



Over the Water -- The View from the UK

By David G.W. Birch
Director, Hyperion
8 Frederick Sanger Road
Surrey Research Park
Guildford Surrey GU2 5YD, UK

daveb@hyperion.co.uk

Where people, networks and money intersect.....Consult Hyperion

<http://www.hyperion.co.uk>

info@hyperion.co.uk

The Card Myth: Why won't people use their cards on the Net?

Why don't consumers use their credit and debit cards on the Net more? How would we know if they did? If I email my credit card number to a retailer to buy something, does the card transaction show up in the books as a Net transaction or just as a mail order transaction? According to research firm Killen Associates, \$4.6 trillion worth of retail and wholesale purchases were made around the world in 1996, of which 13% (\$595 billion) were made remotely, by catalogue, TV, EDI and the Net. All of these purchases will start gravitating toward the Net over the coming decade, but (supposedly) the perceived lack of security is a block on the growth of Net transactions and it will take the deployment of Secure Electronic Transactions (SET) to overcome it.

Unsafe at any Speed

Every few weeks the UK newspapers report yet another Automated Teller Machine (ATM) fraud or attempted fraud. Last month there was a court case involving a guy who had constructed a false side to an ATM and put a tiny camera inside it to record people inputting their Personal Identification Numbers (PINs). Before that, there was a case involving an ATM engineer stealing money from machines he was supposed to fixing. Before that, it was a case where a guy had used a camera with telephoto lens, rented an apartment opposite an ATM machine, and again recorded PINs.

There have even been cases of people installing second-hand ATMs purchased from banks. These ATMs are installed in empty shops or new shopping malls: unsuspecting members of the public insert their cards, punch in their PINs and get a message saying Sorry, unable to dispense cash at this time. In the meantime, the bad guys have used the ATM journal to get a list of card numbers and PIN codes which they then use to create bogus cards and withdraw cash. This kind of inventiveness is not restricted to the UK and similar cases have been reported in many countries.

The media even hype the dangers: witness the recent hysteria about the conviction of an ATM gang of high ambition. A collection of villains compelled a software expert who was in prison (for attacking his wife and child) to help them in their enterprise. The man revealed his role to a prison chaplain and subsequently acted as an undercover informer on his release. The plot was to tap telephone lines carrying encrypted ATM card details to and from the banks. Having decrypted the information, fake ATM cards with genuine details would be manufactured from the 140,000 blanks they had bought. Teams of associates armed with the cards would then withdraw cash in the UK and abroad. The media coverage, based on the claims of the prosecution, said the plot had put the entire banking system in danger, although

my recollection of the case is that the prosecution never managed to demonstrate that the conspirators had the slightest hope of decrypting the data or getting away with fraud on such a large scale.

Deliberate fraud aside, ATM networks go wrong. Just to use one illustrative example: in October, 1996, Ent Federal Credit Union in Colorado Springs announced that it was about to subtract a total of \$1.2M from the accounts of 12,000 customers because, for over a year, multiple identical ATM withdrawals on the same day were incorrectly processed: only the first withdrawal was charged to the account!

What this all of this means is that the general public are constantly reminded that ATM networks are far from perfect and like any other complex machine, they can occasionally go wrong. Cases of phantom withdrawals are rare but not unknown. Yet people use their ATM cards all the time, because there is a compelling reason for doing so: they need cash.

The Dog That Didn't Bark

By contrast, people are reportedly reluctant to use their credit cards over the Net because of concerns about security. The principal concern would seem to be that credit card numbers being intercepted while traversing the highways and byways of the internet, yet to the best of my knowledge there is no recorded case of a credit card number being stolen during transmission over the internet ever. This is not just rare: it has never happened. The few reported cases of hackers stealing credit card numbers involves attacks on poorly configured retailer systems (magazine subscription databases and the like). This is obviously the best way to get credit card numbers. Why root through the billions of packets flowing around the Net on the off chance you might find a credit card number when you can go to a retailers system and find thousands of credit card numbers sorted, organised and arranged (and with expiration dates and billing addresses).

I've used my credit card number over the Net many many times. In fact, I did it last week when I emailed my credit card number to a software company to pay for a CD ROM game I wanted. I wasn't in the least concerned about hackers: after all, if the credit card number gets stolen, that's the credit card company's problem, not mine.

Here's the apparent conundrum then: people read reports of ATM fraud all the time, yet they use their ATM cards all the time. People never read reports about credit card numbers being stolen over the Net (although they do read lots of reports about how this might happen), yet credit card transactions on the Net seem to be held back by fears about security. If its not concerns about security, then why so few apparent credit card transactions on the Net? It seems to me there are two possible explanations, both equally plausible. Either, credit card use on the Net is underreported, or (more likely) people don't use their credit cards on the Net because theres no compelling reason for them to do so.

