

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



- 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

e <u>E</u> dit <u>W</u> indow <u>H</u> elp				
A CONTRACTOR OF A CONTRACTOR O				
d Forms Transfer		P	<< 2	» 🖪 🖬 📭
Land registration distri WELLINGTON	Approved by R Si ct	Registrar-General o Transfer ins ection 90, Land Tré	Land under No. 200 trument Insfer Act 1952	12/1026 More Pages BARCODE
Unique identifier(s) or C/T(s)	All/part	Area/description	of part or stratum	
Transferor		1	Surname(s) mus	t be <u>underlined</u> or in CAPITALS.
Transferee			Surname(s) mus	t be <u>underlined</u> or in CAPITALS.
Transferee Estate or interest to be State if fencing covenant Operative clause The Transferor trans	transferred, or imposed. fers to the Tr	easement(s) or <i>pr</i>	Surname(s) mus ofit(s) à prendre to	t be <u>underlined</u> or in CAPITALS. be created est in the land in the above
Transferee Estate or interest to be State if fencing covenant Operative clause The Transferor trans certificate(s) of title or easement or <i>profit à pri</i>	transferred, or imposed. fers to the Tr computer registe endre is granted	easement(s) or pr ransferee the abc er(s) and, if an eas or created.	Surname(s) mus ofit(s) à prendre to ve estate or inter ement or <i>profit à pr</i>	t be <u>underlined</u> or in CAPITALS. be created est in the land in the above <i>endre</i> is described above, that
Transferee Estate or interest to be State if fencing covenant	transferred, or imposed.	easement(s) or pr	Surname(s) mus ofit(s) à prendre to	t be <u>underlined</u> or in CAPITALS. be created



The University of Auckland

Carrie Tuonafon						
Transfer		P	<<	» 🖪 🖬 📭		
	Annroved by	Registrar-General (of Land under No. 20	02/1026		
	Transfer instrument					
	3	Section 90, Land Tr	ansfer Act 1952	More Pages		
			St. Gane.a	. 6		
Land registration district	t		Approve	BARCODE		
WELLINGTON	-		Sans?			
Unique identifier(s)						
or C/T(s)	All/part	Area/description	of part or stratum			
Transferor			Surname(s) mu	st be underlined or in CAPI.	TALS.	
					-	
Transferee			Surname(s) mu	st be <u>underlined</u> or in CAPI	TALS.	
			2.5			
Estate or interest to be to	ransferred, or	easement(s) or p	rofit(s) à prendre to	be created		
Estate or interest to be to State if fencing covenant in	ransferred, or mposed.	easement(s) or p	rofit(s) à prendre to) be created		
Estate or interest to be to State if fencing covenant in	ransferred, or mposed.	reasement(s) or p	rofit(s) à prendre to) be created		
Estate or interest to be to State if fencing covenant is	ransferred, or mposed.	r easement(s) or p	rofit(s) à prendre to) be created		
Estate or interest to be to State if fencing covenant in Operative clause	ransferred, or mposed.	easement(s) or p	rofit(s) à prendre to) be created		
Estate or interest to be to State if fencing covenant in Operative clause	ransferred, or mposed.	easement(s) or p	rofit(s) à prendre to	be created		
Estate or interest to be to State if fencing covenant in Operative clause The Transferor transf certificate(s) of title or c	ransferred, or mposed. ers to the T omputer regis	reasement(s) or p Fransferee the ab	rofit(s) à prendre to ove estate or inter sement or <i>profit à p</i>	be created est in the land in the al	bove that	
Estate or interest to be to State if fencing covenant in Operative clause The Transferor transf certificate(s) of title or c easement or <i>profit à pren</i>	ransferred, or mposed. ers to the T omputer regis o <i>dre</i> is granted	reasement(s) or p Fransferee the ab ter(s) and, if an ea d or created.	rofit(s) à prendre to ove estate or inter sement or <i>profit à p</i>	becreated est in the land in the al <i>rendre</i> is described above,	bove that	
Estate or interest to be to State if fencing covenant in Operative clause The Transferor transf certificate(s) of title or c easement or <i>profit à prei</i>	ransferred, or mposed. ers to the T omputer regis n <i>dre</i> is granted	reasement(s) or p Transferee the ab ter(s) and, if an ea d or created.	rofit(s) à prendre to ove estate or inter sement or <i>profit à p</i>	est in the land in the al	bove that	
Estate or interest to be to State if fencing covenant in Operative clause The Transferor transf certificate(s) of title or c easement or <i>profit à prei</i> Dated this	ransferred, or mposed. ers to the T omputer regis ndre is granted day of	Fransferee the ab ter(s) and, if an ea d or created.	rofit(s) à prendre to ove estate or inter sement or <i>profit à p</i>	• be created est in the land in the al <i>rendre</i> is described above,	bove that	
Estate or interest to be to State if fencing covenant in Operative clause The Transferor transf certificate(s) of title or c easement or <i>profit à pren</i> Dated this	ransferred, or mposed. ers to the T omputer regis n <i>dre</i> is granted day of	reasement(s) or p Fransferee the ab ter(s) and, if an ea d or created.	rofit(s) à prendre to ove estate or inter sement or <i>profit</i> à p	• be created est in the land in the al <i>rendre</i> is described above,	bove that	

