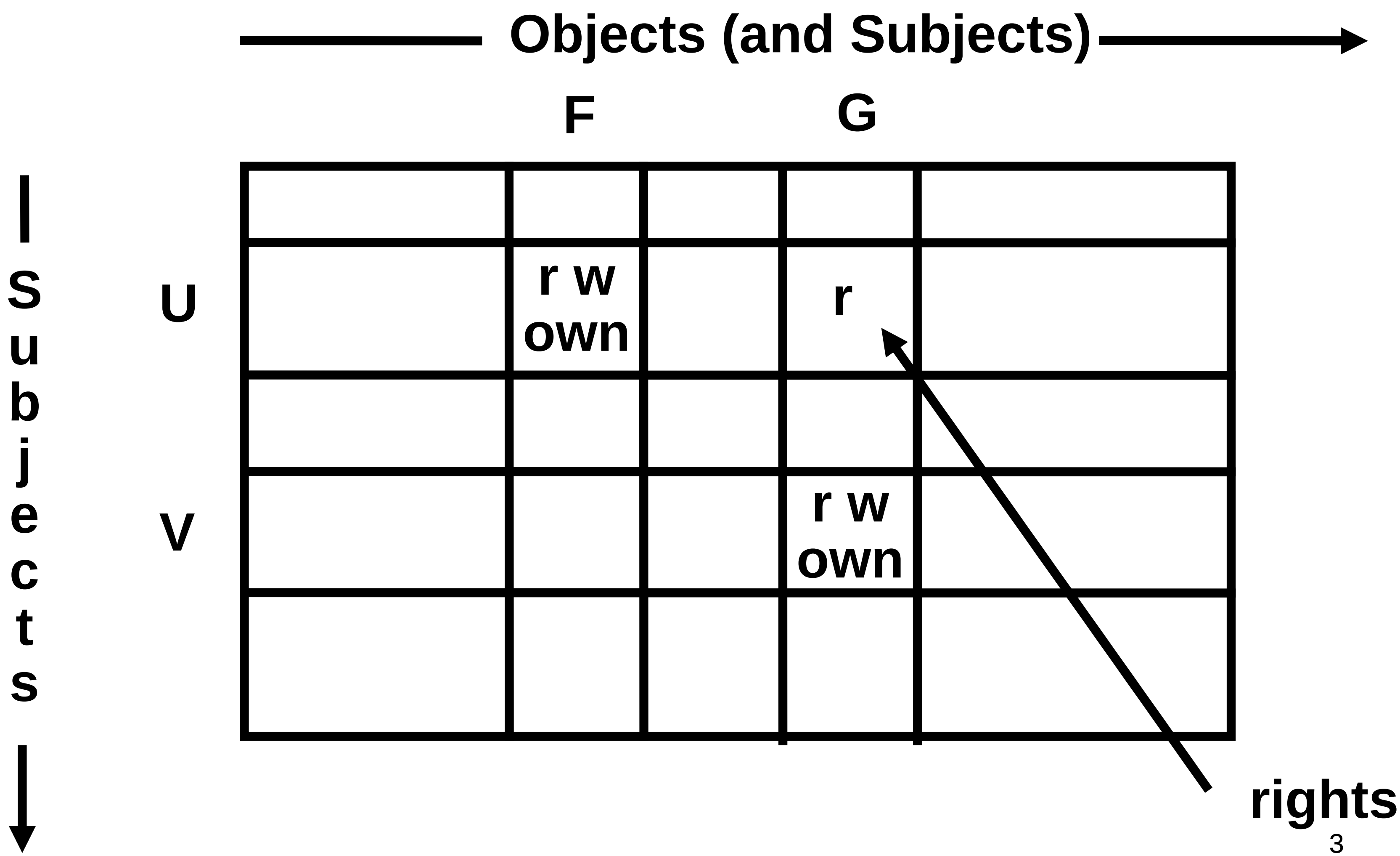
Information Assurance: A Personal Perspective

