NGSCB
A New Tool for Securing Applications

Presentation to the NZ Information Security Forum

Matt Barrett

12th August, 2004

Overview

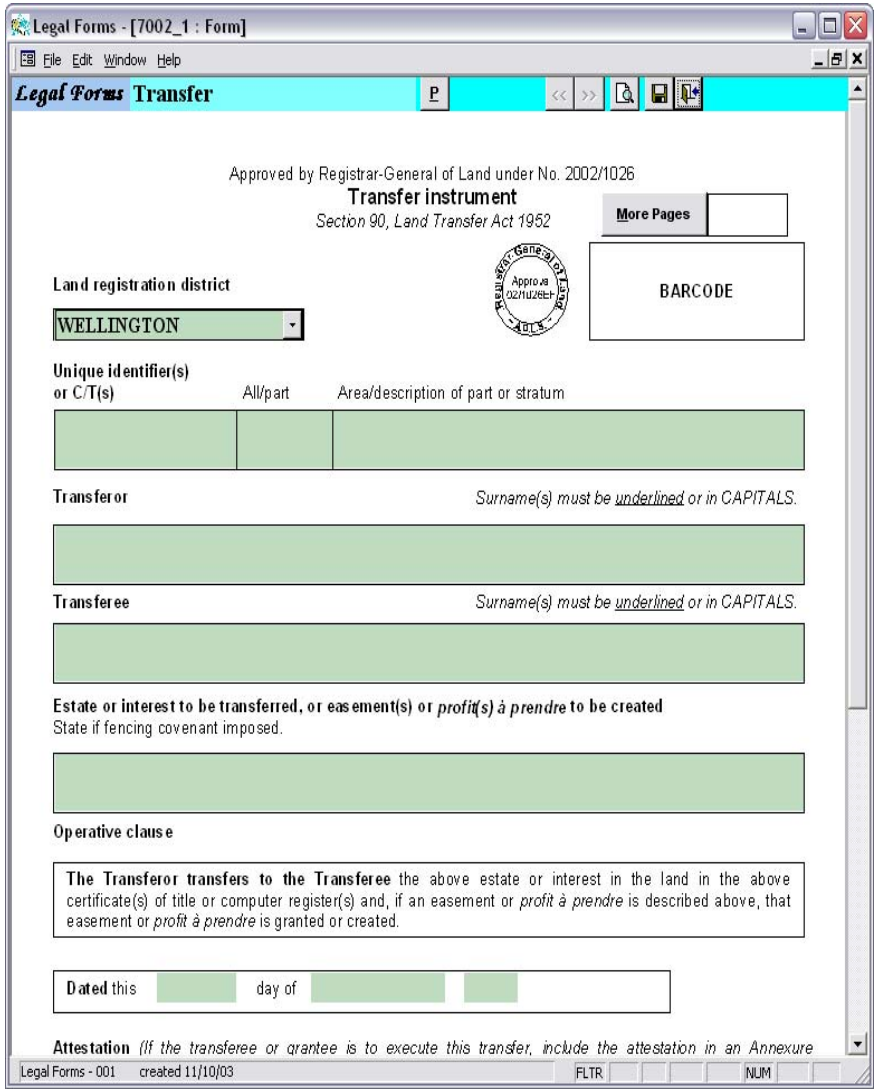
- Auckland District Law Society (ADLS)
  - Electronic Legal Forms (ELF)
- Next-Generation Secure Computing Base (NGSCB)
- Case study on integration of the two
- Technical merits of NGSCB
  - Does it make a strong business case?
  - What security gains can we make?

