

War rages on internet battlefield

Though the internet provides vast opportunities to advance the use of electronic payments, it has also become the hunting ground of cyber-criminals on an increasing scale. The payments industry is fighting back in what has become a war between technology experts on opposing sides

In November 2007 the Science and Technology Committee of the UK's House of Lords pronounced the internet to be "the playground for criminals". The committee went on to slam all involved in internet security for taking a "laissez-faire attitude".

"The committee has a point, but it is just one point of view – it reflects that of the general public," David Dix, an electronic payments expert at UK security solutions specialist Cryptomathic, told *EPI*.

However, he stressed: "Many things are being done by banks and others in the payments market to enhance security."

UK public opinion, said Dix, is in large measure being influenced by data regularly released by payments industry body APACS revealing startling and sharply-rising online fraud losses. In 2007, according to APACS, card-not-present (CNP) fraud in the UK totalled £290.5 million (\$500 million), up 37 percent compared with 2006. Of the total, online fraud accounted for £223.8 million (77 percent), an increase of 44.9 percent. The balance of CNP losses was accounted for by telephone and mail-order fraud.

UK not alone

The UK is far from alone. Indicative of a similar problem in the US, for instance, research undertaken by the Center for American Progress and the Center for Democracy and Technology estimated that internet fraud resulted in total losses of \$7.1 billion in 2007, up 39 percent compared with 2006.

In the UK the rising trend continued into the first half of 2008 with APACS reporting CNP fraud losses of £161.9 million, up 18 percent compared with the first half of 2007. And it is a rising trend Dix believes is set to continue.

"In many respects it is a customer-driven problem," said Dix. "They want to access their money from anywhere and a lot of those channels are via the internet."

However, he added rising fraud must be seen in context of the rise in online shopping.

"You have to look at online fraud figures in terms of online retail spending," he stressed. "Retail spending is rising at a faster pace than fraud losses – it indicates that fraud prevention steps are having a positive effect."

This is confirmed by data from APACS. Between 2000 and 2007, for example, online shopping payment card transactions increased from £3.5 billion to £34 billion, a CAGR of 38.4 percent. This compared with a CAGR of 21.8 percent for total CNP fraud losses over the period. APACS's estimate of online shopping in the UK could be conservative. Notably, an estimate made by global electronic retail industry body the Interactive Media in Retail Group (IMRG) put total online spending in the UK in 2007 at £46.6 billion.

This year, despite a sharp fall in overall retail spending, UK shoppers have continued to flock to online retailers' websites. According to IMRG online sales in the UK in the first half of 2008 increased by 38 percent compared with the first half of 2007 to £26.5 billion. This growth increased online spending to 17 percent of total retail purchases, up from 15 percent during the pre-Christmas 2007 shopping season.

Online banking in the UK has also enjoyed robust growth with APACS reporting the number of adults using online banking increased between 2000 and the end of 2007 from 3.5 million to 21 million, or two out of three adults with an internet connection.

No room for complacency

Despite the growing numbers of online shoppers and bankers there is no room for complacency. In its report on online security the House of Lords' Science and Technology Committee warned: "The internet relies on the confidence of millions of users, and that confidence is in danger of being undermined unless we can reverse the trends our witnesses told us about."

Indicative of the threat online crime poses to confidence, a study undertaken by market research firm YouGov revealed that in 2006, 3.5 million people in the UK had fallen victim to online fraud, a figure that represents about one in ten internet users. Of those affected 1.2 million were victims of online banking or credit card fraud.

A clearer indication of consumer confidence in using a credit card online was provided by a survey undertaken in January 2008 by Finnish internet security specialist F-Secure.

According to F-Secure 50 percent of respondents in the US, Canada, the UK and France felt their credit cards were secure when shopping online while in Germany a mere 15 percent felt the same.

There was a somewhat more positive attitude towards online banking with 65 percent of respondents in the US, Canada, the UK and France reporting confidence in the security of their online banking. However, again German's were far from convinced with only 28 percent of respondents in Germany reporting they were confident in the security of their online banking.

