 million US dollars) for Keycorp's smartcard business assets, IP portfolio, trademarks and Multos Ltd.

The assets acquired include Keycorp's implementation of the highly secure MULTOS smart card operating system, the MULTOS brand, the associated patents and the Key Management Authority (KMA) that manages MULTOS card activations worldwide. Approximately 40 MULTOS experts will join Gemalto, mostly based in Australia and UK. The acquisition will contribute over 15 million of annual revenues to the Secure Transactions and Government Programs segments of Gemalto on an annual basis, with over half of the revenues coming from Asia.

Dr Ken Carr, CEO of Keycorp said "This transaction demonstrates the considerable value of the smartcards business in the current market, built upon by the recent acquisitions of StepNexus Limited and MAOSCO Limited, the vehicle for the Multos consortium, based in the United Kingdom. The deal produces significant value for Keycorp, and will enable the company to evaluate other opportunities in the Australian and Asian markets".

Keycorp will consider how best to utilise the net free cash flow in the region of \$16m to further its strategy to focus on greater contract management and deliver sustainable earnings to shareholders.

Cubic To Run The Oyster System Under New Agreement

It has been revealed that early 2007 Transport Trading Limited (TTL) a wholly owned subsidiary of Transport for London expressed its desire to restructure its contract with TranSys to obtain better terms. Negotiations with EDS and Cubic commenced under the TranSys umbrella and continued through February 2008. At the end of February 2008 TTL notified TranSys that while satisfactory progress had been reached with Cubic, negotiations with EDS had failed. TTL terminated negotiations with TranSys but continued separate negotiations with EDS and Cubic outside the TranSys umbrella.

Negotiations with EDS failed again. TTL then negotiated with Cubic to perform the entire project, both maintaining assets and providing operation services. These negotiations were successful and a new contract called the Future Ticketing Agreement (FTA) has been prepared under which Cubic would provide TTL with all services from 2010 to 2013.

It was TTL's intention to sign this contract simultaneously with terminating the existing TranSys contract. EDS has obtained a temporary restraining order (TRO) preventing TTL from doing this. Cubic believes that TTL will have this TRO lifted by the end of this year. When this occurs Cubic and TTL intend to sign the FTA.

Cubic has been providing all services with regard to assets; e.g. design, manufacture, installation and maintenance, of the Oyster Transport system while EDS has been providing information technology operational services.

London's Oyster Cards Come Under Scrutiny By Channel 4 News

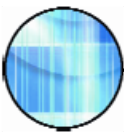
Channel 4 News, televised a news report on the security of the chip used inside Transport for London's Oyster card. The programme discovers new concerns about the security of the chip used inside Transport for London's Oyster card. The Mifare chip, as it is known, has been hacked by researchers in the Netherlands and can be cloned.

A security advisor to Transport for London says the Oyster card needs to be replaced, throwing into question whether cities across Britain will choose this type of technology for their smartcards.

Smart Card New's technical advisor Dr David Everett features within this 12 minute piece.

<http://tinyurl.com/5emsst>





The Real Lessons of the Mifare Classic Card Hack

By Tim Richards, Aconite



Tim Richards,
www.aconite.net

Over 1 billion Mifare cards have been deployed around the world since 1994 in myriad and varied schemes, the chip being one of the most popular smart card types in use in the world today. Yet despite this it took until the end of 2007 for a couple of academics to announce at a hacker's conference that they had demonstrated that the Mifare Classic chip's security was flawed. You could perhaps be forgiven for wondering what the massed legions of security analysts have been doing for the previous thirteen years. At the very least it hardly reflects well on an industry that the world relies on in an age where our very privacy is dependent on the security of the IT systems that surround us: the more so because the attacks on Mifare Classic do not appear to be especially complex.

The truth, of course, is less simple than the headline message and the issue here is not whether the Mifare Classic chip is weak in a cryptographic sense – it probably is, but that's not the main issue – but whether the systems that use the chip are so reliant on it that this attack fundamentally weakens them to the point where they are vulnerable to wider attacks. Good system security design should always take into account the possibility of a major component being compromised or a cryptographic key being exposed and offer ways of dealing with this. Bad system security design simply assumes that the chip is secure and leads to system exposure if the chip security is compromised.

Assuming that a smart card chip is totally secure is just about the most fundamental take that any system security designer could ever make.

The economics of security

Nothing that man can make is totally secure, it's simply a question of how much money it takes to break it. If it takes a million dollars to break a chip so you can take a single trip on the London Underground then no one will really care □ but if it takes a dollar to break a million chips then that's a problem.

However, the problem is more complex than pure economics. A million dollars to break a chip to take a trip to Oxford Circus underground station is stupidity □ or vanity □ but a million dollars to break the same chip to gain entry to the Pentagon or to the backrooms of Heathrow is an entirely different matter. That's why the Dutch government posted armed guards on its buildings when this weakness was uncovered, while transit suppliers have been relatively relaxed.

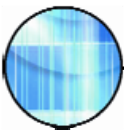
Does this demonstrate that all systems using smart cards are fundamentally flawed? Absolutely not. What it does do is demonstrate that specific systems using smart cards are specifically flawed. Well designed systems should not be reliant on one sort of smart card – it should be possible to swap out one sort of card and replace it with another. Of course there's a cost to this but changing your cards should be the main impact. The trouble is that a lot of systems are built around one specific type of smart card and if you were unlucky enough to choose the Mifare Classic card you may now be looking at a lot of money to upgrade your systems to work with some other type of card. Of course no one would be silly enough to repeat the same mistake again, would they?

Well, don't bet against it.

