InformationAge Webinars

Q&A from the Online Identity Theft, 20 February 2006

Presenters:

- **David Lacey, former Chief Security Officer, *Royal Mail*, and a member of *The Home Office Committee on ID Theft***
- **Ryan Kalember, Technology Director, *Verisign*, and a leading authority on federated identity management technology**
- **Bori Toth, Biometric Research & Advisory Project Lead, *Deloitte & Touche***

Q1 (to Bori Toth): How can we have confidence in biometric methods when "techniques" to trick tem have been demonstrated (albeit crudely) in a number of popular films. Is there a risk that stealing biometric details could result in physical harm to their owner?

> **A1: While there are ways to circumvent biometric systems, methods shown in movies often do not represent realistic means of spoofing. Biometric credentials are quite easily available: we leave our fingerprints everywhere behind which almost always contain enough information for DNA to be extracted as well; our faces are being recorded at every ATM, petrol station, bank etc; our voices are being recoded by many phone-based service providers. These credentials can be copied as well, so the question is not whether biometrics can be spoofed but whether or not the systems in place are sophisticated enough to ensure that the biometric sample obtained was submitted by the live and legitimate user.**
>
> **If a fingerprint system is not properly guarded against attacks using dead tissue (there are several countermeasures to protect against this type of spoofing attack), a dismembered finger might grant access to an unauthorised user. With regards to irises, this type of attack is not possible as the pupil expands within seconds after an eye is removed from the body so that not enough iris stays visible for a recognition to be performed.**
>
> **For more information on spoofing and liveness testing please contact us directly via www.deloitte.co.uk/biometrics.**

Q2 (to Bori Toth): In light of Bori's comment on Biometric security not being failsafe. What is the panels view on the UK ID card being based upon biometrics - after all you can get a new card or token but not a new fingerprint?

> **A2: There are ways to create revocable biometric templates – for example this is naturally possible for iris recognition as iris templates contain 256 data bytes that have no spatial metric. Having no spatial metric means that these 256 data bytes can be put into any order without preventing the possibility of performing comparisons between the enrolled template and the sample submitted for identification / authentication, as long as the bytes in these iris codes were scrambled using the same permutation key. The number of different iris codes that can be created per eye is 256! = 10^507.**

Q3 (to Ryan Kalember): The eBay system might work well, but the fraudsters are contacting the bidders outside the bid process pretending to be eBay. Then take the monies and do not deliver the goods. eBay is ignoring this type of fraud. Why?

> **A3: Although VeriSign cannot speak for eBay in this case, eBay's policy is to have a largely self-regulated user community using feedback mechanisms. The eBay fraud team will become involved with cases meeting certain criteria. VIP involves a similar "trusted network" model, but employs self-learning fraud detection technology rather than user feedback.**

Q4 (to Ryan Kalember): Are the banks going to agree to delegate (federate) their identity systems to eBay? How much indemnity will eBay or Verisign provide them?

> **A4: Banks are not intended to delegate identity systems to either eBay or VeriSign in this model. The "user store" will remain with the bank, and will be composed of the existing directory system (i.e. LDAP or Active Directory). The "token store" will be hosted at VeriSign, enabling the federated VIP model.**

Q5 (to Ryan Kalember): If the verification token is misused the genuine person will get the blame for the misuse. This can be seen internally with investigations to insider misuse.

> **A5: While technically correct, the theory behind VIP is that the authentication token must be used in conjunction with the user information that is already being stored (such as an entry in a directory system). In that way, the security measures that are already in place are enhanced rather than supplanted by the strong authentication**

system. Simply having the token should not guarantee access in the majority of use cases.

Q6 (to Ryan Kalember): Before issuing token you are reliant on the verification procedures at Dun & Bradsteet (or similar) and verification of physical address. Both may have serious flaws. Please comment.

A6. The authentication processes for corporate entities in order to procure a high-assurance certificate have been found to be appropriately stringent. While it should be noted that no system is perfect, it has nonetheless worked well so far and has not been "fooled." The model has changed for issuing tokens – the vision behind VIP is to let consumers, service providers, and other entities in need of strongly authenticating their customers (such as e-commerce enterprises, brokerages, and banks) use a trusted network that uses shareable strong credentials and includes the appropriate fraud detection services.

