Opportunities in NGSCB for NZ Software Producers

Presentation to the NZ Information Security Forum

Prof. Clark Thomborson
Computer Science Department
12th August, 2004
NGSCB: Evolutionary Feature 1

- OS will support “signed and sealed” messages using public key cryptography.
  - Similar crypto-primitives are available in Java and .NET
  - This will improve interoperability and make integration easier.
NGSCB: Evolutionary Feature 2

- Can build “firewalls” between applications running on the same computer.
  - Isolation will make integration more difficult!
    - Windows: “Permit, until it’s necessary to prohibit”
    - High-security: “Prohibit, unless it’s necessary to permit”
  - High-security apps don’t belong on a shared Wintel box, even with NGSCB support.
NGSCB: Revolutionary Features

- Some NGSCB features have never before been available in a mass-produced desktop computer.
- Sealed Storage (from TCP)
  - Your PC can be used to store and manipulate other people’s secrets.
    - The contents of a sealed message might not be readable by any user-level process on the destination PC.
  - Your OS can’t read its own sealed storage unless it is booted into a “trusted” state.
    - Root keys are held in a hardware device that monitors the boot process.
NGSCB: Revolutionary Features

- **Attestation from a hardware kernel**
  - Your PC can “attest” to the validity of the messages it sends.
  - Your PC won’t create a valid attestation unless its OS is booted into a secure state.

- **Secure Paths (c.f. SCTC’s LOCK)**
  - Information flows along “secure paths” between applications, DLLs, and devices.
  - An application can get some security assurances about a path before it sends any information.
What's the benefit for NZ?

- NZ software producers can adjust their development plans, to take advantage of these (likely) developments.

- I think NGSCB’s killer app will be marketed to corporates, not to private individuals.
  - A corporate PC is administered by its owner, not by its user.
  - Corporate users don’t (shouldn’t!) expect to “own” everything on the PCs that they use.
  - Private users do not, as yet, feel a need to trust someone else’s computer.
  - Identification (and accountability) of the “person in charge” of a PC is still problematic, except in a corporate setting.
Sales Pitch: Private Individuals

- More security against hostile apps
  - Additional assurance: if PC can boot into secure state, then it is almost surely safe to use it for internet shopping and banking?
  - Users must be trained to recognise the look and feel of the secure console window.
    - Does your smart card trust your PC?
- End-user security assurance could be a profitable niche market for NZ software developers
- Access to a wider range of copyright media
  - I imagine Microsoft are working on this…
Corporate Uses of NGSCB

- NZ software products could support secure inter-corporate workflows
  - Document transfer (orders, invoices, receipts)
  - Secure paths that affect another corporation’s workflow, payroll, a/r, a/p, warehousing, stocking, manufacturing, personnel, …
  - Secure paths to e-government systems (local and foreign)
- Current-generation “enterprise software” will morph into next-generation “sector systems”
  - Sectors with small businesses
“Free Advice”

- Don’t try to build an enterprise system out of number-8 wire.
  - Cost-effective security, not milspec, not Fortune-500
- Do “productise” (and market!) your number-8 widgets for secure intercorporate communications
- Do seek patent protection in all key markets.
  - New Zealand is producing some excellent patent attorneys – let’s keep them here!
Please contact me…

- Google for “Thomborson”
- Your tax dollars ➔ my research programme
  - Help NZ software developers decide whether or not (and how!) to design new products using trusted PCs
  - Develop new technology in software protection
- Protocol
  - Initial contact: confidential, no cost to you
    - I’ll want permission to report the contact to NZ’s Foundation for Research Science and Technology
  - Publishable case studies: no cost to you
  - Product development: Auckland UniServices incubator with “seed capital” grant from government