Uncovering the secrets of the Mifare Classic card

The underlying problem with the Mifare Classic card is that its security appears to rely on obscurity – once you know how the thing works then it's a matter of grunt work to figure out how to break it. It ought to be possible to publish how a well designed smart card security architecture works without exposing the underlying system to any undue threat.





Asymmetric algorithms like RSA or symmetric ones like DES (or Triple DES or AES) don't rely on keeping the algorithms secret, they simply hide away the cryptographic keys in such a way that no human has access to them. These algorithms are the basis for global schemes like EMV Chip & PIN or the ICAO e-Passport standards.

That doesn't mean that the chips involved in these schemes are unbreakable, far from it – put enough money in and you'll get something out. However, the schemes are designed with this in mind, they limit the scope of any attack and the systems – not the chips – are designed to identify and fix any problems. Which doesn't mean that a crack of a credit card or a passport isn't an issue but at least the chip adds to the overall security rather than potentially weakening it.

Nevertheless, if you look at the system security in all of these schemes – transit, government identity, passports, credit cards – and if you dig hard enough at the security you'll find failures to imagine the worst scenarios.

People defend against yesterday's attacks and fail to see what will happen tomorrow – because, by definition, they can't imagine it. To deal with this it's necessary to build systems that don't focus on specific imaginable threats but which can be used to build more general defences. Smart cards actually lend themselves to this approach because many of them can actually be programmed like a computer. The Mifare Classic isn't one of these types of chip: which makes it cheap – which is probably why so many systems have been built using it.

The solution is designing a flexible smart card system ...

The main problem for all issuers sending out smart card chips is that of static thinking: they build systems expecting that nothing will ever change but fail to account for the possibility of the unexpected. Designing properly secure smart card systems is about more than choosing a secure smart card chip, it's about building a security architecture that is resilient in the face of the failure of any individual component (including an individual smart card) and it's about building flexibility into the backend systems so that should the worst occur you can change your chips or the contents of your chip.

All of this is really commonsense but unfortunately commonsense is sometimes hidden under layers of security jargon and, invariably, costs extra money without immediately adding to the bottom line. The problem is, of course, that by not spending a little extra money up front you may find yourself spending a fortune later on.

... and in EMV chip technology

The worst thing about the type of problem that the Mifare Classic attack is causing for some of the systems using it is that for the most part the systems and chips to have prevented it are widely available. For some systems Mifare Classic is fine, whether it's flawed or not, but otherwise using EMV type technology to manage card contents and payment ought to be standard. Using chips that use standard cryptographic algorithms ought to be standard. Where economically possible using programmable chips rather than memory-type chips like Mifare Classic – which at least allows functionality to be adjusted on new cards – ought to be standard. For preference using re-programmable multi-application chips like GlobalPlatform JavaCards or MULTOS ought to be standard.

Above all, designing the systems that use these chips and algorithms to allow them to be modified in the face of Black Swan type unimaginable attacks ought to be standard. The only prediction we can make about the next attack is that we won't foresee it coming – the security industry couldn't foresee what now looks like an obvious and straightforward attack on the Mifare Classic card so expecting it to see anything a bit less obvious is madly optimistic – and we need to prepare by building systems to be flexible, rather than simply fixing the latest problem to emerge.

In conclusion

The Mifare Classic attack should be a wake-up call for the issuers and users of smartcards. The next time a scheme is successfully attacked no executive or security manager should really be allowed to claim that it was a surprise, no matter how unlikely the attack. After all not every scheme can afford to post armed guards on every point of use.



World News In Brief

Mifare's Security Design Should Have Been Open And Public Says Cryptographer Bruce Schneier

"The security of Mifare Classic is terrible. This is not an exaggeration; it's kindergarten cryptography. Anyone with any security experience would be embarrassed to put his name to the design. NXP attempted to deal with this embarrassment by keeping the design secret.

More generally, the notion that secrecy supports security is inherently flawed. Whenever you see an organisation claiming that design secrecy is necessary for security - in ID cards, in voting machines, in airport security - it invariably means that its security is lousy and it has no choice but to hide it. Any competent cryptographer would have designed Mifare's security with an open and public design." Said Bruce Schneier.

He continues "And while these attacks only pertain to the Mifare Classic chip, it makes me suspicious of the entire product line. NXP sells a more secure chip and has another on the way, but given the number of basic cryptography mistakes NXP made with Mifare Classic, one has to wonder whether the "more secure" versions will be sufficiently so."

AuthenTec Ship 7 Million Fingerprint Symbian Phones

AuthenTec has announced that it has surpassed the 7 million-shipment milestone of AuthenTec-enabled Symbian phones and that it has joined the Symbian Partner Network. The two companies have collaborated for more than five years, resulting in the shipment of more than 7 million mobile phones that utilise AuthenTec's fingerprint sensors and Symbian OS.

The market for Symbian phones continues to expand. Eight handset manufacturers launched 13 new Symbian models in Q1 2008, bringing the total number of models in the market to 154 with a total of 235 models shipped since the formation of Symbian. These cover a broad range of market segments and form factors including high-end converged devices, smartphones and mid-range mobile phones. The majority of these new phones are based on Symbian OS v9 including Symbian's latest product offering, Symbian OS v9.3, which is currently shipping in Japan.

website: www.authentec.com

Elderly Peoples Fingers Will Require Exceptional Handling In UK ID Card Scheme

In a Report by the Biometrics Assurance Group, a government advisory body has said that it is "hard to obtain good quality fingerprints from people over the age of 75 due to a lack of definition in the ridges on the pads of their fingers."

