Smartcards, digital identity and black holes

5th Annual Smartcards Summit
19 October 2009, Canberra

Stephen Wilson
Lockstep Group

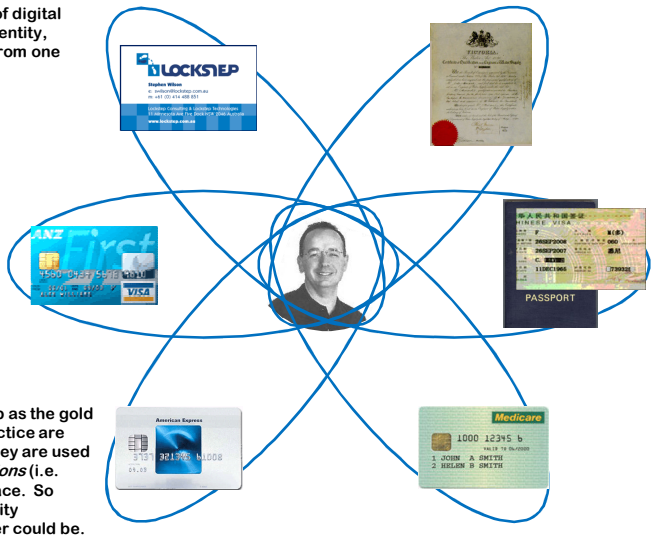
Avoiding the black hole of an ID card

- Recent history shows it is difficult to discuss digital identity, authentication and smartcards without being drawn into the black hole of an identity card.
- This presentation is chiefly concerned with breaking the nexus between smartcards and ID cards. Plenty of other commentators have questioned the fundamental needs for identity cards. Here we'll come at the issue from the other side: what good is smartcard technology in online security and privacy? And how do we design smartcard systems to avoid creating a new ID card by default?
- We do a good job today of identifying people. In a few cases like banking, identification is regulated. But for the most part, identification is a local issue. Most business transactions are based on specific qualifications and credentials. The rules are not worked out centrally, but vary from one sector to another.
- Different identities apply in different contexts, such as when a lawyer signs off on a piece of conveyancing, or when a doctor signs a prescription, or when a customer signs a credit card purchase. A small business owner might have their personal and business bank accounts with the same institution, but they exercise different identities (that is, distinct cards and accounts) when she does business banking and personal banking.
- In the real world, all these different identities are well managed. The pressing problem in cyber security is to be able to use real world identities online, without fear of theft, cloning, replay attack and impersonation.

Copyright © 2008 Lockstep Technologies Pty Ltd

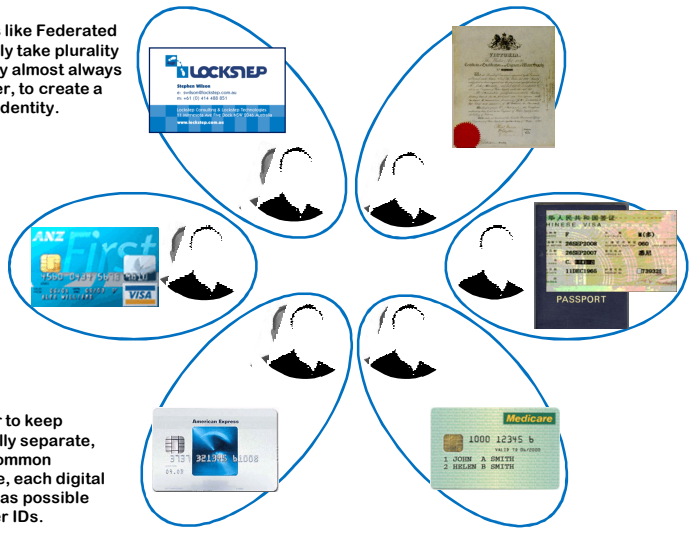
The reality of identity plurality

- Each of us exercises a "plurality" of digital identities. The meaning of each identity, and the rules for creating it, vary from one setting to another.
- Different organisations are generally free to follow their own identification protocols, though in some sectors minimum "Know Your Customer" standards are legislated. Protocols undergo continuous improvement in response to fraud trends. Identification risk management is usually a local issue.
- In business, we're usually more concerned with *what* a person is (in respect of their qualifications and position) than *who* they really are.
- Note that passports – often held up as the gold standard for identification – in practice are not always sufficient for travel. They are used as a special carrier for *authorisations* (i.e. visas) which vary from place to place. So there is actually no universal identity standard, and there probably never could be.