The generally higher level of confidence in online banking is no doubt a reflection of a concerted and well publicised effort by banks to enhance online security, particularly in the area of customer authentication. Initial online banking security using passwords proved vulnerable and in 2005 prompted US federal regulators to issue a guidance that set banks searching for enhanced security systems.

At the time, regulators stated: "The agencies consider single-factor authentication, as the only control mechanism, to be inadequate."

Two-factor authentication became the order of the day. In the UK, for example, in March 2006, Alliance & Leicester became the first UK bank to announce a two-factor solution, PassMark, comprising a small image displayed during log-in to the bank's website which would assure customers the site was genuine and thus safe to enter passwords.

In April of the same year, HSBC followed suit, announcing it would supply online business customers with keyring-sized token devices developed by Swiss security specialist Vasco that generate a single use security code. In July 2007, Barclay's followed this up with the launch of PINsentry, a hand-held PIN and chip card two factor authentication device developed by Dutch digital security specialist Gemalto. By July 2008, more than 1.5 million PINsentry devices had been deployed, an uptake representing half of the bank's online customers and 30 percent higher than original expectations.

In the UK two-factor device market the greatest success has been achieved by XIR-ING. In July 2008 the French security solu-

tions vendor reported that in 18 months it had supplied 4 million of its Xi-Sign hand-held PIN and chip card readers to UK banks, a total representing four out of every five two-factor devices in use in the UK.

Introduction of two-factor authentication in the UK appears to be reflected in fraud related online banking losses in 2007 which, according to APACS, totalled £22.6 million, a decrease of 33 percent compared with losses of £33.5 million in 2006.

However, last year's decline was followed by a dramatic reversal of this promising picture in the first half of 2008 with APACS reporting total online banking fraud losses of £21.4 million, up 185 percent compared with the first half of 2007.

Introduction of chip and PIN hand-held readers and many other two-factor authentication mechanisms did have a positive impact on the UK CNP fraud figures in 2007, said Dix. However, he continued, introduction of new authentication mechanisms has been relatively slow and limited in its coverage. For example, chip and PIN readers have only been issued by a selection of banks so far.

In addition, said Dix, the roll out of two-factor authentication has mainly been implemented for online banking log-on and some funds transfer transactions. Thus although the initial roll out helped the banks in these areas there are still some CNP transactions (mail order, telephone order and some internet transactions) which are not yet secured by the new technology.

"This is another case of fraud migrating to the weakest link," stressed Dix. "The initial roll out focused on the then biggest areas of fraud loss. Now secured, the fraudsters are looking for the next weakest link to exploit."

Certainly one UK bank, Barclays, can claim a significant degree of success from its two-factor initiative and an intensive campaign to educate and assist online customers including offering them free comprehensive internet security software.

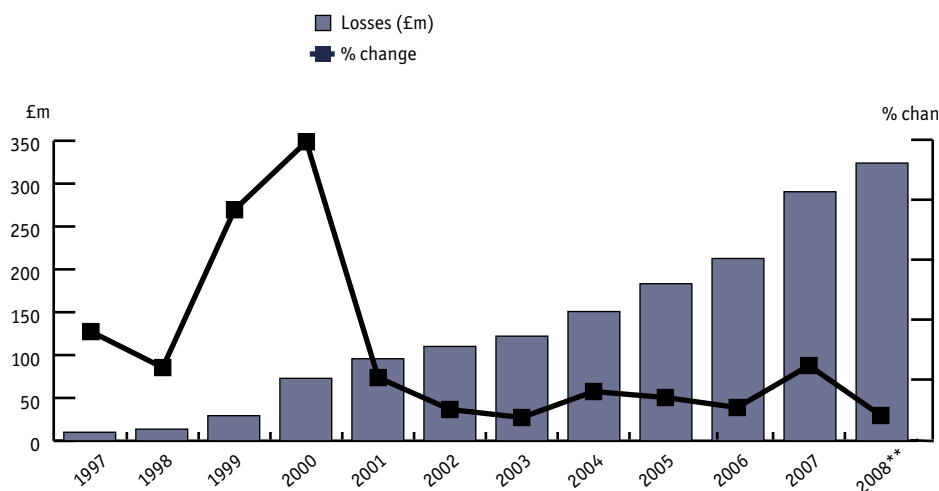
According to Barclays, its online security initiatives resulted in a 91 percent drop in the money lost to fraudsters from 2006 to 2007. In addition Barclays is the only UK bank to have seen a reduction in the number of phishing attacks. However, two-factor hand-held devices have one major drawback.