Auckland District Law Society

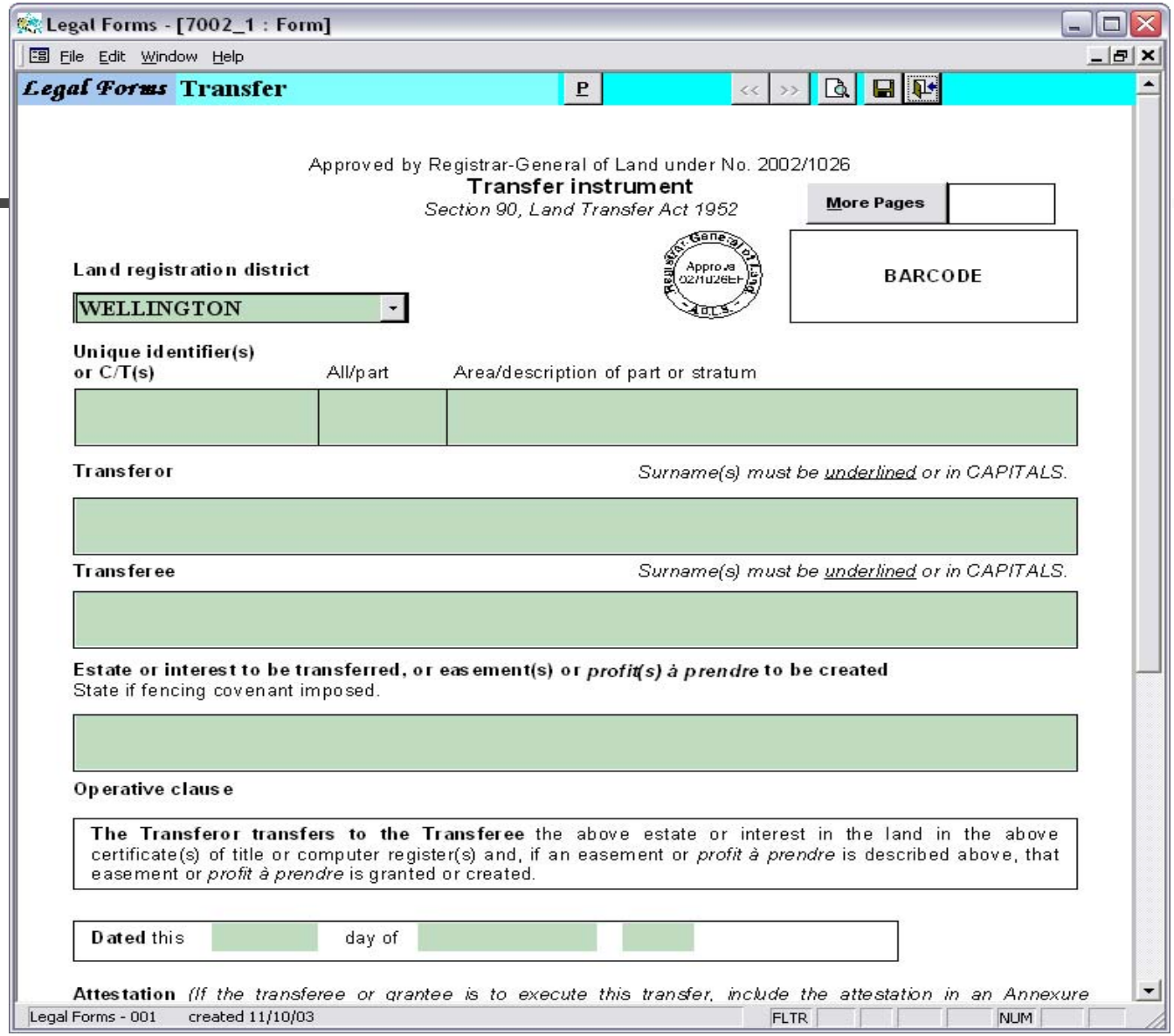
- Auckland District Law Society
  - Currently a non-profit society
  - Deregulation in about 18 months
  - Own the copyright on a number of legal documents
  - ‘Customers’ are lawyers, and indirectly their clients

Electronic Legal Forms

- Approached ADLS after working with ELF
- Business usage of ELF
- WYSIWYG legal form editing
- Users are lawyers
- Forms cost between 75¢ and $2.50
- Simple collaboration features built-in



The University of Auckland



Base Form + Concatenated String = Legal Document

Electronic Legal Forms

- Ideal ADLS Goals
  - Usability
    - The finalised form can be viewed conveniently, by lawyers and their clients
  - Integrity
    - “...a particular word of a particular clause will always appear in the same place on the same page...”
  - Confidentiality
    - No unauthorised viewing of legal forms.
  - Revenue
    - No unpaid reproduction of hard copies.