The group's report advises the government to use iris scans on those people whose fingerprints are unreadable, but warns such a move will end up costing the taxpayer more money.

A spokesman for the Identity and Passport Service has told The Guardian Newspaper that they disagreed with the group's findings. It is extremely rare with the print quality in the over-75 group to be not usable. He added that if a fingerprint did fall below the required standard, it could be passed onto a fingerprint expert who can carry out the coding manually.

Phil Booth, national coordinator of No2ID, said: "Suggestions manual checks will suffice every time the computer says 'no' begs the question, what is the point of the system in the first place?"

Fingerprints Required For SIM Card Registration

The Nigerian Communications Commission (NCC) has announced that in order to cut down on Identity theft, fingerprints will be required in the SIM card registration process.

Mr. Ernest Ndukwe, Executive Vice-Chairman of NCC said to the press "the commission will be working with the National Identity Management Commission and the Federal Road Safety Commission in the development of a national database that would effectively capture details of Nigerians."

"The registration of SIM cards had become necessary following reports of increasing use of mobile phones for nefarious activities by some individuals noting that the country needed to address the problem."

The commission is working towards ensuring that the anti-mobile phone theft scheme currently being developed is rolled out before the end of 2008 fiscal year.



Interview with Michael Trader – President of M2SYS Technology

By Tom Tainton, Smart Card & Identity News



Tom Tainton

M2SYS is an industry leader in fingerprint identity management technology. Delivering fully functional recognition software, the U.S based company has helped accelerate growth of biometric technology adoption in the global marketplace. I spoke to company president Michael Trader and grilled him on M2SYS and the state of the biometric technology industry.

M2SYS received the Frost and Sullivan Biometrics Technology Award in 2007. What did that mean to your company and in terms of innovation how have M2SYS progressed since?

Receiving the Frost and Sullivan award was a significant event for us. It officially acknowledged the impact that Bio-Plugin has had on the biometrics industry, and reassured us that our business strategy was sound. The market had responded to our technology, and this award helped to solidify our place. Since receiving the award, we have continued to press forward with more innovation initiatives including most recently the release of Bio-AI, a revolutionary biometric technology that significantly reduces false reject rates by using a dynamic profiling technique to ‘learn’ about a person’s fingerprint over time. Once the engine is trained, users can scan partial prints and the system will still identify them. This is an extremely valuable innovation because user operation, for example the consistency with which users properly scan their fingers, cannot be controlled.

How have Biometrics changed since their inception, and how do you predict further developments will alter our lives in the future?

Biometric technology has been in existence since the late 19th century. During the 20th century, the use of biometric technology increased rapidly, particularly in the area of public safety, where fingerprint systems were used to capture and convict criminals. It wasn’t until the 21st century that the use of biometrics in the private sector began to explode in popularity, and a big reason for this was the introduction of our Bio-Plugin technology. While biometrics is still most commonly associated with public safety, we anticipate that biometric technology will continue to gain acceptance in the commercial marketplace. We are already seeing biometrics being used in creative ways, such as the identification of standardized test takers or using voice recognition to access bank information. This trend will continue as people become more aware of the value that biometrics can deliver. As with other areas of science, the continued adoption of biometrics is only limited by our imagination.

How are biometrics currently used in finance and telecommunications? Do you see banking and mobile phone sectors as a potential market for M2SYS?

Banks are using biometrics to identify employees that are accessing sensitive information, performing high dollar transactions, identifying customers to prevent fraud, and more. M2SYS works closely with Fortune 500 financial institutions that use it in their loan origination software to identify loan officers that are authorizing loans. In telecom, voice recognition systems are being used to access account information or perform transactions. We think that banking has an enormous amount of potential for M2SYS and our solutions because of the increased emphasis of industry regulations that protect identity fraud and the sensitive nature of financial information. As the use of mobile phones becomes more popular to access information and perform critical transactions, the market potential for biometrics will grow exponentially. M2SYS plans to capitalize on these industries by continuing to enhance products such as Bio-Plugin Web server and by unveiling software for mobile devices.





Some police departments now carry portable fingerprint readers. Do you feel biometric technology is preferable to smart card authentication?

We think that the combination of biometrics with smart cards provides a very reliable method of identity verification. Two-factor authentication that requires a person to provide something they have, like a smart card, with something they are, biometrics, is always more secure than one or the other. The widespread use of biometric data stored on a smart card will require interoperability between systems and increased focus on fool proofing the technology.

What challenges do you face in the industry, particularly in the healthcare and public safety markets?

In the healthcare industry, biometrics is being used to identify health care professionals, and identify patients. Some challenges that must be overcome include barriers to capturing a clean fingerprint image for healthcare employees that wear medical gloves, for example. When identifying patients, there are operational challenges with training people how to properly scan their finger to produce a consistent image. With public safety, it can be challenging maintaining system performance as the size of the fingerprint database increases. We have developed a product called Parallel Server to meet this challenge, which enables the fingerprint system to easily scale as the fingerprint database increases over time.

Your flagship product, Bio-plugin can be integrated into systems across many industries with minimal hassle. How unique is this, and is it the company's key business differentiator?

In the biometrics industry, Bio-Plugin provides software developers with the most rapid path to adding fingerprint authentication. In a matter of hours, as opposed to weeks or months, developers can integrate Bio-Plugin with their application, instantly providing a fingerprint module that can be sold to their customers. In addition, as opposed to alternatives such as a low level fingerprint SDK; Bio-Plugin resides outside of the host application run-time, so developers never have to compile their software with ours. This significantly reduces the cost and headaches involved with ongoing support and maintenance. This is a unique selling proposition in the marketplace and unmatched by any other company across the competitive landscape.

