

Computer Weekly – June 2008, Hardware reputation and the online fraud arms race

By Bob Tarzey, Service Director, Quocirca Ltd

Banks are used to arms races. In the 1960s and 1970s the easiest way to for thieves to get hold of a bank's money was to turn up in person at branches with a gun and demand cash. So banks placed their workers behind bulletproof glass. This forced the thieves on to the roads where the vans transporting cash became the main target. When the vans themselves were armoured it was the man walking from the van to the bank who became the target, he too was armoured.

These days such armed robberies are rare, partly because banks and their "real world" cash are now too well protected but also because an easier and safer way for thieves to separate banks from their money has emerged - online fraud. Banks are in a new arms race - can they win this one?

First, we should never underestimate the thieves. Bad they may be, but they are also clever. "Real world" bank robbers may have put stockings over their heads, but for an online fraudster, disguise is more subtle and easier to achieve. The easiest way to commit fraud is to pretend to be someone else with a good reputation. This is why data leak prevention has become such an issue with all the big IT security providers making acquisitions in this area - Symantec/Vontu, Trend Micro/Identum, McAfee/Safeboot.

Data leak prevention focuses on making sure sensitive data only leaves the business for good reasons and when it has to it does so securely. Such products aim to help reduce the embarrassing data losses faced by many organisations over the past 18 months or so which potentially provide rich pickings for the would-be online thief. But this does not prevent banks' customers giving their own details away through online scams such as phishing attacks (e-mails purporting to be from respected organisations asking for financial details) or key loggers (spyware the records activity on users' PCs). Customers can be encouraged to install desktop protection tools, but many do not.

Banks can tackle phishing directly by working with service providers such as Mark Monitor that identify and close down phishing sites before they can have an impact. But despite all these efforts, personal financial information will get into the public domain and fraudsters will have IDs with a previously good reputation to transact online with. Spotting a thief using someone else's ID online is hard and banks and their business customers don't want to turn away valid business or make it too hard to transact online.

Banks and credit card companies try to spot anomalous behaviour for a given customer and are using stronger ways of authenticating them. However, there is another line of defence that is about to get a big push in Europe. It is not just people that have reputations, hardware devices do too. Hardware reputation is the business of Iovation, a vendor founded three years ago in the US which has just secured new funding for overseas expansion.

Iovation has a database containing more than 30 million hardware devices and their reputations. This information is used to allow transactions to go ahead from trusted hardware and question any that are not. For example, most people will conduct online banking from the same PC on a regular basis. Over time, that device will become trusted. If they start using a different device questions might be raised. It might be a device known to be owned by an internet café or a newly manufactured device (both probably OK) or it may be a device that has previously been used for fraud (clearly not good).

But even a device that Iovation has never seen before may come under suspicion. Many online fraudsters conceal their behaviour by keeping transactions small, better to get little amounts of cash using hundreds of different stolen credit card records than raise suspicions by making one large transaction using a single record. However, Iovation can easily spot serial requests for different credit cards coming for the same PC, warn its customers and flag the device in its database as untrusted.

There are no privacy issues as Iovation does not store anything other than a device's reputation to date and its identity which is made up of a number of factors that make it unique (software serial numbers, hardware configuration, MAC address etc). Even so, Iovation says its customers are loathe to go public because this would alert the fraudsters of which banks to be wary of and take evasive action. For obvious reasons banks are a large part of Iovation customer base, but it is also signing up online

retailers, gambling sites and gaming sites - all of which transact online.

Hardware reputation is not a silver bullet, but used alongside other techniques, data leak prevention, scam detection, user education and so on, it makes life harder for the fraudsters. The arms race is likely to continue, but on the whole banks are maintaining the trust of customers to transact online and that in itself is a victory.

About Quocirca

Quocirca is a primary research and analysis company specialising in the business impact of information technology and communications (ITC). With world-wide, native language reach, Quocirca provides in-depth insights into the views of buyers and influencers in large, mid-sized and small organisations. Its analyst team is made up of real-world practitioners with first hand experience of ITC delivery who continuously research and track the industry and its real usage in the markets.

Through researching perceptions, Quocirca uncovers the real hurdles to technology adoption – the personal and political aspects of an organisation's environment and the pressures of the need for demonstrable business value in any implementation. This capability to uncover and report back on the end-user perceptions in the market enables Quocirca to advise on the realities of technology adoption, not the promises.

Quocirca research is always pragmatic, business orientated and conducted in the context of the bigger picture. ITC has the ability to transform businesses and the processes that drive them, but often fails to do so. Quocirca's mission is to help organisations improve their success rate in process enablement through better levels of understanding and the adoption of the correct technologies at the correct time.

Quocirca has a pro-active primary research programme, regularly surveying users, purchasers and resellers of ITC products and services on emerging, evolving and maturing technologies. Over time, Quocirca has built a picture of long term investment trends, providing invaluable information for the whole of the ITC community.

Quocirca works with global and local providers of ITC products and services to help them deliver on the promise that ITC holds for business. Quocirca's clients include Oracle, Microsoft, IBM, Dell, T-Mobile, Vodafone, EMC, Symantec and Cisco, along with other large and medium sized vendors, service providers and more specialist firms.

Details of Quocirca's work and the services it offers can be found at <http://www.quocirca.com>