Electronic Legal Forms

- Requests for an electronic document
- Portable Document Format - PDF
  - The use of PDF to improve availability is acknowledged by the ADLS
    - *August 2003* newsletter
  - But strongly deprecated
- This misuse leads to the opening of an abuse frame
  - Integrity, revenue, and confidentiality attacks are possible against a document in PDF

Electronic Legal Forms

- Security Issues - *Integrity*
  - PDF - an *open* format
  - A number of cracks are available
  - PDF documents are created by remote authors using tools outside the control of ADLS
  - PDF documents may be modified by third parties
  - All ELF-produced documents should be trustworthy, not just those from authors who know how to protect their PDF.

Electronic Legal Forms

- Security Issues - *Revenue*
  - ADLS collects revenue from final prints of legal documents - a few dollars a print
    - Once a form is printed to PDF, it can be printed and distributed without restriction
    - This applies to any file format
- *Confidentiality*
  - PDF can be forwarded to, and read easily by, anyone.
  - ELF document descriptors are read easily by people with ELF software, but are difficult for others to read.

Possible Solutions

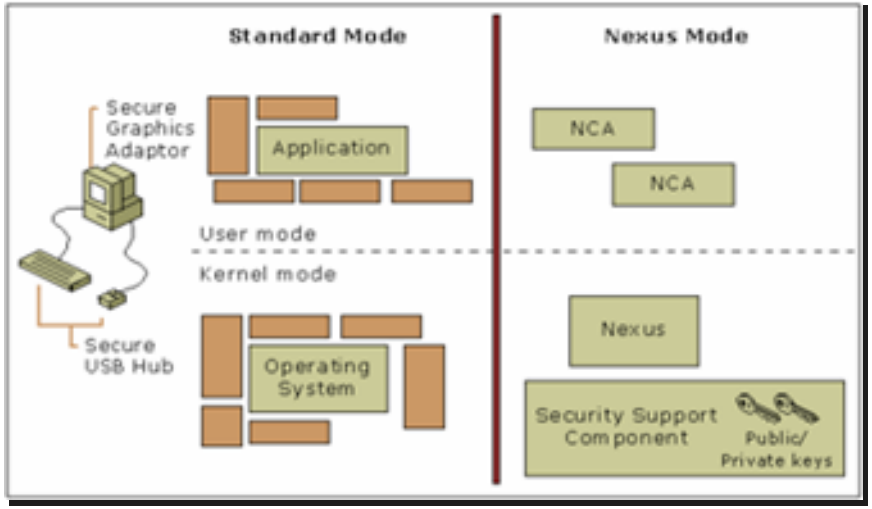
- Adobe's authoring tools allow restrictions to be set by the final author
  - Careless authors / inappropriate restrictions
  - Revenue attacks: change default restrictions
- Authentica *Pagerecall*, 2003
  - Supports distributed authoring of PDF document, but similar abuse frames to Adobe's authoring tools
  - Supports metered printing, but requires management by a central server (infeasible/unacceptable for ADLS)