Q7 (to Ryan Kalember): Who is the person using the tokens etc? Who authenticates the individual?

A7: The VIP network members can choose how they wish to originally authenticate the individual. For example, a bank can issue a VIP token to a user in a branch, or allow the user to register their Motorola mobile phone as a strong authentication token for an account that already exists. The legitimate use of a token by a user then contributes to the data used in the Fraud Detection System, such as the user's typical geolocation, browser, etc., helping to make the VIP network more secure.

Q8 (to Ryan Kalember): Wouldn't it be better to use tokens already owned by the user e.g. Credit or Debit cards rather than additional tokens?

A8: To a large extent, the VIP does seek to take advantage of users a consumer already has, such as a mobile phone or a USB memory stick. However, credit and debit cards are not capable of generating a one-time password, for instance, making them ill suited to replace traditional passwords. In addition, the credit card providers have a transactional model for charging their users, which is not easily extensible to the variety of functions that can be enabled with the VIP network (such as account access, not simply completing a transaction).

Q9 (to Ryan Kalember): Risk based Two Factor Authentication has not been mentioned as a solution i.e. validation of device ID, IP address etc for login, with stronger authentication if required based on a risk score. Is this solution not considered as effective, adaptable, cost effective and a common solution with minimal customer impact?

A9: The Fraud Detection Services which are an integral part of VIP do use risk-based analysis factors, such as IP address, geolocation, operating system, browser, etc. Additionally, the services are self-learning, helping to increase the security of the network over time and proactively defending against new types of fraud. This is dependent on the web applications in question using the services to use additional information to authenticate suspicious logon attempts or transactions.

Q10 (to Bori Toth): Biometrics are good once you know who the person is but how do they help determine who the person is initially?

A10: Biometrics cannot help to establish the identity of a person at the initial enrolment. However, even those currently maintaining several identities can only enrol one identity in a biometric system – provided the architecture has been properly designed.

Q11 (to Bori Toth): Once ID cards come in, it will be nice and easy to get hold of biometric data....

A11: Biometric data does not constitute information that could be regarded as secret or private: our facial images are recorded every time we enter a bank, supermarket or even just pay at the petrol station; our voices are recorded by many phone-based service providers; and we leave our fingerprints and DNA behind everywhere we go. So, biometric data is widely available and under circumstances it is also rather easy to copy them. There are however effective countermeasures to spoofing – the only question is whether these technologies will be implemented in the ID scheme where it matters.

Q12 (to Bori Toth): Is your panel aware of the Passport office pilot on biometrics? Iris, fingerprinting and face scan. Best results were about 88% accurate. Not good enough to authenticate an individual.

> **A12: At the time being, there is little up-to-date scientific information available from independent UK sources with regards to the technical performance of biometric technologies and devices. The last technical performance test in the UK was performed by the National Physical Laboratory in 2000. Other trials and tests were either vendor-driven or not laid out to measure technical performance. A good example for the latter is the UKPS "Biometrics Enrolment Trial" of 2004 which was not a technical trial, according to its own set of defined objectives. Nevertheless, the final report published some technical performance metrics which are still being cited. In April 2005 Deloitte entered a partnership with the National Physical Laboratory to launch a new project to assess the technical performance of the latest biometric devices from an independent, scientific point of view. We are pleased to announce that the final report is currently in preparation and should be available in April2006. Once finalised, we will be happy to send you a copy of the report upon request which you can log at www.deloitte.co.uk/biometrics.**

Q13 (to Bori Toth): Biometrics may seem like a good solution now, but how much research has been done into the future possibilities of your biometric data being forged? Surely that puts people at even greater risk if even their biometric identity can be stolen too! This may seem like sci-fi now but it is highly likely to become a reality.

> **A13: Please see the sections above that talk about spoofing & counter measures.**

Q14 (to Ryan Kalember): I am the preferred training provider for APACS and FLA in identity fraud education for staff. Very few of the members have taken up this training/education to stop entry to the systems at the initial application. So I agree with Bori. Senior and middle management are reluctant to do anything regarding the issue as happening to someone else, not them.

