The body as password - biometric technology and the form of appropriate legislation

Jay Forder

Follow this and additional works at: http://epublications.bond.edu.au/law_pubs

Recommended Citation
Jay Forder. (1998) "The body as password - biometric technology and the form of appropriate legislation" .

The body as password —
Biometric technology and the form of appropriate legislation

by Jay Forder, Consultant Editor.

The authentication problem
Is it becoming more and more difficult for you to keep track of numerous PIN numbers and passwords? Most people would answer a resounding “Yes!” to this question. Recent advances in the way we use technology, such as electronic commerce, depend on a user proving they are who they purport to be. This is known as the (identity) authentication problem.

Current digital signature technology includes the ability to authenticate a user. It is based on a system of double encoding using public and private keys.1 But like PINs and passwords, it is not infallible. Nor is it ideally suited to some situations such as withdrawals from an ATM. The ultimate goal is a system that is quick, inexpensive, 100% reliable and as unobtrusive as possible.

We have all seen the prototypes in science fiction. Heroes pass through security doors and access computers without having to stop and enter passwords. Books and movies have envisaged automatic identity checking for years.

Fact or fiction?
Using unique personal characteristics (such as fingerprints or voice patterns) to authenticate an individual’s identity is known as biometrics. Biometric systems get closer to the ideal than most other systems because they can’t be forgotten, forged or transferred and they can often be measured with minimal intrusion.

The International Computer Security Association (ICSA)2 suggests we have turned the proverbial corner. ICSA is a voluntary industry body with no formal authority but, following six weeks of rigorous testing by their Certification Lab, they recently announced the award of six biometric product certifications.3

The testing included using a random sample of over 1,000 volunteer subjects. Certifications were issued to:

- TechniLock Technologies Inc. for their Biometric Access Control System fingerprint verification product;
- iNTELTRAK Technologies for their CITADEL GateKeeper voiceprint recognition product;
- Miro, for their TrueFace facial recognition software;
- Mytec Technologies for their Touchstone fingerprint verification product;
- National Registry for their Secure Authentication Facility for Windows NT; and
- SAC Technologies for their SACcat fingerprint verification system.

Other biometric systems under investigation include thermal emissions of the body, hand geometry, vein measurement, skin pore mapping, the chemical composition of body odour and measuring features of the eye. Only three are considered to be truly unique to each individual: fingerprints, retina scans and iris patterns.4 Iris patterns in particular would be suitable for authentication at ATMs because of the ease with which they can be measured by video surveillance. Oki Electric Industry Ltd in Japan and Citibank in New York are both testing such systems.5

Technology-neutral legislation
Legislation may be necessary to deal with the legal effect of such systems. Digital signatures, which perform a similar function, have received legislative attention in many jurisdictions recently. There have been several calls for digital signature legislation in Australia.6

The previous issue of this newsletter gave an overview of the report of Australia’s Electronic Commerce Expert Group to the Attorney General released on 31 March. Legislative provisions from around the world were considered.

Fortunately the Expert Group recognises the advantages and disadvantages of some of the different approaches taken. One of the drawbacks of specific legislation for digital signatures is that it doesn’t cater for other methods of authentication, such as biometrics (the Expert Group considered digital signatures and biometrics to be part of a broader category which they called “electronic signatures”). Jurisdictions that legislated early, such as Utah, USA in 1995, were prone to assume that digital signatures based on public/private key cryptography were the only viable solution. Their legislation is technology specific.

Adopting the line taken in UNCITRAL’s model law, the Expert Group’s report recommends legislation that is technology neutral. This approach should be welcomed.

Legislation with two levels
The Expert Group also acknowledges the disadvantages in this approach. Legislation that is technology neutral needs to be formulated at a high level of abstraction. This significantly limits the scope for specifying detailed legal consequences, since different authentication systems may not have the same features or standards. Thus one could not state generally that all authentication systems presuppose binding the user as if a written document had been signed. The report recognises that “it may be desirable to have a two-level approach in legislation. The first and broad level would be technologically neutral, accepting all or most electronic authentication mechanisms for some purposes such as satisfaction of form requirements. The second level would … not [mandate] particular technologies, but … would … [require] that authentication mechanisms meet particular legislative standards or pass an approval process before their use is invested with other legal consequences.”7

Two models are contemplated to cater for future technologies: stating general
standards in the legislation and leaving it to the courts to determine whether a system meets those standards, or setting up an administrative body that sets standards and approves systems. The report does not express a view as to which is preferable. Regrettably it does not even expressly support this two-tiered approach to legislation in its final recommendations.

While acknowledging some anxiety over the proliferation of administrative bodies, I would suggest that it is the preferred solution in this instance. It has these advantages:

- It would allow standards to develop consistently as the technology develops. Thus, for example, it could respond in a timely manner to advances in computing power that would render insecure a system that appears reasonably secure today;
- It would not depend on litigants bringing their disputes to court;
- It would overcome the problems of expense and delay for individual litigants; and
- Consumers are more likely to be protected if they are able to know in advance that a particular system is accredited and that the legal consequences are relatively certain.

A legislative model along these lines would encourage consumer confidence and accelerate the realisation of many advantages of the information age.  

1 For a clear explanation of the way this works, see RSA Labs' Cryptography FAQ at <http://www.rsa.com/rsalabs/newfaq/>, particularly the answers to questions 1 and 3.
2 See the ICSA (formerly NCSA) web site at <http://www.ncsa.com/>.
5 John D Woodward, Believing in Biometrics, above.
6 See for example Standards Australia's Strategies for the Implementation of a Public Key Authentication Framework (PKAF) in Australia, published in 1996.
8 "Electronic Commerce: Building the Legal Framework", para 4.5.11.