Ravi Sandhu
www.list.gmu.edu

Agenda

- Selected highlights from my 25+ years in this business (roughly chronological wrt start)
  - Typed Access Matrix (TAM) Model
  - Multilevel Relational (MLR) Model
  - Role-Based Access Control (RBAC)
  - Policy-Enforcement-Implementation (PEI) Layers
  - Usage Control (UCON) Model
  - TriCipher Authentication Ladder
- Selected ongoing research projects
  - Assured Information Sharing Enabled by Trusted Computing
- Perspective on the future of Information Assurance
- Q&A

Safety in Access Control:
Access Matrix Model (Lampson, 1971)



Safety in Access Control: HRU Model (1976)

command $\alpha(X_1, X_2, \ldots, X_k)$
  if r_1 in (X_{s_1}, X_{o_1}) and
    r_2 in (X_{s_2}, X_{o_2}) and
      $\ldots$
    r_m in (X_{s_m}, X_{o_m})
  then
    op_1
    op_2
    $\ldots$
    op_n
end

enter r **into** (X_s, X_o)
delete r **from** (X_s, X_o)
create subject X_s
create object X_o
destroy subject X_s
destroy object X_o

Theorem 1. Safety in HRU is undecidable

Theorem 2. Safety in monotonic mono-operational HRU is undecidable

Safety in Access Control: TAM Model (Sandhu, 1992)

command $\alpha(X_1 : t_1, X_2 : t_2, \ldots, X_k : t_k)$
  if r_1 in (X_{s_1}, X_{o_1}) and
    r_2 in (X_{s_2}, X_{o_2}) and
      . . .
    r_m in (X_{s_m}, X_{o_m})
  then
    op_1
    op_2
    . . .
    op_n
end

enter r **into** (X_s, X_o)
delete r **from** (X_s, X_o)
create subject X_s
create object X_o
destroy subject X_s
destroy object X_o

Theorem 1. Safety in TAM is undecidable

Theorem 2. Safety in monotonic acyclic ternary TAM is polynomially decidable

Safety in Access Control: From HRU to TAM

HRU (HRU 1976)

↓

Take-Grant (JLS 1978)

↓

SSR (Sandhu 1983)

↓

SPM (Sandhu 1988)

↓

ESPM (Ammann-Sandhu, 1990)

↓

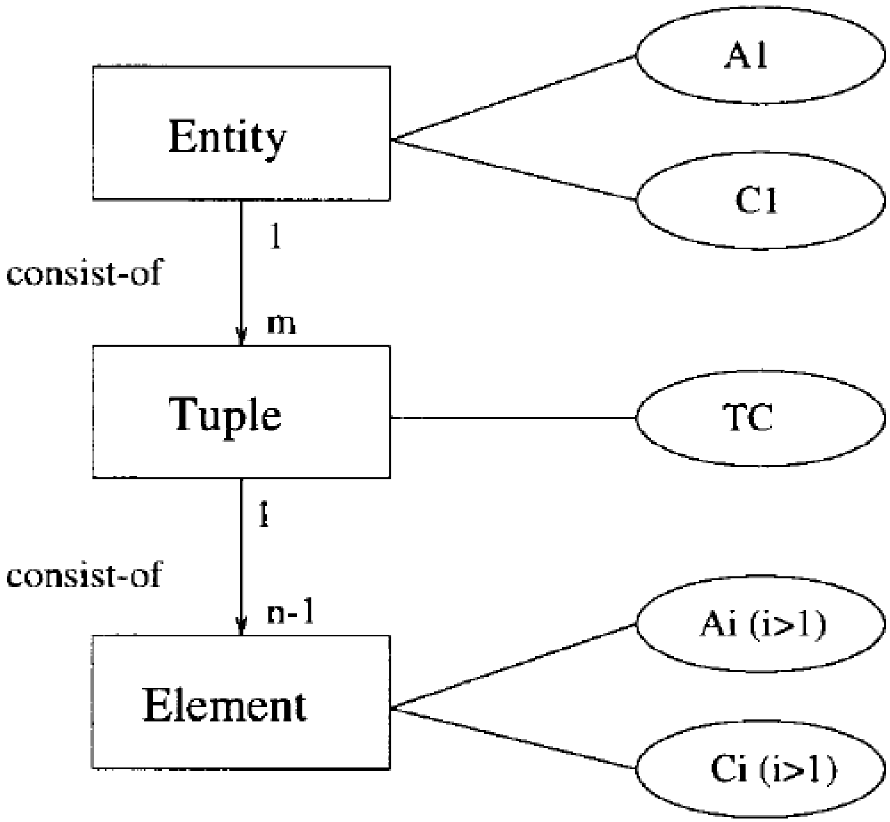
TAM (Sandhu, 1992)