What advantages does Bio-plugin have over a common fingerprint SDK?

A traditional, low-level fingerprint SDK is just a library containing the components that are needed to develop a fingerprint matching system. The burden of taking these components and building, integrating, and supporting a fingerprint recognition system is placed squarely on the shoulders of the developer. Also, with any SDK, these components must be loaded into the host application at runtime, so you must compile your software with the fingerprint library whenever a modification is made to either the host application or to the fingerprint system. Depending on the scope of the project, it can often take 8-12 months of development before the fingerprint system is ready for production deployment using a traditional SDK. In comparison, Bio-Plugin is delivered as a pre-developed fingerprint software system. The time, headache, and resources that are required to develop and integrate the fingerprint system are completely eliminated with Bio-Plugin. The integration process takes only a few hours. We've had customers integrate and release the fingerprint module for production rollout in just a few days. In addition, as opposed to low-level fingerprint SDKs, Bio-Plugin resides outside of the host application runtime, so the host software never has to be compiled with the fingerprint software. This greatly simplifies the extraordinary burden of ongoing maintenance and support.

M2SYS announced a fingerprint product that aims to limit the possibility of a false reject. How do false rejects negatively impact biometric companies?

Bio-AI is a Bio-Plugin product enhancement that was built to address the issue of false rejects with the fingerprint system. A false reject occurs when the system fails to identify an enrolled user. In environments where speed is important, this can cause significant frustration with the fingerprint system. Bio-AI uses a dynamic profiling technique to "learn" a little more about a user's fingerprint during every scan. After activating the Bio-AI enhancement, user's will begin to experience a reduction in the false reject rate over a short period of time.





What are some of the key changes in the industry that M2SYS has witnessed over the past year?

As I mentioned earlier, biometric technology initially got its start in the government sector. What we have witnessed in the past few years is a dramatic shift of biometrics adoption from the government sector to the private sector. This has created a tremendous opportunity for M2SYS and other biometric technology providers.

An increased and growing emphasis on security has also helped to fuel the recent growth predictions for biometric technology. More countries are looking to biometrics to secure their borders, eliminate voter identity fraud, and to safeguard citizen welfare. The growing presence and use of wireless technology has also driven biometric technology providers to develop solutions that are compatible with mobile devices.

What type of security features do you employ to ensure privacy and protection of the information collected?

During the enrolment process, Bio-Plugin uses a one-way algorithm to convert the captured fingerprint image into a unique 'binary template' once the fingerprint has been captured. At this point in the process, the image of the fingerprint is destroyed. What remains is a data file that cannot be reverse-engineered to reproduce the fingerprint image. This data file is proprietary to the software application and would be virtually meaningless to anyone that hacks into the system. In addition, all data is stored using the AES 128 bit encryption algorithm.

In the future, where do you see potential growth and new revenue streams for your company?

M2SYS is poised to benefit from the significant growth potential in the biometrics industry during the next 4-5 years. In particular, fingerprint biometrics is forecasted to reach \$2.7 billion by 2012 making it the largest growth sector of the biometrics industry. We do, however, expect certain vertical markets to outperform others. For example, companies that are interested in using biometrics to manage time and attendance functions are adopting fingerprint technology rapidly. We also anticipate significant growth in the healthcare industry, given the demands that HIPAA compliance is putting on both for-profit and non-profit healthcare institutions.

World News In Brief

Hundreds Of Fake Cards & PIN Pads Seized From UK Card Factory

The Dedicated Cheque and Plastic Crime Unit (DCPCU) - the special police unit that tackles cheque and card fraud crime in the UK - has raided a sophisticated counterfeit card factory in Birmingham. Two people have been arrested in connection with this raid and were charged on 12th August with conspiracy to defraud.

Detective Chief Inspector John Folan, who heads up the Unit, said: "These arrests are a significant development in our fight against the organised criminal gangs responsible for this type of fraud. To date, compromised chip and PIN terminals have been found in less than 30 retail outlets throughout the UK. Together with the banking and retail industries we are working to ensure this figure is minimised. We are sending a very clear warning to fraudsters these crimes will not be tolerated, and that we will continue to target them and disrupt their fraudulent activity."

Equipment needed to steal card details and make counterfeit cards on a massive scale - including stolen chip and PIN terminals, card account numbers, a card reader/writer, computer software and fake magnetic stripe cards - were found in the premises. Early indications are that these criminals have been tampering with retailers' chip and PIN terminals in order to steal card transaction data and PINs from these machines.

With these details, criminals are able to create fake magnetic stripe cards that can be used fraudulently in countries that have yet to roll out chip and PIN. This type of fraud - fraud abroad - increased 77% last year, totalling £207.6 million.

The DCPCU is fully sponsored by the banking industry through APACS - the UK payments association, and has an ongoing brief to help stamp out organised card and cheque fraud across the UK. It is a unique body that comprises of officers from the Metropolitan and City of London police forces who work alongside banking industry fraud investigators.





HBOS Chief Executive Has Bank Accounts Raided By Identity Thief

It was revealed this month that HBOS chief executive Andy Hornby has had his Identity Stolen from an African fraudster.

The fraudster managed to obtain at least £7,000 in one day but was later caught on CCTV making withdrawals from a HBOS branch.

"They think the thief is from an African background. He certainly looks nothing like Andy. It appears he used one of Andy's statements as proof of name and address in a branch." said a commenter.

"Bank staff had to call Andy on holiday to say they were freezing his accounts. If it can happen to him, it can happen to anyone."