Next-Gen Secure Computing Base

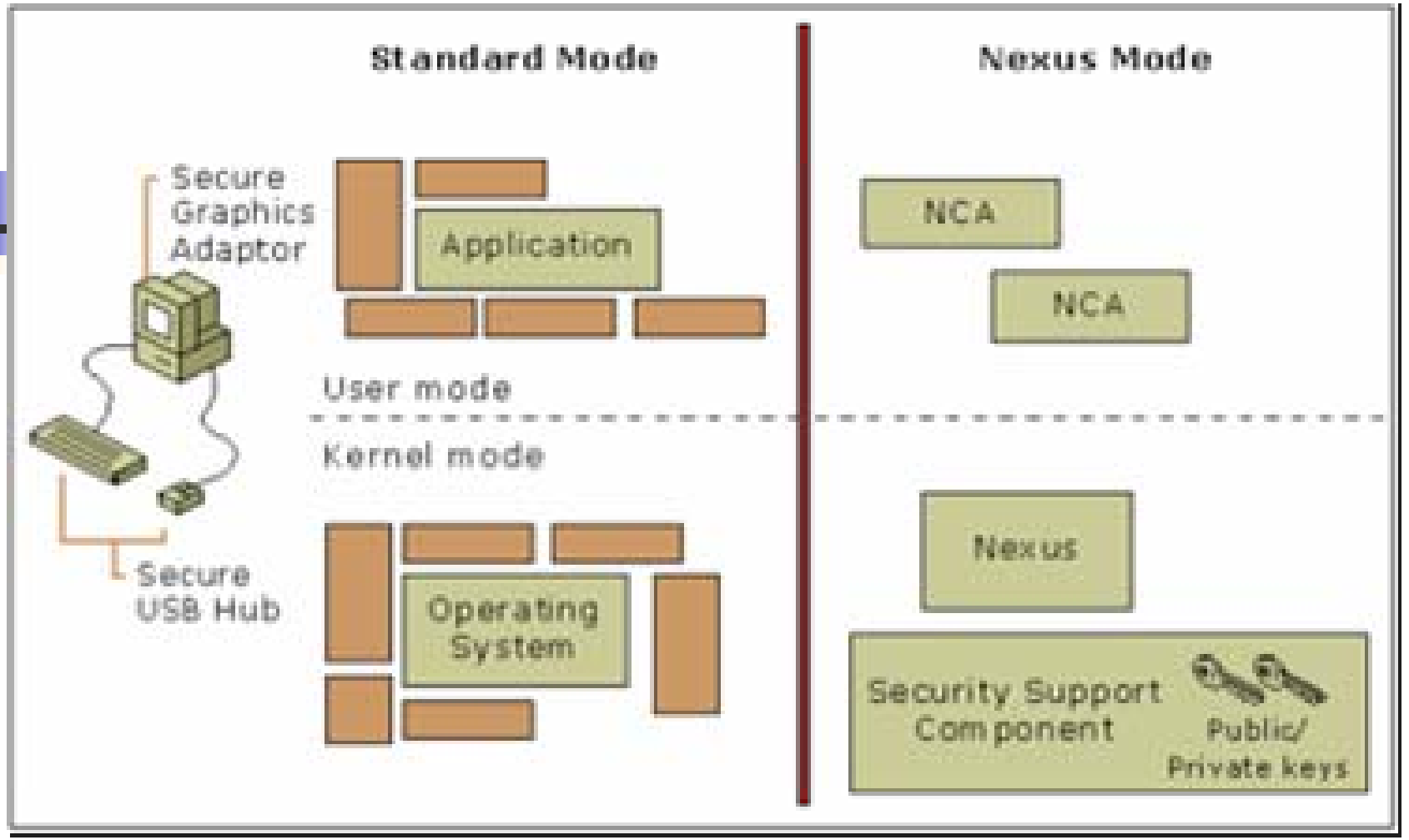
- Roll our own solution with NGSCB
  - Attempt an integration of the two products
    - Minimize re-implementation
    - Maximize ease of use
  - NGSCB as a *tool-box*
    - Use the primitives provided to solve existing security vulnerabilities
    - Don’t try and build new features

OS Changes - Software

- NGSCB will ship with Microsoft's Longhorn
  - Next major OS release
  - Final feature set is yet to be determined
  - Insecure, untrusted *Left Hand Side* and a secure, trusted *Right Hand Side*