The Multilevel Relational (MLR) Model: Taming Polyinstantiation (1998)

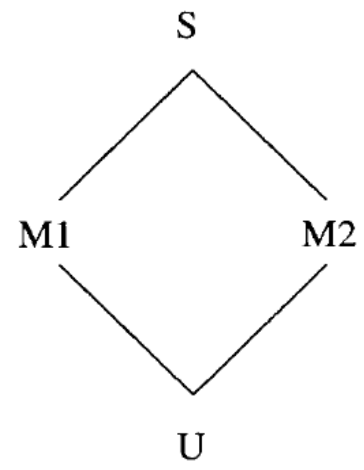
Enterprise	U	Exploration	U	Talos	U	U
Enterprise	U	Spying	S	Talos	U	S

Enterprise	U	Exploration	U	Talos	U	U
Enterprise	U	Spying	S	Talos	U	S
Enterprise	U	Exploration	U	Rigel	S	S
Enterprise	U	Spying	S	Rigel	S	S

The Multilevel Relational (MLR) Model: Taming Polyinstantiation (1998)

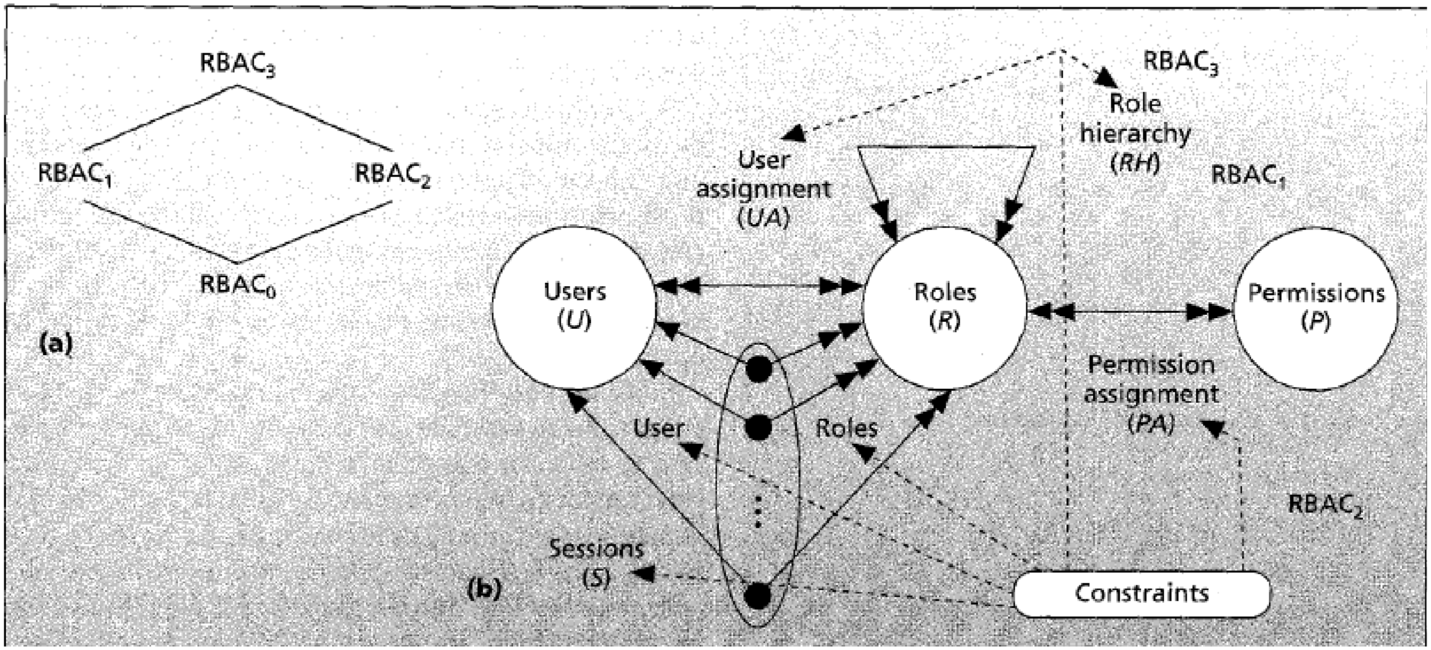


The Multilevel Relational (MLR) Model: Taming Polyinstantiation (1998)



SHIP		OBJ		DEST		TC
Enterprise	U	Mining	M_1	Sirius	M_2	S
Enterprise	U	Mining	M_1	Talos	U	M_1
Enterprise	U	Exploration	U	Sirius	M_2	M_2
Enterprise	U	Exploration	U	Talos	U	U

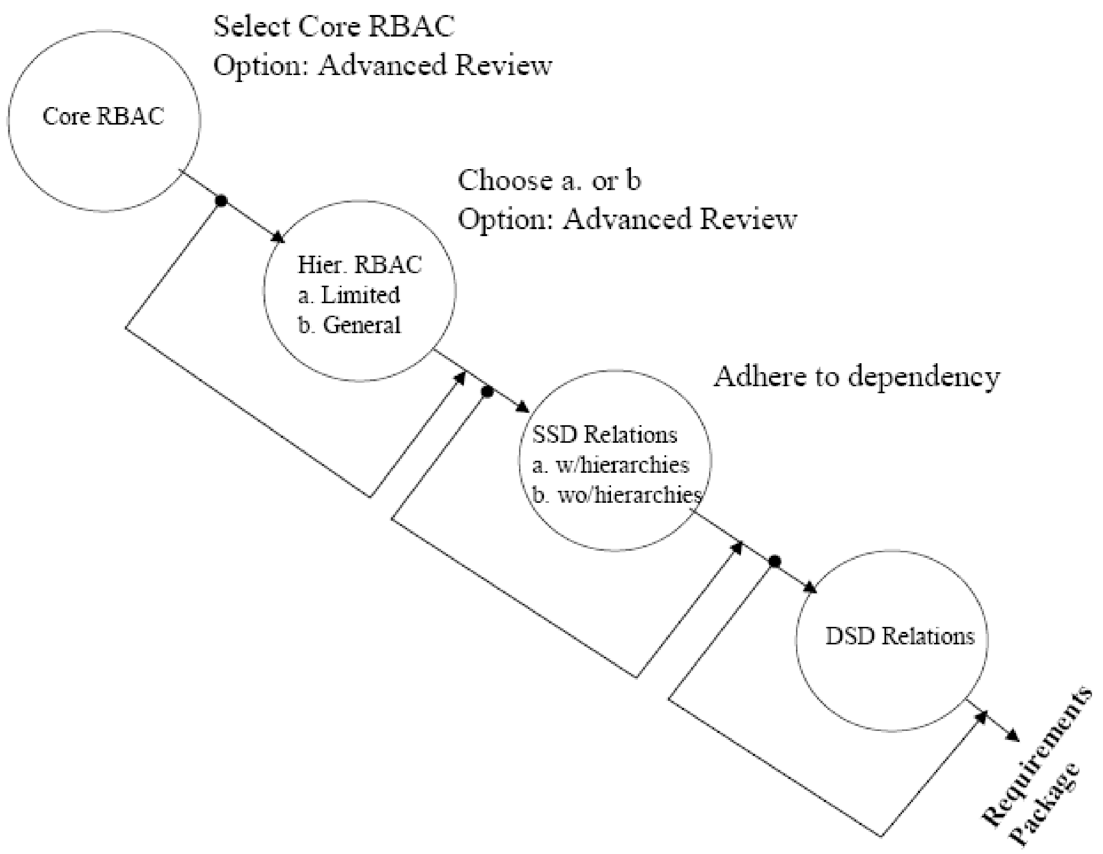
Role-Based Access Control: RBAC96 Model (1996)