Mr Hornby left Asda to become chief executive at the Halifax in 1999. Mr Hornby became chief executive of HBOS in 2006 and earns £1 million a year.

Best Western Hotels Suffer Massive Data Theft

This month revealed that an Indian hacker had successfully breached the Best Western Hotel's online booking system and has sold the details of how to access it through an underground network operated by the Russian mafia.

The personal details of about 8 million customers that booked into the Best Western's 1312 continental hotels since 2007, is thought to have been scooped up in the attack.

Although it is difficult to track, it is thought that the hacker succeeded in bypassing the system's security software and placed a Trojan virus on one of the machines used for reservations, so the next time a member of staff logged in, their username and password were collected and stored.

The stolen login details were then put up for sale and shared on an underground website operated by a notorious branch of the Russian mafia

ISNR (International Security & National Resilience) Event

ISNR will bring together government, public sector, police and emergency response, transport and critical national infrastructure stakeholders with

commercial and private security organisations. This focused event is an opportunity to learn from a comprehensive seminar program and high-level, industry leading conference and showcases the complete range of real-world, workable security solutions.

ISNR takes place on the 2nd & 3rd December 2008 National Hall, Olympia. London. To register for free now please visit www.isnrlondon.com/smart

Ebay Laptop Contains Million Bank Customers Details

A computer containing a million bank customers' personal data has been sold on an internet auction site Ebay. An ex worker from archiving firm 'Graphic Data' sold the laptop for £35 on eBay without removing sensitive information from the hard drive.

The Royal Bank of Scotland and its subsidiary, Natwest, have confirmed their customers' details, including account details, signatures, mobile numbers and mothers' maiden names, were involved.

This massive data loss, one of the worst ever in Britain, is a clear breach of the banks' obligation under the Data Protection Act to keep all personal information secure.

UK Government To Invest £5.5m In Data Privacy Projects

The Government is to invest over £5.5m in three new research projects that will help to develop the next generation of secure identity management systems.

The Technology Strategy Board, Engineering and Physical Sciences Research Council (EPSRC) and Economic and Social Research Council (ESRC) have joined forces to back the three projects with an investment of over £5.5 million.

The three projects are:

EnCoRe, which will focus on the issue of providing more rigorous means for individuals to grant and revoke their consent for the use, storage and sharing of personal data, bringing together technological, procedural and regulatory developments. (<http://www.encore-project.info>)

VOME, a research project that will reveal and utilise end users' ideas and concepts regarding privacy and





consent, facilitating a clearer requirement of the hardware and software required to meet end users' expectations. (lizzie.coles-kemp@rhul.ac.uk)

Privacy Value Networks (pvnets), will generate a detailed understanding of individuals' and organisations' conceptions of privacy and identity across a range of contexts and timeframes - using a range of techniques including in-depth privacy value and devalue chains analysis to model the impact of the personal information. (ian.brown@oii.ox.ac.uk)

Explaining the background to the decision to invest in the three projects, the Technology Strategy Board's Chief executive, Iain Gray, said: "The next few years will see governments and businesses around the world making substantial investments in identity management infrastructures. In order to prepare UK businesses for competition in this global market, practical and cost effective solutions need to be developed which inspire public confidence by improving privacy and enabling consent as an integral part of future procurements."

Wood Key Cards at Democratic National Convention

CPI Card Group, working with Sustainable Cards LLC, provided the environmentally sensitive electronic key cards for the 2008 Democratic National Convention in Denver, Colorado. As part of the host committee's commitment to organising the greenest political convention in history, they have selected sustainably harvested wooden key cards for the approximately 70,000 hotel key cards that will be produced for convention visitors.

Just being introduced to the U.S. now, the wooden key and gift cards have been used successfully in Europe for nearly 10 years.

NXP Acquires Conexant's Set-top Box Operations

NXP Semiconductors, a semiconductor company founded by Philips, confirmed the completion of the acquisition of the Broadband Media Processing (BMP) business of Conexant Systems, Inc.,

With this transaction, the first for its Home Business Unit, NXP's existing set-top box and digital TV operations will be combined with Conexant's BMP business. NXP will become top three-technology player in the Digital Video Systems market.

Under the terms of the deal, NXP will pay Conexant US\$110 million in cash up front, and additional consideration of up to US\$35 million based on

achievement of certain revenue milestones.

London's NFC O2 Wallet Trial Results Released

According to the results of Europe's first large scale NFC (Near Field Communications) mobile phone pilot, almost 80 per cent of trialists who sampled the O2 Wallet agreed that the Visa payWave functionality is a service they would like from an NFC phone. One in five trialists stated that their decision to purchase a mobile phone in the future would be positively influenced by the addition of a payments feature.

Visa launched Visa payWave contactless payment technology in London last year and is one of a number of industry partners who worked with O2 to run the O2 Wallet trial from November 2007 to May 2008. The trial was designed to establish what services and functionality consumers would like from an NFC phone in advance of entering full commercial production. Barclaycard was the Visa Issuer involved in the trial.

Almost half (41%) of trialists said that they felt this payment application offered an easier and faster way to pay for smaller items than using cash. Trial findings also indicate that as an added security measure there would be benefits in asking consumers to enter a PIN from time to time when making a purchase, similar to the contactless card experience today. Trialists also requested wider Visa payWave acceptance in retail outlets to make the payment facility more appealing.

Identity Cards For Foreign Nationals Roll-Out Date Announced

The UK Border Agency from the 25th November 2008, will start to issue identity cards to foreign nationals. The identity card for foreign nationals is the first part of the National Identity scheme and will be rolled out on an incremental basis over the next three years to all foreign nationals.