The University of Auckland



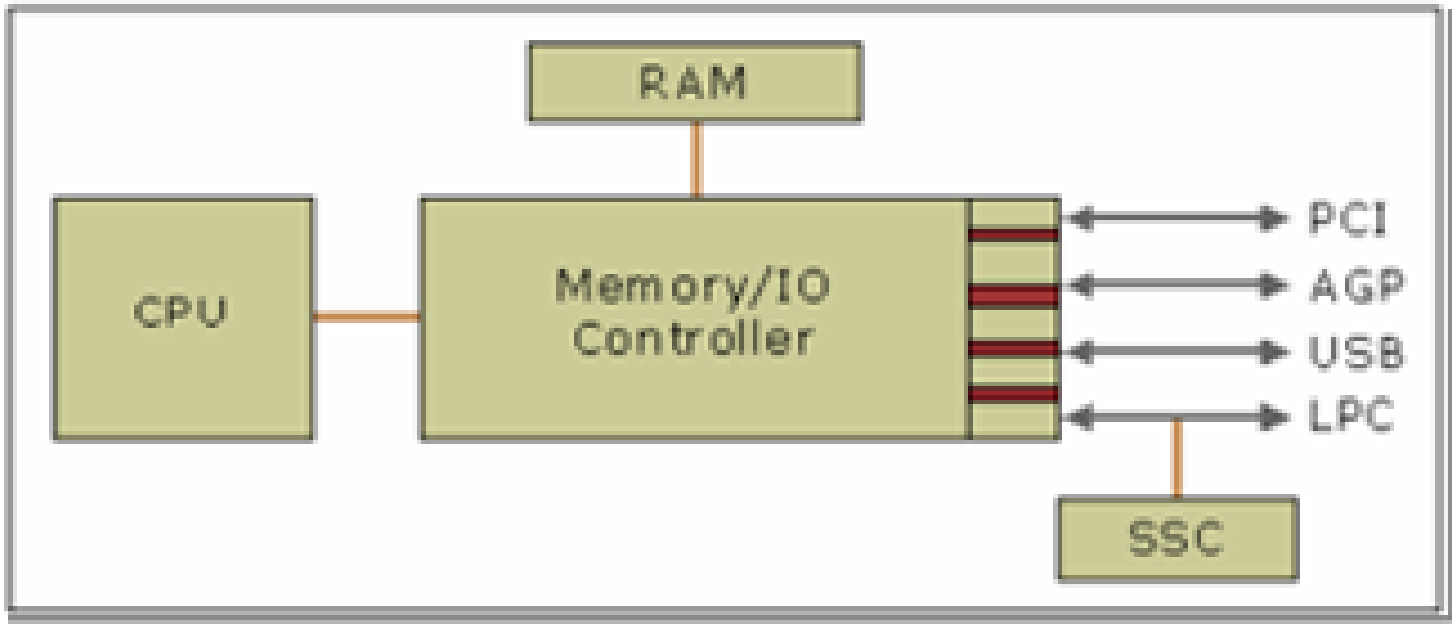
Left Hand Side *Right Hand Side*

- Nexus Computing Agents (NCA)

- Nexus will rely on LHS for majority of services - DoS?

Platform Changes - Hardware

- You will need to buy new hardware
  - Motherboards, videos cards, keyboards and mice all may need to change
  - Security Support Component (SSC)
  - Trusted Platform Module (TPM)



Four New Security Primitives

- Strong Process Isolation
  - Derived from virtual memory protection
- Sealed Storage
  - …file systems with mandatory access control lists (ACL)
- Attestation
  - …signed executables
- Secure Paths
  - …root prompt, screen scraping prevention

Strong Process Isolation

- Keeping applications protected
  - RHS memory space is protected at the hardware level from the LHS
    - *Curtained Memory* is effectively invisible to applications running in non-curtained address space.
    - Marked by an extra addressing-mode bit
  - The Nexus also enforces memory separation between NCAs
    - However, this isn't done in hardware

…Strong Process Isolation

- Non-Execute Hardware modifications
  - Hardware modifications also include Non-Execute, or NX, flag
  - X86 architecture gets something for nothing here - a hardware enforced differentiation of code and data. No more buffer overflows?
    - Unix architectures have had this for a long time
    - Already present in Windows XP SP2

Sealed Storage

- Program-based access control
  - *Code Identity:* a cryptographic hash based on the *manifest* describing the NCA
- Who owns and controls your data?
  - A *sealed* file cannot be *unsealed* except by the same application that *sealed* it, and on the same machine
    - The ultimate data lock-in!
  - You can debug an NCA
    - With some caveats

Attestation

- Foundations
  - Allows the security boundary to extend from an NCA running locally, to include that of an NCA running remotely.
  - Policy projection from one computer to another can occur.
  - Makes use of code identity to strongly identify program binaries, and ensure they have not been modified

Attestation

- Hierarchy
  - SSC verifies Nexus
  - Nexus verifies Nexus Computing Agent

- Trust is *rooted* in the hardware chip
  - Trust is optional
  - Operational enforcement is not optional