"Card holders do not like carrying card readers around with them," noted Dix.

In a search for a more convenient alternative many banks are keen on a product developed by US vendor Innovative Card Technologies (InCard) said Dix. In essence, InCard's solution is a conventional payment card that incorporates a button that when pushed generates a one-time password that is displayed on small screen on the front of the card.

■ UK ELECTRONIC PAYMENTS FRAUD

Card-not-present losses*



* Internet, phone and mail order ** First half annualised

Source: APACS

Though InCard's solution is a great concept it is too expensive, said Dix.

"Banks are in business to make money and the cost of the solution to counter fraud must be less than the cost of the fraud itself," he said.

Mobile solutions

In their quest for a cost-effective and convenient solution for customers many banks are looking to mobile phones as a potential two-factor solution, said Dix.

In response to this, mobile phone-based solutions are making their appearance. One of these is Celso, a two-factor authentication solution developed by UK online security services company Commerce Media.

Celso was developed for the Ministry of Defence's (MoD) Disposal Services Authority which sells surplus equipment, Commerce Media's MD Michael Robertson told *EPI*. Celso, he added, was designed to replace a token device, that had previously been used by the MoD.

"We looked at a number of options and came up with Celso," continued Robertson. "It is simple, secure and scalable and needs no special hard- or software – just a mobile phone."

With the Celso solution, when a customer logs on to a bank's website a one-time user password (OTP) is automatically sent to his or her mobile phone, email account, or via instant message. When prompted by the web application, the OTP is entered by the user. The user decides the length and complexity of the password and its validation period, which could be a few minutes, hours or days.

The Celso solution, said Robertson, has many advantages, including significant savings achieved by obviating the need for hand-

held devices and lower ongoing system running costs.

Celso also addresses human error security issues. For example, said Robertson, research has shown that it is not unusual for bank customers to keep their hand-held security device in the same bag as their laptop computer. By contrast, people invariably have their mobile phone on them, he added.

Undoubtedly, the MoD provides a solid reference to the efficacy of Celso.

"The MoD has also had Celso tested independently and it came through with flying colours," said Robertson.

He added that in addition to the MoD there is already a big user base in the private and public sectors undertaking trials with Celso.

Under siege

Solutions such as Celso come at a time when criminals are mounting an unprecedented assault on online commerce and banking. This is evident in data from APACS that reveals phishing attacks at luring customers of UK banks into disclosing sensitive information increased almost three-fold to 20,682 between the first half of 2007 and the first half of 2008.

In the US the Federal Bureau of Investigation warned in October that "major attacks" are on the rise.

"New groups of hackers – virtual gangs – are a growing threat, banding together to pool their expertise and carry out coordinated cyber attacks," said Shawn Henry, assistant director of the FBI's Cyber Division, in a statement.

Henry explained that in the physical world if a gang wants to rob a bank, it needs criminals with various skills – safe cracker, get-away driver, look-out and so forth – essentially what

is found in the cyber world today, only virtual gang members have never met in the physical world.

“There are organised groups that are very successful,” said Henry.

Fortunately at least one of these cyber-gangs, the Dark Market Website (DMW), is out of action and 56 of its members in custody thanks to action taken by the FBI and the UK’s Serious Organised Crime Agency. At the time of the arrests some \$70 million in compromised victim accounts was at risk.

According to the FBI, the DMW was a virtual transnational network of criminals involved in buying and selling of stolen financial information including credit card data, login credentials and equipment used in financial crimes. At its peak the DMW had over 2,500 registered members.

Methods used by online criminals are also becoming more sophisticated in areas such as social engineering which is, in essence, the ability to deceive people into divulging confidential information. Phishing attacks are the most common form of social engineering but not the only one.

One of the most successful of these alternative social engineering attacks occurred in 2007 and was described by internet security developer McAfee in a recent report.