The UK Border Agency will first start issuing compulsory identity cards to foreign nationals who apply for further leave to remain in the United Kingdom within certain categories (student and marriages or civil partnerships). Following the issuing of identity cards to foreign nationals, the national identity scheme roll-out will continue with identity cards for workers in sensitive roles and locations like airports next year. In 2010 voluntary identity cards will be offered to young people and in 2011-12, voluntary identity cards will be offered to large numbers of the British public.





Beyond compliance: Dispute management is a cornerstone to success

By Richard Sanders, Business Consultant, ACI Worldwide



Richard Sanders

According to a report from PSE Consulting in July, the cost of complying with the EU Payments Services Directive (PSD) could amount to €6 billion over the next 18 months for 30 of the biggest international banks in Europe. This is the potential reality facing banks as they work to comply with the mandatory EU regulation by November 2009. In the current financial market turmoil, many banks are understandably considering solutions which merely tick the correct boxes. However, not all banks can be accused of taking this somewhat reticent approach. Seeing the opportunity to implement new IT strategies that benefit the bank and its customers in the long term, some financial institutions are taking a strategic approach to the necessary PSD investment to improve longstanding processes for the better.

One such area that is benefiting from this approach is dispute management. As part of the long-neglected area of card payment processing, many banks and third party processors still rely on legacy systems coupled with highly manual processes to resolve customer queries. However, there is at present a 'perfect storm' of developments within the financial services industry, including the imminent PSD, which is making largely manual chargeback systems untenable.

Under pressure

Across the board, banks are increasingly looking to implement more innovative solutions that are cost-effective, co-ordinated with their risk strategies and encourage customer retention. In the past, investing in dispute management hasn't been viewed as being able to yield strong returns in any of these areas. However, it is becoming increasingly clear that this is no longer the case.

Over and above the effect of the PSD on banks' dispute management strategies, there are several industry trends that are shaping their renewed focus on improving dispute management systems. It is crucial that the emergence of new regulations, as well as new payment channels and, indeed, new customer spending habits are all taken into account in the development of dispute management systems. The handling of disputed transactions is an integral part of card management and an important point of customer interaction for banks battling to retain market share.

As pressure mounts on the need for customer transparency combined with a drive for greater cost efficiencies in the front and back office, and the requirement to continue to deliver strong financial results, dispute management is seen as an increasingly attractive area for improvement.

Drivers for change – the evolving landscape of dispute management

The Payment Services Directive is widely regarded as the most significant retail banking legislation in recent years and there are numerous considerations across multiple banking channels. The need to become legally compliant with the PSD, which is due to come into force in November 2009, is a strong motivation for change.

With the introduction of the PSD, banks will face a more stringent approach to managing disputed transactions as the onus of proof is clearly put on the bank. As such, the old method of dispute resolution is no longer satisfactory and instead of relying on an archaic form of manual data recoding which requires manual checking to prove what actually occurred during the transaction, banks must ensure that they implement electronic journaling as an irrefutable audit trail. This will eliminate the costly and lengthy process of traditional checks and provide financial institutions with the capability to query and retrieve accurate data relating to the transaction in question. Migrating to an automated dispute management system and keeping an electronic record of all transactions will also support financial institutions in meeting the requirement of the PSD to maintain records for a minimum of five years.





Beyond regulations

On top of the challenge presented by the PSD specifically, which has provided the final catalyst needed for investment in dispute management, there are a number of other factors contributing to the growth in the volume and complexity of disputes that payment card providers currently have to handle. Combined, these present an obvious business case for banks to ensure the necessary procedures are in place to manage customer disputes.

The introduction of EMV cards aimed to increase security and reduce the amount and cost of chargebacks. However, the liability shift to the non-EMV party in the transaction has meant that fraud has migrated to the card-not-present (CNP) environment which is unprotected by EMV. As a result, the potential number of disputes raised is actually greater. With criminal behaviour and techniques evolving at an alarming rate, fraud-prevention technology must follow suit. Banks require automated systems that can alert banks to suspicious activity which can range from repeated queries on transactions by customers playing the system to organised criminal activity which targets specific bank accounts.

In addition to regulatory changes, card systems are also being modified on a continual basis to keep up with consumer demands and market trends. Banks must regularly review and update their dispute management procedures to meet the changing nature of the cards landscape and new products. One example is that of contactless transactions. Currently, most banks have a minimum chargeback threshold of around £25 for all payments, below which pursuing a chargeback is uneconomic because of the associated Payment Scheme fees and processing costs. However, contactless card transactions will all be capped at £10, at least initially. Under the current procedures, therefore, all disputed contactless transactions would be written off without investigation which offers an opportunity to organised crime as well as to the less than honest cardholder. Furthermore, banks also want to aggregate contactless transactions on statements to reduce costs, which may further complicate the situation.

Due to the growing popularity of this emerging payment channel, banks must develop a new strategy for handling disputed transactions from contactless cards. They need improved and more appropriate chargeback procedures that reflect the change in the volume and variety of card transactions. Given that all contactless transactions in the UK will initially have a limit of £10, the sheer volume of expected activity means banks cannot afford to write off all disputed contactless transactions. As receipts are optional under payment scheme rules, the pressure on current chargeback systems will grow.

Over and above the number of external and internal pressures banks are facing, the various participants involved in payments processing such as merchants and third party processors all have different requirements when it comes to dispute management. This further increases the need for automated and flexible dispute management systems to handle the different requirements for chargeback processing and support the growth of revenues and profits.