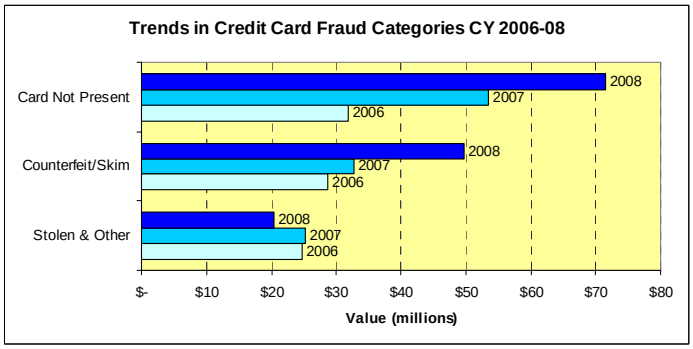
Keeping identities separate

- Currently popular movements like Federated Identity or "Identity 2.0" usually take plurality as their starting point, but they almost always go on to link identities together, to create a single sign on, or a new uber identity.
- Federation might be convenient but privacy and risk management are hugely complicated by joining up online identities. Traditional real world identities are issued in silos with tightly controlled risk profiles and strict Ts&Cs. Joining an identity to another silo exposes it to threats beyond the control of the original issuer.
- I contend it is generally better to keep different digital identities totally separate, and to not 'hang them off' a common master ID. For privacy's sake, each digital identity should reveal as little as possible about its owner and their other IDs.



Copyright © 2008 Lockstep Technologies Pty Ltd

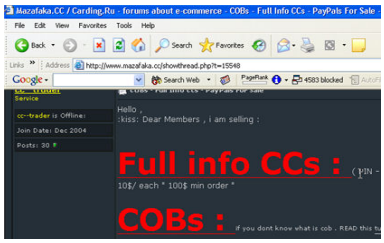
CNP fraud: the model cybercrime



Data adapted from APCA statistics released 15 May 2009

- The *model* cyber crime is online credit card fraud, for it illustrates how easy it is to assume numerical digital identities of others. Stolen credit card numbers are traded in enormous numbers in online black markets. Crucially, most card numbers are not stolen from customers as they shop online, but from department store databases and processing bureaus.
- Several hundred million credit card numbers are stolen worldwide every year. Over 50% of Australian card fraud now occurs online. Global online card fraud is likely to be worth tens of billions of dollars.
- To curtail identity fraud, we need to render stolen identities useless. Instead of any one new uber identity, we urgently need better means for translating *existing* identities into the digital world and protecting them there.

Take care of your keys



Identity Fraud: A$4B p.a.
AFP 2005

Car Theft: A$1B p.a.
ABC Four Corners 2006

- Digital identities are literally the keys to Internet banking, e-commerce, e-government and e-health. But at the moment almost all of our digital identities are vulnerable to theft and replay. At left is a screen shot from a leading Eastern European "carding" site where millions of stolen credit card ("CC") numbers are traded, along with CVV numbers, billing addresses and even PINs.
- We take more care with car keys than we do with our digital identities. Modern car keys cannot be copied willy nilly, and they come with electronic enhancements like engine immobilisers. But most businesses are timid about stronger online authentication, in case it compromises customer convenience. So we've got ourselves into a situation where identity fraud in Australia exceeds the cost of car theft.
- Smartcard technologies can safely convey real world identities online, so they cannot be stolen and replayed,. No new and arbitrary identification processes are required.
- Smartcard technologies are widespread in cell phones, bank cards, cable TV, and increasingly in government. We should be making more use of these technologies to protect digital identities.

Copyright © 2008 Lockstep Technologies Pty Ltd

Next gen Authentication needs

We're on the verge of large scale next generation services, with identity risks and community expectations that far exceed the rather relaxed norms set by e-banking and e-commerce to date

e-Health

Personal Health Records are emerging at a great rate, from Google Health, Microsoft Healthvault, Walmart in the US to name a few, as well as numerous commercial services in Australia. Few if any even of them offer multi-factor authentication, instead of using single factor password security (which is no longer deemed adequate for Internet banking). NeHTA is working on a life-long Individual Health Identifier. Is it safe to contemplate such a mission-critical digital identity without built-in security against theft & replay?

OSN, media

Age proofing is a hot issue. Most OSNs in the US have been held to account by state Attorneys General for not doing enough. New ACMA regulations in Australia require customers of MA15+ and R18+ online content to be age verified. But there are still no effective solutions. Best practice in the US involves social security numbers and identity checks, which changes the risk profile and business model of the OSNs, and requires trust in unknown new start-up companies.

e-Voting

Voting over the Internet is eagerly pursued for armed forces personnel and other workers stationed overseas; it is a long term strategic goal for the general public. The confidentiality needs are paramount, and must be met without compromising integrity.

This slide deliberately left blank

Copyright © 2008 Lockstep Technologies Pty Ltd

What's so smart about smartcards?