Base Form + Concatenated String = Legal Document



The University

of Auckland

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.



The University of Auckland

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



- 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.



The University of Auckland

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)



The University of Auckland

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

The University of Auckland

 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





Left Hand Side

Right Hand Side

- Nexus Computing Agents (NCA)
- Nexus will rely on LHS for majority of services DoS?



The University

of Auckland

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



The University of Auckland

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



The University of Auckland

... 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

The University of Auckland

- 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

The University of Auckland

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

The University

- of Auckland Hierarchy
 - SSC verifies Nexus
 - Nexus verifies Nexus Computing Agent

Trust is rooted in the hardware chip

- Trust is optional
- Operational enforcement is not optional



University

of Auckland

Attestation

Police Officer

Is fixed in hardware

States identity of..Security Guard

States identity of..Citizens









The University of Auckland

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

The University of Auckland

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

The University of Auckland

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



The University of Auckland

- Problem
 - Usability
 - Integrity
 - Confidentiality
 - Revenue

Roll our own solution with NGSCB

- Attempt an integration of the two products
- Use NGSCB as a tool-box



- 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



The University of Auckland

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

f Forme Transfer	10	P		_
Transfer				
		anta a mar manana		
	Approved by	Registrar-General of Land under No. 20 Transfer instrument	02/1026	1
		Section 90, Land Transfer Act 1952	More Pages	
		Care a		
Land registration district		(and the first of	BARCODE	
WELLINGTON		Ante		
Inique identifier(s)				
or C/T(s)	All/part	Area/description of part or stratum		_
2				
fransfer or		Surname(s) mu	t be <u>underlined</u> or in CAPITAL	S
fransferee		Surname(ti) mu	t be <u>underlined</u> or in GAPITAL	S.
state or interest to be	transferred, o	r easement(s) er profit(s) à prendre te	be created	
State # fencing coven an	t imposed.			
				-
)perative clause				
Operative clause The Transferor tran	sfers to the	Transferee the above estate or inter	est in the land in the abov	
Operative clause The Transferor transcent from the transferor tran	isfers to the computer regi	Transferee the above estate or inter ster(s) and, if an easement or profit & p d or created	est in the land in the abov which is described above, this	e at
Deerative clause The Transferor tran certificate(s) of title or easement or profit à p	isfers to the r computer regi rendre is grante	Transferee the above estate or inter ster(s) and, if an easement or profit à p d or created.	est in the land in the abov which is described above, the	e at
Derative class e The Transferor tran certificate(s) of title of easement or profit & p Dated this	r computer regi rendre is grante	Transferee the above estate or inter ster(i) and, if an easement or profit à p d or created.	est in the land in the above, the	at
Operative classe The Transferor trat certificate(s) of title of easement or profit à p Dated this	esfers to the r computer regi rendre is grante day of	Transferee the above estate or inter- ster(s) and, if an easement or profit à p d or created.	est in the land in the abov endre is described above, the	e at
Operative classe The Transferor tran certificate(s) of title of easement or profit à p Dated this	esfers to the r computer register designs of deay of	Transferee the above estate or inter statut and, if an essement or profit à p d or created.	est in the land in the abov endre is described above, the	at



The University of Auckland

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



The Iniversity

Auckland

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



- 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!



The University

of Auckland

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



The University

Auckland

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



- 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



The University of Auckland

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

The University of Auckland

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