Customers come first

As the number of payment types are increasing, so are the variety of customer communication channels. Banks must be able to accept notifications of disputes through a number of different outlets and they need a comprehensive understanding of customer problems to provide speedy resolution. Increased regulatory intervention, such as the Treating Customers Fairly (TCF) Directive, which aims to ensure an efficient and effective market and thereby help consumers achieve a fair deal, has meant banks must be more transparent in the processing of claims and offer accurate explanations of any issues or resolutions.

Customer retention and satisfaction should be a major driver towards the adoption of an automated dispute management system, particularly as the cost of customer acquisition rises as more players enter the payment card business. In the UK market, for example, the cost to recruit a new credit card customer is estimated to be £120.

Benefits for banks

Due to the liability shift that is mandated by the PSD, banks are being somewhat forced to ensure their dispute management systems are robust enough to compete in the emerging European landscape. With PSD compliance a fundamental driver towards upgrading dispute management procedures, the opportunity for banks to ensure the system doesn't simply just tick a box and instead benefits the entire business is strong.





There are several factors beyond legal necessity which make dispute management an attractive area for development.

Automating the chargeback function has some clear, measurable benefits and given the changing landscape of dispute management, regulatory requirements and the competitive customer service space, now is the right time for banks to implement innovative and flexible solutions.

Aside from the external benefit presented to customers, an automated dispute management system can help to make efficiencies in staff levels. The chargeback area can be staffed by a smaller, better informed and more engaged team. This also allows the bank to provide enhanced customer service, in some cases facilitating an increase of up to 70 per cent in the number of chargeback cases it can handle which leads to a reduction in net write-offs. Through an automated system, chargeback cases created per employee can be increased by 40 per cent and calls answered at the call centre increased by 30 per cent.

A reduced number of personnel working on individual cases significantly lowers costs, and error rates become almost non-existent at just 0.02 per cent. This compares to reported rates even as high as 10 per cent on some manual systems.

Regulation is a major factor in banks upgrading from manual to automated systems. New reason codes and validation rules mandates of the payment schemes need to be automatically updated every six months, ensuring the chargeback process is fully compliant. Scheme waivers are increasingly rare.

Embracing change

With the main strategic objectives for banks this year according to Gartner being cost reduction, revenue growth and improved risk management, many existing legacy dispute systems cannot be enhanced to meet these goals or adapt to changing market requirements, rising levels of fraud and competitive levels of customer service.

Ignoring the current flux in the payment processing industry, from regulation to pressure on enhanced customer service and new products, means that banks will risk a rise in costs through manual and inefficient processes. This will prevent revenue growth due to the inevitable loss in customers that were expensive to recruit in the first place.

Dispute management has not been a major point of focus for the card payment processing industry to date. However, it should be considered a valuable tool to help banks meet all their strategic objectives, especially in the current market environment.

World News In Brief

\$1M For Breaking AES Cryptography

Permanent Privacy has offered a \$1M for breaking its encryption mechanism. Their scheme is based on AES encryption but has an extra layer of security to pre-process the plaintext which the developers claim makes it impregnable. It explained that the idea came from encrypting a piece of plain text that was unintelligible gibberish. It believes that it is so hard to crack that it is offering \$1 million to anyone who is able to break into the system.

The company explained that doing a key exhaustion would be to no avail because the plain text is gibberish and you wouldn't know when you have selected the right key. Peter White, managing director of Permanent Privacy, said: "The world of cryptography shuns and disparages outsiders, but Permanent Privacy is the real thing. You can now send emails and store data with 100 per cent

security. Even the Pentagon cannot read your secrets if they do not have the keys."

Now perhaps I am missing something but first of all they seem to assume that you can do a key exhaustion attack on AES (256 bits?), I'll bet there's a lot of people who would pay more than a \$1M if you can find a way of doing that and then this extra layer of security, is it going to be proprietary I wonder? Hopefully not if they have been reading about Mifare and if it's a public pre-processing algorithm then you are dependent on the effective work function including time memory trade offs for that mechanism. Perhaps you could use AES for the pre-processing algorithm?

I'm not sure that the world of cryptography shuns and disparages outsiders but they might just ignore the obvious particularly when it doesn't live up to the claims.





Monitoring the Web: What Information is our ISP logging?

By Tom Tainton, Smart Card & Identity News



Tom Tainton

For years web companies have been trying to gather information about their users with the intention to deliver adverts tailored to the individual's viewing habits. Recently, these schemes have accelerated with major providers such as AOL and Microsoft trying to combine information gathered on their own sites with that obtained from consumers on other networks. There is clearly a strong financial incentive for Internet providers to gather data about what users read and what they search for and sell on this information for a hefty sum. If a service provider can track every click of the mouse they will be capable of finding adverts that indulge every user's weakness.

Naturally, many of us who regularly use the Internet are under the impression that we are doing so in private. We believe e-mails are only being read by the intended recipient and no one is tracking our online purchasing habits. This is often not the case. Proponents of ISP monitoring systems argue that the worst-case scenario is people see advertising related to their interests, hardly a big deal. Unfortunately, the reality is far more complex than that. There is always a risk of leaked personal data, just like bank details being accidentally revealed by online stores.

Law enforcement authorities argue it is important to work with ISP's to gather information about individuals suspected of being involved in criminal activities or terrorism. The U.S justice department recently passed a bill requiring all Internet service providers to track their customer's online activities to aid police in future investigations. Employees of a provider who failed to store the information could face a prison sentence and a fine.