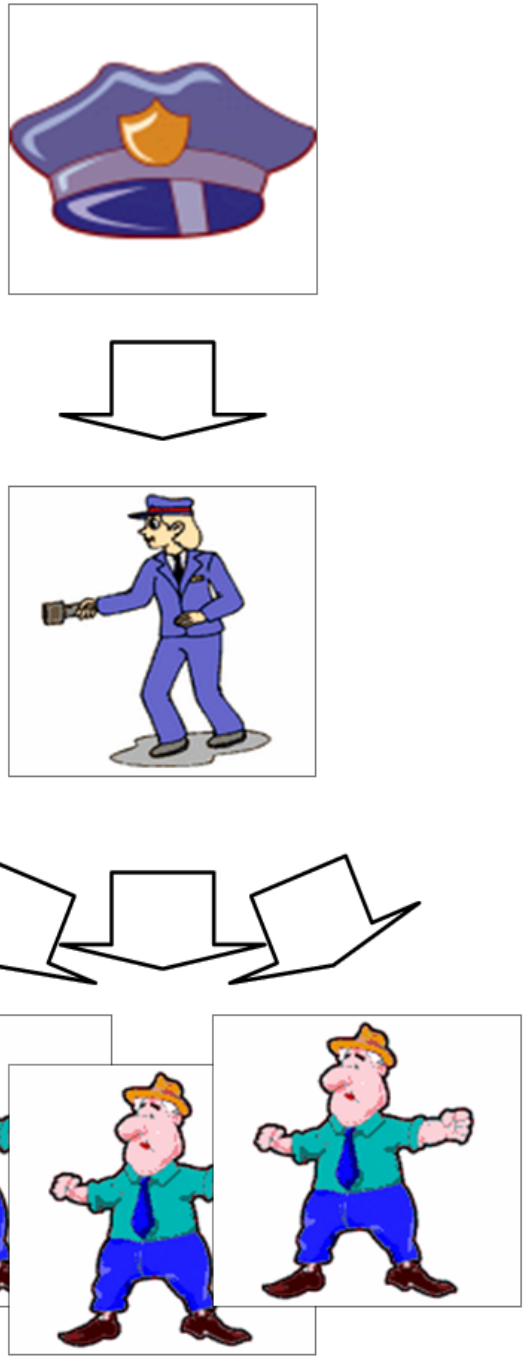
Attestation

- Police Officer
  - Is fixed in hardware
  - States identity of..
- Security Guard

  - States identity of..
- Citizens

Attestation

- NGSCB developers
  - Claim it sends the wrong message to users
  - Would prefer to say i is the LTSA
- It is difficult to obtain a universal metaphor



Secure Paths

- Who are we talking to?
  - Starts with a secure graphics adaptor, keyboard and mouse
    - Secure means each device is cryptographically enhanced, and all input/output is signed
  - Provides protection from…
    - Screen scraping
    - Local man-in-the-middle attacks
    - User input spoofing
- Other manufacturers are expected to release printers, speakers, etc

NGSCB

- How open will it be?
  - Open-source code review
  - Can others write their own nexus?
  - Microsoft's code review process
  - Nexus is small
    - Easy to maintain, find bugs
    - Aware of distrust in closed source system, and wish to prove them wrong
- How open can it be?
  - Researching an open, trusted computing platform

Electronic Legal Forms

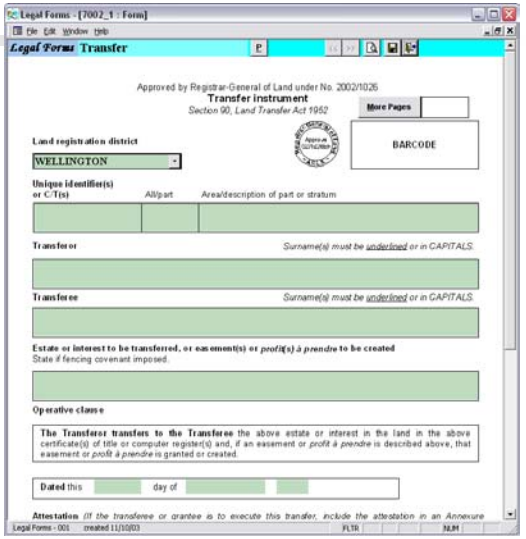
- Problem
  - Usability
  - Integrity
  - Confidentiality
  - Revenue

