Lockstep Consulting
ABN 59 593 754 482
Contact: swilson@lockstep.com.au

Is security and privacy a zero sum game?

Stephen Wilson
Online Banking Review column No. 12
August 2005

In late June, Sydney played host to the inaugural Australian Smartcards Summit. Presentations ranged across the business, policy, technical and project management aspects of EMV, healthcare, human services, ticketing & tolling, and e-passports.

Attendance by financial institutions was rather low. Perhaps most bankers feel they have heard it all before by now. Nevertheless, the summit brought out many fresh perspectives. In the UK, the *Chip and PIN* scheme has reached the milestone of 100 Million smartcards and is processing hundreds of transactions per second across the system. In the US, the Federal Government has finalised a technical specification called FIPS-201 for employee badges, which is likely to be favoured by Australian driver licence authorities.

The purpose of smartcards – and the value proposition for rolling them out – is most often thought to be protection against counterfeiting and skimming. Sometimes the smartcard's multi-function capabilities are also of interest, where loyalty programmes, ticketing, prepaid phone accounts and so on can be added to a basic bank-issued card. And as discussed in several of my recent columns, smartcards have unique powers to combat phishing and website fraud, not shared by any of the regular two factor authentication devices.

But this month I'd like to look more closely at an altogether different issue: privacy. With national identity cards back on the political agenda, sweeping claims are being put about that smartcards offer some sort of silver bullet to weed out terrorists and fraudsters. On the other side of the so-called "debate" are counter-claims that a national identity card would lead to secret surveillance of ordinary people, and that smartcards in general threaten privacy.

But one wonders if we're truly having a proper debate as yet. On both sides we see a great deal of fear, uncertainty and doubt, nay-saying and hype. As an advocate for smartcards, I long for a more sophisticated public analysis of their pros and cons, especially so that no matter what happens with the national id card, we don't see all smartcard schemes unfairly labelled as privacy invasive.

There is a worrying gap between most privacy and technology specialists. Part of the problem is that technology is currently on the nose amongst mainstream businesses. The "tech wreck" heralded a broad backlash against technology. Senior banking executives have famously questioned the true value of IT to the business, and it has become fashionable to say that such-and-such (insert your favourite business problem here) "is not a technology issue". The response of many technologists has been surprisingly defensive, with CTOs, CIOs and even vice presidents of crypto vendors adopting the slogan that "security is not a technology issue".

Is it helpful to polarise these debates, as if there are pure business issues in one corner and technology ones in the other?

Those who worry, in good faith, about the pitfalls and excesses of IT need to develop a more sophisticated understanding of the technology, if only so that they know what questions to ask in the debate. At the Australian Smartcard Summit, academic lawyer Justin Malbon tried to provide some balance in the privacy-security debate. But unfortunately Dr Malbon undermined his own position when he confessed that "most of [the technical talk] would be way beyond my capacity to understand". There are good privacy enhancing technologies out there, but it's going to be difficult for them to be fairly assessed unless privacy advocates and policy makers take a bit more time to understand the nuances.

For instance, smartcards are not mere storage devices, and yet "technology neutral" policy makers often presume there is no fundamental difference between smartcards, magnetic stripe cards and even floppy diskettes. On the contrary, smartcards can apply intelligent access controls before turning on certain functions. They can run business logic off-line, to enforce business rules in diverse operating environments and shut down critical functions if suspicious patterns of activity are detected. And they can use powerful on-chip cryptography to mask personal identifiers and to anonymise certain transactions.

Further details can be found in Lockstep's public submission to the recent Senate Inquiry into the Privacy Act; see http://www.lockstep.com.au/library/privacy/submission_to_the_2005_senate.

On the other hand, while some policy makers over-simplify matters, technologists often range immodestly into areas of social policy outside their own domain of expertise. Recently we've heard security specialists take the more or less political line that the balance between civil liberties and security has changed since 9-11. Not only does this simplistic analysis appear expedient, it also perpetuates the myth that security must inevitably be traded off against privacy.

Security and privacy need not be a zero sum game. There is a range of interesting new privacy enhancing architectures that can be built into smartcards. Multiple personal identifiers – or what some privacy advocates neatly call "digital personae" – can be loaded onto a smartcard, to keep the card holder's various e-business activities quite separate. And transactions launched using the smartcard can be secured using anonymous digital certificates, making it impossible to re-identify their origin, and yet still impossible to forge. These privacy enhancing functions open up new possibilities for value-adding bank-issued smartcards, with special services like electronic voting.

Therefore, rather than damning all smartcards out of hand, privacy advocates and policy makers ought to be asking more probing questions about precisely what type of systems are to implemented. And they can work with financial institutions to ensure that extending smartcards into retail transactions (whether those cards are issued by banks themselves or by third parties) is done with privacy safeguards built in.

Lockstep's considered position, based on independent research and analysis, is that greater use of smartcards – not less – is urgently required in all Internet business settings, to combat identity theft and thus protect the privacy of ordinary Australians. As the Victorian Privacy Commissioner Paul Chadwick said recently, "there's no worse privacy breach than for someone to pretend to be you".[1]

Privacy enhancing technologies not only make smartcards safe; they will also see smartcards being re-used for applications like electronic secret ballots (for shareholder meetings as well as government elections), census collection, electronic health records, and anonymous retail commerce. Given these possibilities and their broad based social importance, it's time we saw governments and financial institutions work together on the rollout of smartcards as critical infrastructure.

[1] SBS Television Insight Programme "I Spy" 15 March 2005.

Highlights

— New smartcard based Privacy Enhancing Technologies (PETs) can preserve both security and privacy

— Privacy advocates need to better understand the technical nuances while technologists need to stick to their knitting

— The business case for smartcards could be enhanced if financial institutions and governments worked together on the critical infrastructure.

About the author

Stephen Wilson is a leading international authority on identity management and information security. In early 2004 Stephen established Lockstep Consulting to provide independent security advice, and to develop new smartcard solutions to identity theft. Contact swilson@lockstep.com.au.