And it's not just user privacy either. ISP monitoring could spark conflicts in the marketplace. For example, if Yahoo! can tell you that you searched for car insurance while on AOL, there is less reason to pay for a targeted advert while on AOL's network. It can only be a matter of time before the mobile phone and telecommunication networks find themselves in a similar position.

Mike Barwise, from Infosecurity Adviser, suggested that two-dimensional databases such as the planned government telecommunication database breed a host of privacy issues. According to Barwise, when the time and location-based data is obtained from the cellular carriers, then a three-dimensional view of the person is created. Not only would the companies have access to the numbers called and the locations called from, the information would also disclose business and social contacts, as well as web browsing habits. Mobiles containing GPS devices will be able to track what stores we visit and where we choose to eat. How much would McDonald's pay to send adverts to a person who regularly visits Pizza Hut?

One Ex-ad ware company, Phorm has already spawned a chorus of outrage at its plans to access the surfing habits of 70% of British households with broadband. The company is working with major British ISPs including British Telecom and Virgin Media to monitor browsing habits and serve relevant advertisements to the user. It works by sifting out keywords from requests, categorising user interests and then matching them with advertisers who wish to target that particular audience.

Trials are very much underway, even if they are kept behind closed doors. British Telecom reportedly ran a secret trial in 2006, intercepting and profiling the habits of 18,000 of its broadband customers. Again, in 2007 BT tracked the web browsing of tens of thousands of users. Despite denying testing the Phorm service BT eventually admitted to doing so when confronted with technical evidence of a link between the two companies. BT made the paltry excuse that customers who participated in the tests were not made aware of the trial, as one of the aims of the validation was not to affect their experience. The message is pretty clear: If you care about your privacy, don't use BT as your Internet provider.

Concerns over the proposed service have been highlighted amid fears of breached confidentiality and data property rights. The Foundation of Information Policy Research published a letter to the British Information Commissioner claiming that Phorm violates privacy law. Sir Tim Berners-Lee, the developer of the Internet





said he would rather switch providers than have his browsing monitored. In an interview with the BBC he said, "I want to know if I look up a whole lot of books about some form of cancer that the information isn't going to reach my insurance company and my premiums rise because they've figured I'm looking at these books for a reason." A Phorm spokesman defended the technology in the face of what he called "misinformation from bloggers claiming a threat to privacy. The system is legal and respectful of the individual because it doesn't store any personally identifiable information. Users can opt out of the system entirely if they wish too."

The 'opt-out' default of Phorm means that information will be taken and used commercially until told otherwise. However, the contents of the websites visited will still be mirrored to its system. All computers and applications would need to be configured to successfully opt out. Thus, it has since been declared by the information commissioner that Phorm would only be legal under UK law if it were an opt-in service.

Although Phorm is not readily identifying an individual, users who are targeted may still feel that they are vulnerable to having their personal details revealed. AOL discovered the same thing last year when it released a number of anonymised search requests with the personal IDs replaced by random numbers. The list had to be withdrawn in haste when it became obvious that users could be identified from that information alone.

There are effective ways for users to maintain privacy. Devices such as (NIDS) Network Intrusion Detection System can monitor and restrict sensitive documents being released. The Micro expert Network Auditor is an appliance that monitors all network traffic looking for suspicious behaviour. This falls into two types, external and internal attack. External attacks are generally from the Internet whereas internal attacks are errors such as confidential data being accidentally leaked, perhaps via email. In both cases the box keeps an audit trail of pre-set events and can also be made to prevent some action happening, for instance an email that could be dropped.

Phorm claims it is not endangering the users. They point out that because their equipment is installed entirely within the ISP's infrastructure then they are not doing anything illegal, as a service provider can be expected to know at least some information about the user. The company also maintains that they protect against online fraud and phishing. If users try to access a phishing site that is listed on a database available to Phorm, a warning will appear on the browser. Ironically, some security experts such as Kaspersky Lab have suggested Phorm's targeting cookies would be detected as the online virus ad-ware.

The criticism has certainly had an impact on stock price, with shares plummeting nearly 30% in May indicating that Shareholders might share public concerns. Phorm also seems to have some technical problems to contend with. Microsoft Office products employ the same 'user agent' identifier as Internet Explorer. Therefore, Phorm cannot distinguish between the service provider and other software such as Microsoft Word. Phorm could then monitor emails sent and received, and which Word documents you had opened, effectively shattering user copyright protection and potentially landing Phorm in very hot water indeed.

Even Internet giant Google finds itself in a legal wrangle with Viacom over allegations of copyright infringement. Viacom claimed to have identified around 160,000 unauthorised clips of its programmes on YouTube, which had been viewed more than 1.5 billion times. Much to the detriment of user privacy, The US court has ordered Google to hand over the logging database which is updated each time a video is watched on the site. The database contains unique login ID, IP addresses and the locations of the computer affecting millions of viewers.

Primarily, ISPs must outline rights in their privacy agreements. So, if an ISP agrees to protect the users privacy and then fails to do so, the ISP is violating FTC (Federal Trade Commission) fair trade practices. In one instance in 1998, action was taken against a company for violating its own privacy policy. In this case, GeoCities collected information about users who used its service. Its privacy policy explicitly stated the information would not be released to third parties without permission. The FTC accused GeoCities of selling this information in spite of its policy and later ordered the company to prominently display its privacy policy on its home page and wherever it collected information.

Fortunately, however dwindling our rights to privacy may be, they do remain intact. The highest appeal court in Germany decided that T-Online, one of the largest German ISPs has to delete all IP logs to guarantee the privacy of their customers. This ruling makes it impossible for organizations to trace an IP-address back to a customer of T-Online, once their dynamic IP address has changed.