- Roll our own solution with NGSCB
  - Attempt an integration of the two products
  - Use NGSCB as a tool-box

Electronic Legal Forms

- Integrity
  - Solved through cryptography
  - Need to design a framework so that individuals are able to communicate securely
- Public Key Infrastructure
  - We can control enrolment into the scheme
  - Requires a new server
  - Installation procedure at user's site now includes generation of asymmetric key pair, and registration with this server
- Integrate into the ELF workflow
  - *Address* the legal form to its intended recipients before it is sent
- This gives us confidentiality and integrity between users of ELF

Electronic Legal Forms



- Move away from PDF
  - Create a light-weight document viewer
    - Re-use code from ELF application
- This is the correct, intended use of NGSCB
  - Write small, secure components
- Write our own NCA
  - Displays the legal form, but does not allow editing
  - This small executable would be distributed by the law firm to its clients, before a legal form is sent
- Establish a trust relationship between a law firm and its clients, to enable one-way information flow

Electronic Legal Forms

- Revenue
  - Restrict printing
    - We can completely remove the ability to print from within our NCA viewer
  - NGSCB allows us to do better than this
    - When a legal form is addressed to a client, the lawyer can attached a number of print credits
    - ADLS debits the law firm for these prints
- This is an excellent use of attestation, to extend the security boundary to include that of the NCA viewer. We can project printing policy onto the remote computer.
  - If a user can print from the NCA viewer, the abuse frame opens up

Electronic Legal Forms

- Revenue
  - When a legal form is addressed to a client, the lawyer can attached a number of print credits
- Replay Attacks
  - Storing the print credits with the form would allow a user to exhaust their credits, then replace the form with the original
  - NGSCB does not give us secure persistent storage
    - Relies on insecure LHS for persistent storage
  - We could engage in an arms race

Electronic Legal Forms

- Revenue
  - NGSCB does not give us secure persistent storage
- NGSCB development team
  - Aware of this issue
  - Conceive of an NGSCB registry
- Trusted Computing in general
  - Requires a trusted monotonic counter
  - Trusted mass storage
  - Trusted peripherals
    - In our case, printers!

Electronic Legal Forms

- Usability
  - Gaining strong confidentiality and integrity requires some investment of time
    - Need to setup trust relationships, both two- and one-way.
  - Viewing a form is no longer a one-step process
    - Of course, NGSCB is required on all platforms.
- All security is a compromise
  - Confidentiality, integrity and availability

Electronic Legal Forms

- User acceptance
  - Integrate the process into the workflow
    - Discourage use of PDF as much as possible, and shrink abuse frame
    - As simple as a *Send form to…* icon
- Confidentiality relies on the user
  - NGSCB binds data to a specific platform

Electronic Legal Forms

- Recap
  - Satisfying our goals
    - Confidentiality
    - Integrity
    - Revenue
    - Usability
  - But it is *very* difficult to plug all the gaps
    - No secure printing capability
    - Replay attacks
    - In the end, security depends on a social issue: trust in individual users

Electronic Legal Forms

- NGSCB assessment
  - Does it make good business sense to use?
    - A large security ‘hammer’
    - Final product may be lighter, and easier to use
  - A (vague) technology prediction
    - Trusted Computing will find its way into corporate desktops
- Alternate designs
  - Intertrust Docbox, in Acrobat 5.0 (2001)
    - Enforces DRM (circumvented by Skylarov and others)
    - Unsupported / discontinued, 2004
  - Integrate with Adobe Acrobat
    - Rely on a hardware dongle with plug-in
    - Wait until Adobe integrates with NGSCB

References

- Microsoft NGSCB Webpage
  - http://www.microsoft.com/ngscb/
- TCPA FAQ, Ross Anderson, 2003
  - http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html
- Trusted Computing Group
  - https://www.trustedcomputinggroup.org/home
- Auckland District Law Society
  - http://www.adls.org.nz/
  - http://www.adls.org.nz/shop/elf.asp
- How Secure is PDF?, Bryan Guignard, 2001
  - http://www.cs.cmu.edu/~dst/Adobe/Gallery/PDFsecurity.pdf

- Images taken from *NGSCB Technical Whitepapers,* published by *Microsoft,* http://www.microsoft.com/resources/ngscb/archive.mspx