Lockstep Babysteps No. 2

A fresh look at smartcards

Smartcards are feared at large as potential instruments for surveillance by the state and therefore thought to be an almost automatic threat to privacy. Many are anxious that the smartcard's chip will surreptitiously monitor user behaviour and enable authorities to make linkages across databases. Multiple usage is widely regarded with suspicion.

But a fresh alternative view recognises that smartcards bring a unique bundle of capabilities to protect and empower consumers:

— resistance to skimming and counterfeiting

— proving the true identity of online services, to combat phishing, pharming and web fraud

— intelligence to release cardholder data only to legitimate and verified systems

— encrypting not just one but multiple, diverse identifiers, to quarantine backend systems.

Smartcards can therefore radically enhance privacy and security at the same time.

What's really so special about smartcards?

The headline issue around smartcards in most peoples' minds seems to be their ability to store 'large' amounts of data, and to track cardholder behaviour. Smartcard memories are in fact puny; no commercial card today can save more than a few kilobytes, so amassing personal data is not practical.

In contrast, the embedded microcomputer and security module in modern smartcards provides a raft of unique capabilities:

- For all practical purposes**, a smartcard cannot be skimmed, cloned or counterfeited**. Security codes secreted in the chip mean that even if a smartcard is lost *together with its PIN*, the worst that can happen is misuse of that one card; thieves cannot use it to spawn bogus cards.
- Smartcards act as **keys to online services**. Rather than hold personal information, the chip can carry *security codes* to access computer systems.
- **Multiple keys for multiple services** can be managed on the one smartcard, helping to decentralise backend databases and keep them separate. Users retain control of the keys at all times, empowering them, and protecting privacy.
- Smartcards can safeguard the "master codes" for SSL-authenticated web sites. The chip is smart enough to verify each web site before connection for **genuine "mutual authentication", preventing spoofing, phishing and pharming**.
  In fact smartcards are recognised by the US Government as the only practical solution to "Man-in-the-Middle" Internet attacks, and are being adopted for remote logon by federal employees.
- Their intelligence allows **tighter control over the release of sensitive cardholder data**, only to mutually authenticated services.
- Smartcards can **autonomously tally pre-defined transactions and enforce daily transaction caps without ever going online** to backend mainframes. Thus, lost & stolen smart credit cards are much safer against misuse; smart health cards can readily detect and flag doctor shopping and other fraud.
- By undertaking fraud detection within the chip and offline, smartcards **dramatically reduce the volume of sensitive personal data** transmitted across public networks.
- Smartcards can **encrypt personal identifiers** to render them meaningless outside the context of the card, preventing reverse identification of card holders from their transaction records.

What should we be doing with smartcards?

Years ago promoters of smartcards focused on multi-functionality; it was said that combining payments with stored value, calling card, ticketing & tolling and loyalty could be compelling, yet bringing these complex products to market proved almost impossible. But a more powerful vision is now clear, driven by today's security and privacy imperatives, and flexible enough to integrate with diverse backend systems with far less re-design and project management risk.

It's time to re-think what smartcards are for. Most importantly, they should become the **preferred means to control access to sensitive online services**. Phishing, pharming and Man-in-the-Middle attack mean internet banking, e-health records, e-voting and the like cannot be protected by one-way authentication alone (including most of the two factor security devices on the market today). Smartcards also provide **secure containers for multiple electronic identities**. By encrypting identifiers, a smartcard issued by one organisation can be 'topped up' with extra security codes and used safely to access services in other online communities, without cross-talk or information leakage between backend systems.

Fundamentally, smartcards can be regarded as **intelligent proxies for their owners**. The card can automatically enforce security rules to protect against loss & theft, decentralise personal information stores, and actively verify the legitimacy of every single party the card holder ever has to deal with.