Information Security: Safe, Easy, and Controllable? An R&D challenge

Stefek.Zaba@hp.com

A different view of usability: "What are They doing next?"

- How does an ordinary user assess trustworthiness?
  - some principles
  - three examples
  - a few anecdotes
  - perhaps a conclusion!

Cryptography is hard…

- Cryptography is hard to get right
  - failure in confidentiality is silent
  - failure in authorisation may be effectively silent
    - successful impersonation raises no alarms
  - failure in availability isn't silent
    - but may look like "normal" unreliability!

… and security is harder

- Protocols are hard
  - even though every engineer can dream them up easily
- Implementation and administrative practice are hardest of all
  - The overwhelming majority of attacks are directed here, not at cryptography or protocols

So how do I know it's OK?

- The "ordinary user" must rely on something beyond personal verification of the entire process
  - infeasible effort would be needed
  - specialist skills needed
  - vulnerabilities may be harder to address if they become suddenly widely known
  - sensible users DON'T CARE (much)

Possible “somethings”

- Coercion: “this is how it’s done”
  - state, monopoly supplier, employer, …
- Alignment of interests: “they want what I want”
  - or enforced (partial) alignment by regulation
- “Neutral” expert assessments
  - consumer champions, Common Criteria, standards, …

We'd better hope…

- … that the goals of these "proxies" for the user's interests are more or less aligned with the user's goals
- … that system designers don't just sing the "mechanism, not policy" song, which leaves a hundred low-level controls in the hands of the astonished users

How does it work in practice?

- Three interesting cases:
  - “Chip and PIN” payment cards
  - RFID
  - Trusted Computing

Chip and PIN payment cards

- Shared-secret short number replaces physical signature at point of sale
- Only “new” in the UK!
- Truly widespread deployment
- Lots of Customer Service experience
- Established technical standard
  - cautious crypto, security practices
  - whole-system operating guidelines

Chip-and-PIN: user proxies

- "Coercion": specifications enforced by payment operators (VISA, MC, …)
- "Alignment of interests":
  - banks, acquirers want satisfied consumers and retailers
  - consumer credit regulations apply
- "Neutral" experts established
  - consumer organisations, technical critics… and open literature on smartcard penetration!
- Presence of all three suggests success…

RFID

- Already established in supply-chain logistics
- Announcements of widespread planned use for individual retail items
- Some pilot trials at retail level
- Wide variety of technologies
  - differing capacity, “smartness”, reading range, cost…

RFID: user proxies

- Coercion: major supply-chain controllers demanding RFID from suppliers
  - but at “big box” level, not individual item
- Alignment of interests: logistics OK…
  - …but consumers NOT: price reductions? warranty/service improvements? no receipts to lose? “smart” goods?
  - seem to be marginal benefits and unknown risks

RFID: user proxies, continued

- Regulation for alignment of interests
  - few specific measures so far
  - but Data Protection principles clearly apply
- "Neutral" experts
  - technical standards established
  - mass use coming under active dispute
    - little "neutrality" so far: technical enthusiasts versus "prophets of doom"
    - much confusion over goals and practicalities
- Uptake not yet established

Trusted Computing

- Industry initiative to make common computers (PCs, …) less “wide-open”, at minimal (hardware) cost
- Proposals:
  - TCPA / TCG
  - Palladium / NGSCB
  - LeGrande
- Initial products now available
  - clearly aimed at corporate, not consumer

TC: proxies?

- Coercion: not that I can see
  - industry consortium reacting to (corporate) customer needs
  - visible caution in approaching consumer marketplace
  - but there is fear of possible future actions by dominant market participants

TC: proxies?

- Alignment of interests
  - in place for corporate deployments
    - "owner" versus "user" distinction
    - administrators exist who can adapt the raw mechanisms to their own policy
    - expected usage in line with legal position
  - less clear for "home", "ISP customer" usage
    - protected-storage, integrity-measurement have useful benefits here
    - remote "attestation" is contentious

TC: proxies?

- Regulatory assistance in alignment of interests:
  - Data protection principles clearly apply
  - EU and European national governments taking a keen interest
  - Competition authorities also interested

TC: proxies?

- "Neutral" experts:
  - Neutrality seems to be in short supply…
  - 200-member organisations are not very nimble
  - Previous record of key participants may give rise to cynicism
  - Some recent developments, e.g. Open-Source utilities, show movement towards transparency
- Universal adoption far from assured

Some conclusions

- Of the three mechanisms, “alignment of interests” seems to be the most adaptive
- Neutrality may be a myth; in any case it needs to be carefully assessed
  - (or coerced, aligned, or neutrally assured!?)
- “Profiles” to balance flexibility against usability?
- Usability concerns of coercers, aligners, and assessors may not be those of the users either!