Theorem. RBAC can be configured to enforce

- Lattice-Based Access Control (or Bell-LaPadula), and
- Discretionary Access Control

Role-Based Access Control: The NIST/ANSI Standard Model (2004)



Policy-Enforcement-Implementation (PEI) Layers (2000 onwards)

What?

Objectives
Policy Model
Enforcement Model
Implementation Model
Implementation

How?

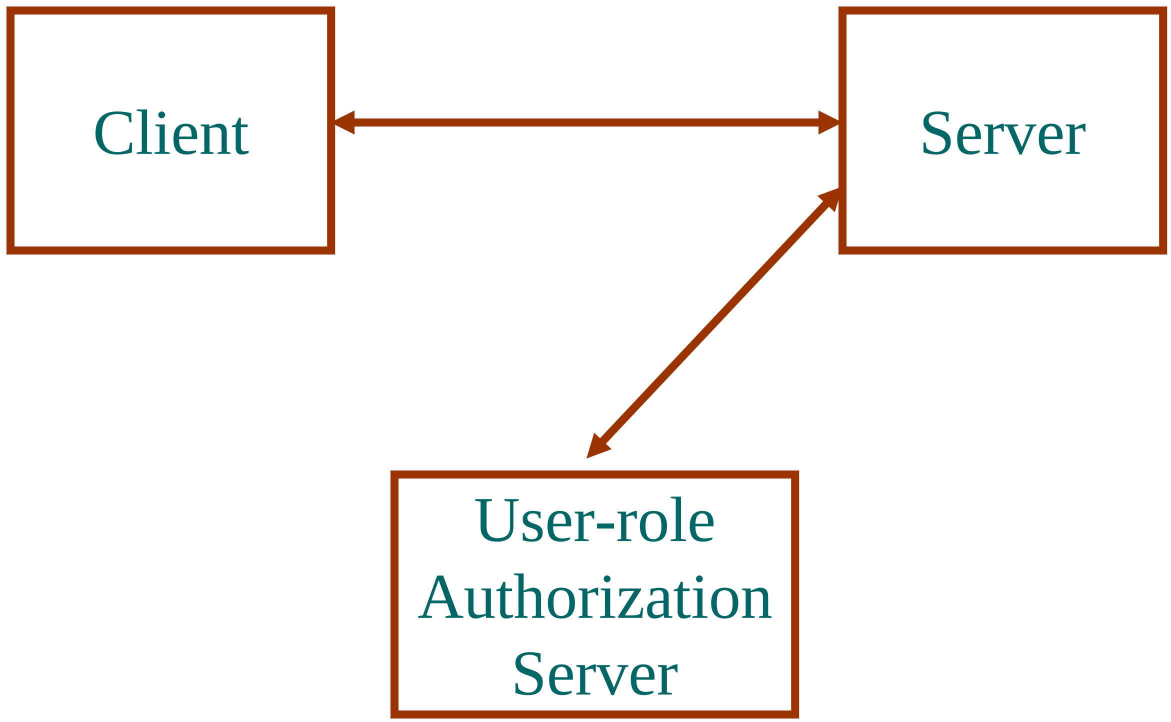
PEI and RBAC

What?