It takes time for new technologies to enter the market: It took a few years for debit card use to overtake credit card use, for example, in the UK. Interestingly, debit card use is now growing in the US as well and ATM surcharges appear to be one of the main reasons because cashback on point of sale (POS) transactions avoids a costly trip to an ATM. Perhaps its as simple as this: people don't use their credit card numbers over the Net because its new, and they're not used to it. Perhaps credit card use on the Net will increase over time as people become more familiar with the idea of buying over the net, as secure email becomes more widespread and as secure web connections become the norm. It took a few years for credit card mail and telephone orders to grow to current levels.

Game, SET and Match?

So where does SET fit into this? Since the major card schemes agreed to cooperate, SET has progressing slowly but surely and the first SET transactions took place last year, just: IBM, MasterCard and Danish Payment Systems (PBS) performed the first SET transaction on December 30th 1996. Both Visa and Mastercard have major European pilots planned for the coming year.

Theory has it that because SET makes credit card transactions on the Net secure, consumers will step up credit card use automatically. However, as more than one industry observer has noted, SET won't mean anything to the vast majority of consumers. So far as Joe Sixpack is concerned, he's still using his credit cards on the Net. SET is a solution (to a problem that might well fade in time anyway) for technology providers, banks and card schemes. It delivers no additional functionality to consumers and this suggests that SET will only prosper in the mass market if it can be somehow linked in with other facilities that do deliver improved functionality. An example might be a link with new microbilling protocols, or the use of SET certificates in other areas (to prove that the holder is over 18 or whatever).

In Europe, something else is happening with SET. Visa, Mastercard and Europay have already announced that they intend to bring the SET and EMV (smart card) specifications together later this year. If smart cards become vehicles for carrying SET certificates (unlikely at the time of writing since these certificates are large) then most consumers will have SET certificates issued to them in this form. This kind of implementation actually has a particular advantage: the SET certificate is now personal and portable rather than being tied to a specific PC as in the current SET implementations. In France, Carte Bancaire has already started work on its CSET (Chip SET) project. This uses smart cards to carry information relevant to the payment scheme. When a CSET card holder purchases from a CSET merchant (whether over the phone, Minitel, Net or in person) an efficient smart card-to-host protocol is used which moves all security processing off of the network involved because its handled by the smart card. When a CSET card holder purchases from an SET merchant, the CSET to SET gateway uses the information found on the CSET smart card to dynamically generate an SET certificate. This provides a potentially richer vision of SET in the Net marketplace. In this vision, efficient software or smart cardbased payment schemes operate over the Net with SET operating in the background as the backbone carrier. So long as different acquiring and authorising networks use SET as their external gateway, they can interoperate. Internally, however, they will use a more efficient implementation.

Historically the Net has been an American space. This has naturally meant that early work in the payments field has focused on the use of PC-based software and credit card clearing and settlement as the basis for electronic commerce. This work has therefore ignored the more sophisticated payments infrastructure in Europe, has not taken account of the rapid transition from dumb cards to smart cards underway in Europe right now, or the prevalence of debit and ATM cards: in the Netherlands, Interpay chose to use iKP rather than SET because most Dutch consumers want to use debit cards rather than credit cards .

None of this is to say that implementing SET is not worthwhile: merely to point out that to think that implementing SET will transform consumers use of credit cards has no basis in fact: the use of credit cards over the Net is a more complex matter than it might seem at first.

This decision will clearly depend on their view of the core business: is it applications such as SET or is it the certificate business? The Internet Driving Licence First, a short tutorial. Public key, or "asymmetric" cryptography depends on the use of two different (but related) encryption keys. A private key known only to the sender of a message, and a public key known by, well, the public. If I want to send you a message that only you can decode then I encrypt it with your public key. When you receive the message, you can decrypt it with your private key. This technique is at the heart of S Norwich Over the Water or the Silver Triangle is the name given to a district located in the north city centre of Norwich, England, that spreads outwards from the city centre towards Sprowston. The term "Silver Triangle" has also been used to refer to the large expanse of Victorian terraced north of Magdalen Street, after the city's other Victorian district, the Golden Triangle. Magdalen Street is a busy, cosmopolitan street home to many independent businesses, pubs and churches. The United Kingdom might be small but its countryside is mighty, and incredibly diverse, from rolling green hills and ancient woodland to impressive mountain peaks, idyllic lakes and rugged moors. To see all the different kinds of landscapes the UK calls its own, take a tour of the UK's 15 National Parks, from the flat Norfolk Broads and the wilds of Exmoor to the high drama of the Lake District and Peak District and the internationally recognised dark skies of Northumberland. Discover the most beautiful national parks in the UK.