

Complex protection made simple

By Bruce Kelton, Keltec Industries and **Andy Rushworth**, PeopleCount Australia

In 1996, a report presented by the Australian Transaction Reports and Analysis Centre stated that: “criminal groups ‘exploit’ payment systems in different ways. Some groups seek to profit from defrauding or otherwise attacking payment or transaction systems, while other groups will use the speed and anonymity of systems to perpetrate or launder proceeds of crime perpetrated elsewhere”. This exploitation now includes the creation of false identities.

I was exposed to two of those exploitations years earlier when returning to Australia from an overseas business trip. Did I pay AUS\$100 for a Gucci briefcase or forget a few zeros’ doing the conversion, or was it a fake? Why did my card statement show overseas transactions after my return?

Thanks to Australian Customs and those stamps they put in your passport, my card and I had arrived in Australia before some white card copy with an imprint travelled throughout Asia having a wonderful spending spree.

Luckily I could prove I was me, that I entered the country before the spending spree and had the real card in my wallet for presentation to the card company. And, the Gucci was real; bonus! But, what if I couldn’t prove I was me? What if I didn’t have information on my passport to prove the re-entry date?

White card and identity fraud are recent in Australia, but have been around for years overseas. Criminals will only get better at duping the honest, unless government goes one better and makes this fraud very expensive and very difficult to perpetrate, instead of putting the onus on the citizen to prove innocence.

“The use of false and stolen identities is a growing threat and Australia is not immune,” said Senator Ellison, Attorney General in 2004. “Identity theft and fraud underpins many criminal activities, including terrorism, and costs the Australian community at least AUS\$1.3 billion annually,” he confirmed. “An

individual’s identity is a part of who they are. Victims can often spend years and thousands of dollars trying to restore their good names”.

In Australia, banks have been using a 100-point check to validate a person’s identity. But a criminal doesn’t need to fully create your identity. With basic information and slick talking your bank account can be emptied without you knowing until after the event.

Identity fraud is enabled using fake or modified documents or by knowing enough about you to emulate your identity. Would a citizen, when submitting documents and information for a bank account, electronic passport/visa, driver’s license or ID card, be overly inconvenienced if a biometric were included for their protection? It’s already there as a signature.

Biometric identification is the use of biological attributes for unique identification, and confirmation that you are who you say you are. I don’t see the problem in the government having a biometric or two of mine, as long as they don’t abuse the privilege. But I would like the right to approve or decline the use of my biometric and choose the biometrics. Can I trust the bureaucrats to use them wisely and have they thought of the following?

- While technology designers make assumptions about us the user, their assumptions will exclude and discourage many. If we consider people with different abilities and limitations

[not disabilities] it doesn't take long to identify problems with each and every one of these current techniques for some potential users. Particularly if only a single biometric is used in isolation (extract: Tim Noonan, Blind Citizens Australia).

- Fact! The more levels of security you apply, the harder it is to break and the more secure the item becomes. Coupled with more user options, the design process using multi-layer security may become complex, but the application can still be simple.
- A chip-only solution on plastic isn't the answer and a duty of care exists when considering what hardware and technologies to use and how to deploy them.

In the US, hacker conventions attract full-time computer security professionals, law enforcement agents and the traditional hacker. Hackers and IT professionals have been attending conventions such as Defcon and Toorcon for years – and more recently, LayerOne.

At last years' LayerOne, a Mr Hulton stated that SIM card security was "security through obscurity". It is secure if no one breaks it. Well, it appears that Mr Hulton has broken it. David Hulton and another hacker demonstrated the vulnerabilities in smart cards, cable modems and parking metres, showing how SIM cards could be hacked using simple and cheap devices. Ian Goldberg, another hacker at LayerOne, showed how a narrow pipe attack on encryption reveals key information on a chip and can crack the data on it in 115,000 queries, defeating the chipkill capability when tampered with.

When dealing with documents that establish a person's identity, check that they are true and correct. Send a copy of the document to the issuing authority and ask for verification through a different transport mechanism that the document is true and correct. If you're the issuing authority, establish that the person making the request is who they say they are and the authority requesting the confirmation is who they say they are. Identity verification is the most critical part of identity creation. If it's a flawed

process then everything subsequent is worthless.

If you are going to use a biometric, use more than one. A citizen's approval for two is no greater to achieve than it is for one. But don't ask for five!

Consider those with different abilities and limitations when choosing the biometrics and hardware deployment. And, when choosing a technology and a medium for it, accept that technology alone is not the panacea.

Because of its security features, the LaserCard optical memory card was chosen over all other identification solutions by the US Department of State. Security features that are necessary for the widely used tamper-resistant permanent resident or green card and LaserVisa cards include optical media created using proprietary materials with additional security features to prevent counterfeiting. Cardholder information such as photograph, fingerprint and signature are written to the optical media and as an embedded hologram. Laser-written information appears on the optical media as a visual image and as a digital file. The same information is thermally printed on the reverse side of the polycarbonate card. Digital data, holograms and watermarks are embedded in the

optical media and cannot be changed or altered without destroying or invalidating the card. Complex technology deployed on a complex substrate is very difficult to change, emulate or copy.

Yet, verification is simple; match the laser-written hologram to the cardholder and to the thermally printed information on the card. In addition, a complete digital file of the personalised hologram can be interleaved within the hologram image, providing another way to positively verify the cardholder.

And, I keep my biometrics with me, allowing or declining their use when submitting the card for verification and authentication.

Some of these biometric and security features can be placed on a chip, but not all can – nor should they be. Using a single technology improves the probability of compromise.

Like the optical memory card (OMC), chips on plastic have been around for some time; the first licences were sold to Honeywell Bull, Schlumberger and Phillips from 1976 to 1978, well before the OMC in 1983. While the top half of the world embraces the LaserCard, we ponder the resistance here. ■



If we consider people with **different abilities** and limitations [not disabilities] it doesn't take long to **identify problems** with each and every one of these **current techniques** for some potential users