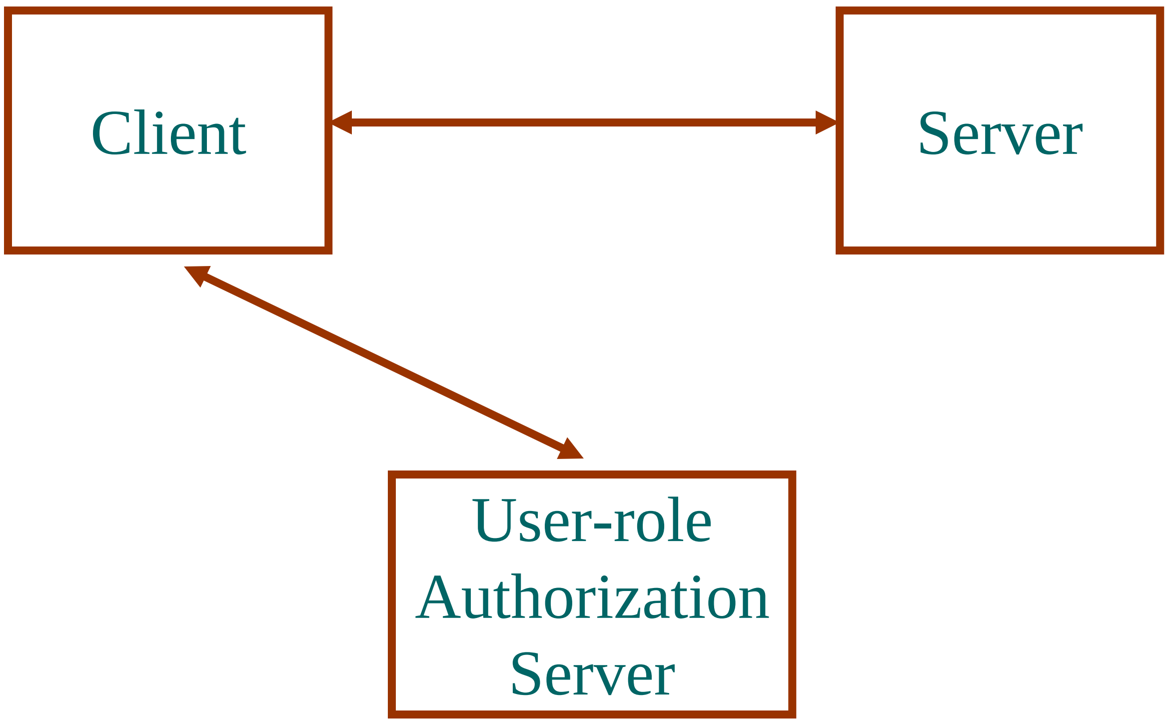
Policy Neutral
RBAC96, NIST/ANSI04, ARBAC97, Delegation, etc.
User-Pull, Server-Pull
Digital Certificates, Cookies, Tickets, SAML assertions etc.
Implementation

How?