Simply, smartcards know what's going on around them

Smartcards have numerous special functions that are privacy enhancing

- **Access controls**
  Access to all data and functions in a smartcard is controlled by the built-in operating system. Several layers of access control can apply. One or more cardholder PINs/passwords typically unlock major functions; critical functions can require PIN re-entry to protect against abuse of a card left unattended in a reader, or against Man-in-the-Browser attack.
- **Mutual authentication, reader-to-chip**
  A smartcard can authenticate the card reader before enabling any functions. The card can differentiate between "dumb" readers and sophisticated official readers, and can disable some or all functions depending on the circumstances.
- **Anti-skimming**
  Authenticating the reader is the main defence against skimming. A smartcard can tell if it's inserted into an unofficial reader and can refuse to reveal its owner's secrets. Some secret codes (like embedded private keys) are generated inside the smartcard chip and are never revealed to any reader, thus fundamentally preventing card cloning.

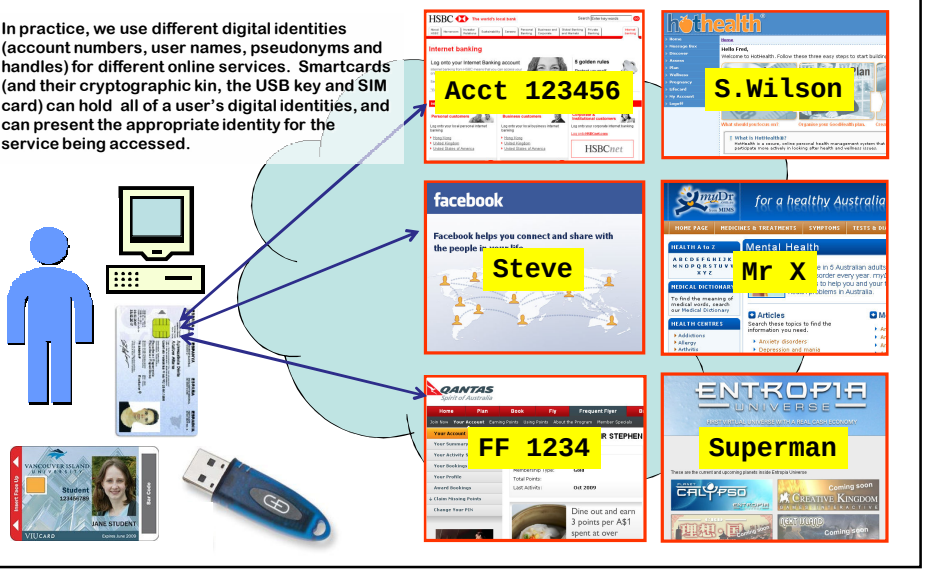
What's so smart ... cont.

- **Self-monitoring**
  A smartcard can tell how it is being used, and can thereby automatically detect abuse. For instance, a Chip-and-PIN card can monitor transactions against the daily limit, and block additional purchases if the limit is exceeded. Similarly, if a health smartcard had to be presented when a GP issues a prescription, it could automatically detect unusual repeat transactions suggestive of "prescription shopping". Card abuse could be detected without having to data-mine all innocent prescription data.
- **Transaction signing**
  To prevent ID Theft and replay of credentials with fraudulent transactions, a smartcard can automatically digitally sign each transaction, using an embedded private key, to render it unique. A card can hold multiple keys, each dedicated to a different family of transactions. For instance, one health & welfare smartcard could be loaded at the owner's discretion with respective private keys for a longitudinal electronic health record and any number of private sector record services.

Copyright © 2008 Lockstep Technologies Pty Ltd

A smart proxy for the user

In practice, we use different digital identities (account numbers, user names, pseudonyms and handles) for different online services. Smartcards (and their cryptographic kin, the USB key and SIM card) can hold all of a user's digital identities, and can present the appropriate identity for the service being accessed.



To stop ID theft

To stop digital identity theft, we must prevent the replay of credentials and the coupling of stolen credentials to new fraudulent transactions. Digital signatures offer the most robust protection against replay and fraud. A smartcard card can automatically check the context and select the appropriate embedded private key and digital certificate to sign the transaction.

Copyright © 2008 Lockstep Technologies Pty Ltd

Smartcard, not Id Card

Smartcards are not necessarily ID cards. To avoid a new health smartcard morping into an ID card, we should enforce the following characteristics:

- Opt in
- Dedicated to health
- No arbitrary new identification
- No new identifiers
- Preserve plurality of existing identifiers
- Create user centred utility

Discussion

www.lockstep.com.au

anthill SMART 100

finextra certified innovator 2009

2008 - Asia GLOBAL SECURITY CHALLENGE Top-5 Security Start-Up

Featured in the Australian Technology Showcase

Secrets of Australian IT Innovation WINNER 2006

Copyright © 2008 Lockstep Technologies Pty Ltd