In the attack, customers of Swedish bank

Nordea received an email that appeared to have originated from the bank. The email offered anti-spam software to the customers, 250 of whom downloaded and installed what was in fact a Trojan virus that enabled the criminals to collect customer information, log into the bank’s web site and steal money. The world’s biggest online theft on record the scam resulted in Nordea losing \$1.1 million.

Issuing a warning of potentially worse to come, Jeff Green, a senior vice-president at McAfee’s Avert Labs, said: “Cybercriminals are crafting attacks that are virtually impossible for computer users to identify.

“Phishing scams, e-mail attacks, Trojan horses, and other attacks are so personalised that even someone with the most watchful eye could fall for a carefully socially-engineered trap.”

Of significant concern, McAfee believes that “socially engineered spam [emails] will explode”. For example, it is predicted that criminals will use information collected from data breaches to fake customer loyalty programmes or offer discounts to recent shoppers.

And proving that no one is immune to online fraud, the French government has announced it is investigating the theft of money from French president Nicolas Sarkozy’s online bank account. His bank faces the prospect of

■ UK ONLINE BANKING

Phishing attacks targeting banks

Six months to	Attacks
June 2005	312
December 2005	1,378
June 2006	5,087
December 2006	9,069
June 2007	7,224
December 2007	18,573
June 2008	20,682

Source: APACS

some form of punishment for not preventing the security breach.

Rising criminal activity also comes at a time when banks find themselves under pressure to increase security. In July 2008, for example, the House of Lords called on the government to enact legislation that would underpin UK banks’ liability for customer losses resulting from online crime.

Of particular concern in the current economic environment is the extent to which spending on technology in general and security in particular will fare.

“Unfortunately, when it comes to spending on IT it is often security and testing that suffers first,” said Dix. ■

■ SECURITY

MIFARE Classic smartcard’s security flaws put out on public display

In an academia version of ‘publish and be damned’, researchers from the Digital Security group of the Radboud University Nijmegen (RUN) in the Netherlands have made public their research paper detailing serious security flaws of the world’s most widely used radio frequency identification (RFID) smartcard, the MIFARE Classic.

The researchers headed by Professor Bart Jacobs made their paper, *Dismantling MIFARE Classic*, public at the European Symposium on Research in Computer Security 2008 conference in Malaga, Spain on 6 October.

Publication of their findings followed abortive legal attempts by Netherlands-based NXP Semiconductors (NXP), the developer of Mifare Classic, to prevent Jacobs and his team going ahead.

The RUN team first announced that they had found weaknesses in the authentication mechanism of the Mifare Classic in March this year. Their announcement followed a similar claim made by in December 2007 by German researcher Henryk Plötz who in August 2008 submitted his findings to the

Humboldt University in Berlin in the form of a 100 page thesis. His thesis, in German, is freely available on the internet.

Of particular significance in the RUN team’s findings was that they were able to reconstruct the Mifare Classic card’s CRYPTOTO1 encryption algorithm “in detail” and discovered “a relatively easy method to retrieve cryptographic keys, which does not rely on expensive equipment,” noted the researchers.

“Combining these ingredients we succeeded on mounting an actual attack, in which a Mifare Classic access control card was successfully cloned,” the researchers added.

In a response to the RUN team’s publication of its findings NXP said it had “an open dialogue” with the RUN and other researchers on the MIFARE Classic’s security and had “taken the lead in communicating the effects of attacks and possible countermeasures to industry partners who need to know”.

However, rectifying the card’s flaws is no easy matter.

“Security upgrades, whether still based on MIFARE Classic or migrating to a different card format, are complex system modifications which may involve a combination of hardware and software in the cards as well as in the infrastructure and back-end equipment,” conceded NXP.

“As these upgrades can – based on the particular system security requirements – take up to a number of years, it is not conceivable that all MIFARE Classic infrastructures have their security upgraded to the necessary level yet.”

With about 1 billion in use the Mifare Classic contactless smartcard commands a 70 percent global market share according to NXP.

Used in a wide range of applications the card has been highly successful in public transport where it accounts for 80 percent of all electronic tickets.

Major contactless payments transport projects that have deployed the card include those in London (Oyster), Netherlands (OV-chipkaart), Boston (Charlie Card) and Beijing (One Card). ■