> **A14: Our experience is that consumers are sufficiently wary of identity fraud to want a better way than the traditional, easily-compromised password. In addition, banks, e-commerce companies, and a host of others have realised direct, significant financial losses from identity theft. The motivation for a new solution is evident, and if these managers are not attuned to this, hopefully they will be soon before they subject those who depend on them to further risk.**

Q15 (to Ryan Kalember): What are the main USPs of VeriSign tokens vs. competitors?

> **A15: VeriSign does not actually manufacture tokens, instead using open standards for authentication (www.openauthentication.org) and operating a Unified Authentication and VIP service using tokens, software, and smart cards from the leading strong authentication providers in the industry.**

Q16 (to Ryan Kalember): To what extent do the panel believe that the rise in CNP fraud is attributable to the roll-out of Chip and Pin? Is this a good example of 'substitution' or the 'balloon effect'?

> **A16: Certainly some of the rise in "card not present" fraud in the UK is attributable to the substitution effect caused by the introduction of Chip and Pin. However, the demands of modern e-commerce and the inevitable relocation of many crucial services to the internet means the trend will not abate without a more comprehensive, network-based approach. This will likely have the substitution effect of increasing fraud where passwords are still used.**

Q17 (to Ryan Kalember): How are you proposing the consumer validates the server? Presumably by some "high-assurance" cert? But this still implies that the CA will sign a very large number of web-site certificates. If any of those web sites were compromised or the CA was tricked into signing a certificate, it opens an opportunity for the browser to say "highly trusted" when it isn't - and may even be a different web site if DNS could be compromised. And in any case it would take a long time, if possible at all, to persuade all sites to get the signed by one of the "blessed" CAs. And that's not counting for trojans that compromise the browser and any checks.

> **A17: The consumer would validate the server via a high-assurance certificate, which, in the next version of Internet Explorer (and likely other browsers) will turn the address bar green. The web sites still need to secure both their operating systems and applications, and pharming will remain a threat (although a pharmed**

site would not turn the address bar green). CAs like VeriSign offering high-assurance certificates have not yet been tricked into issuing a certificate to a fraudster, but the point is well-taken that sites should have a high-assurance certificate as soon as possible (the biggest banks, brokerages, and e-commerce companies largely already do). Trojans are another threat, which is mitigated by the use of time-based tokens and fraud detection. Users will still of course need to patch and protect their machines.

Q18 (to Ryan Kalember): Won't users rebel against having to carry many tokens for everyone they transact with?

A18: Yes, absolutely. This is precisely why the VIP tokens are designed to be used in a federated way, and enable users to use the same token to replace as many of their passwords as possible.

Q19 (to Ryan Kalember): Can we have some examples of fraud management models for ecommerce and edentity systems? I've been looking at rules based systems to analyse fraudulent behaviours and also stochastical mathematics but wanted to know what solutions may be in use already?

A19: Please see the press release for information on VeriSign's fraud management model. The technology uses pattern recognition and behavioural modelling to detect fraud, and has a self-learning capability.
http://www.verisign.com/verisign-inc/news-and-events/news-archive/us-news-2006/page_036986.html

Q20 (to Ryan Kalember): Project carried out: Human problem. 250 people stopped at Waterloo Station they were questioned about ethics at work. The questions were trying to obtain all personal and work information. Such as DOB, mother's maiden name. Direct telephone numbers and passwords to work stations at companies. 248 people gave all the information. Average password used was word 'passport'. So what is the answer to the human weakness in passing on to anybody critical confidential information? I have more on this if you want.

A20: There are several ways around this very fundamental issue. While a password is easy to share, it's not really possible to pass around a one-time password, for instance. Extensive user testing with tokens has also led to the conclusion that people generally take much better care of a physical credential than a password (or their mother's maiden name, for that matter).

Q21 (to Ryan Kalember): Does using a digital signature on email increase security?

A21: Using a digital signature on email increases the assurance that the sender is who he/she says he/she is. A signed email with a high-assurance certificate is almost certainly not a phishing attempt, for example. It does not protect the confidentiality of the email content in transit, however; that requires email encryption.