PEI and RBAC: Server-Pull Enforcement

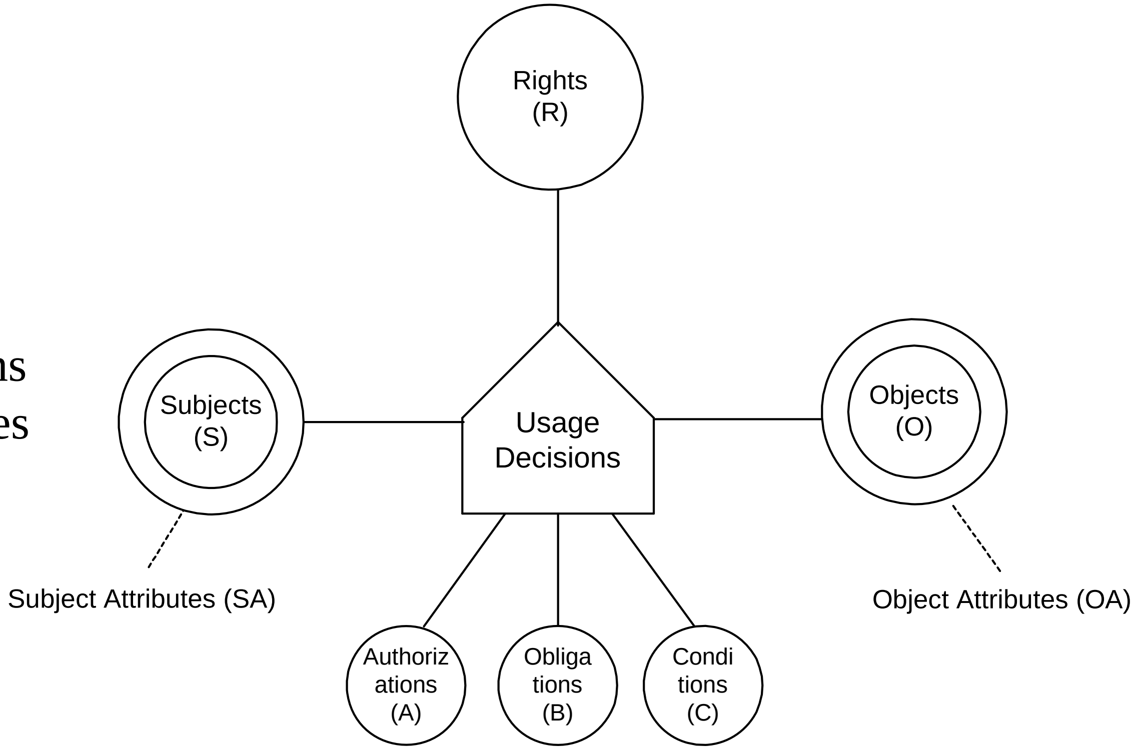


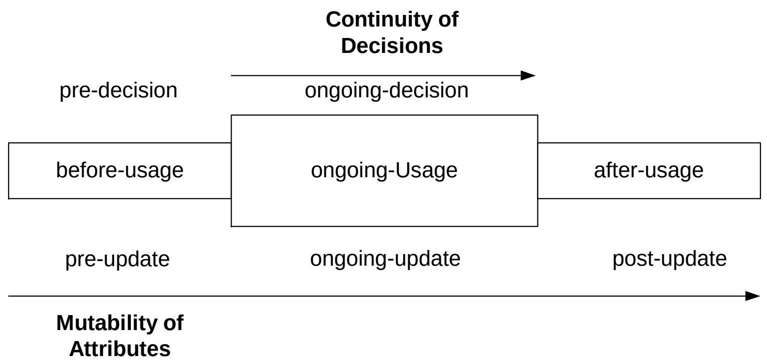
PEI and RBAC: User-Pull Enforcement



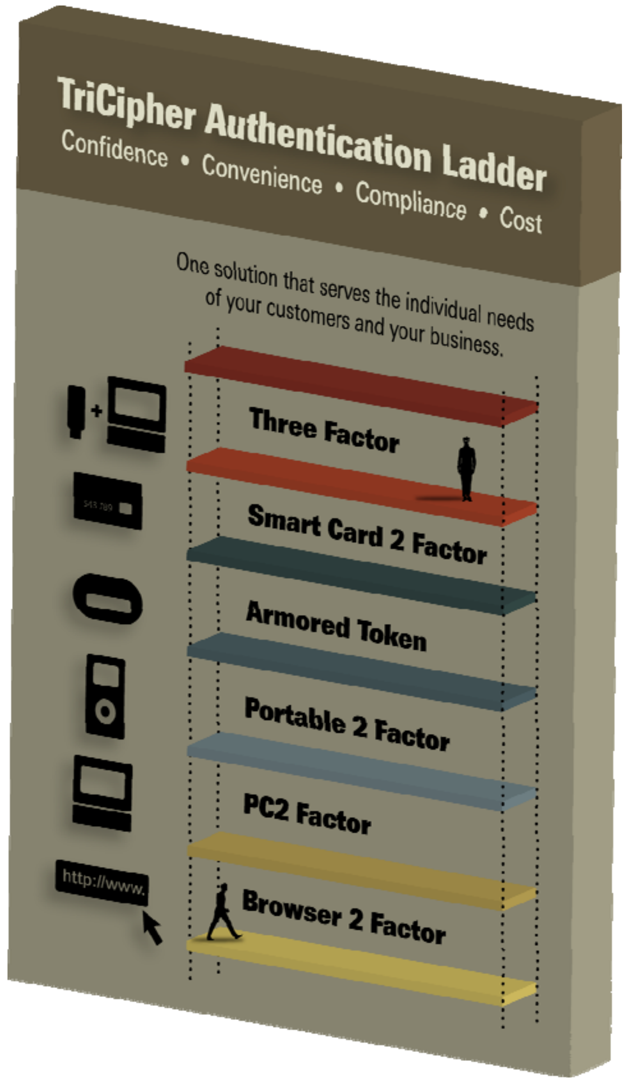
Usage Control
The UCON Model (2002 onwards)

- unified model integrating
  - authorization
  - obligation
  - conditions
- and incorporating
  - continuity of decisions
  - mutability of attributes





TriCipher Authentication Ladder: Functional View



TriCipher Authentication Ladder: Underlying Science

- 2-key RSA
  - Private key: d (used to sign)
  - Public key: e (used to verify signature)
- 3-key RSA
  - Net effect: as though single private key d was used to sign, BUT
    - Private key: d1 (used by user to partially sign)
    - Private key: d2 (used by TACS server to partially signature)
  - Public key: e (used to verify signature)

TriCipher Authentication Ladder: Underlying Science

$$e * d = 1 \bmod \phi(n)$$

$$d1 * d2 = d \bmod \phi(n)$$

Constructed on client PC from multiple factors under control of user

Stored on TACS server and used to partially sign on behalf of authenticated user

password

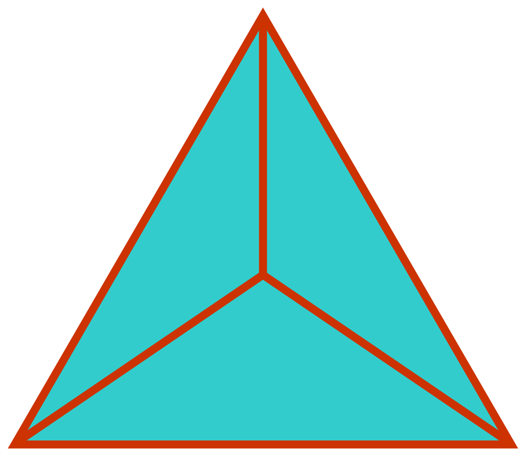
random string 1

random string 2

...

Assured Information Sharing Enabled by Trusted Computing (Ongoing work)

Secure Information
Sharing (IS)
“Share but Protect”
“Mother of all Security Problems”



Policy-Enforcement-
Implementation Layers (PEI)
&
Usage Control Models (UCON)

Trusted
Computing (TC)

What is Trusted Computing (TC)?

- Basic premise
  - Software alone cannot provide an adequate foundation for trust
- Old style Trusted Computing (1970 – 1990's)
  - Multics system
  - Capability-based computers
    - Intel 432 vis a vis Intel 8086
  - Trust with security kernel based on military-style security labels
    - Orange Book: eliminate trust from applications
- What's new (2000's)
  - Hardware and cryptography-based root of trust
    - Trust within a platform
    - Trust across platforms
  - Rely on trust in applications
    - No Trojan Horses or
    - Mitigate Trojan Horses and bugs by legal and reputational recourse

Massive paradigm shift

Prevent information leakage by binding information to Trusted Viewers on the client

What is Information Sharing?

- The mother of all security problems
  - Share but protect
- Requires controls on the client
  - Server-side controls do not scale to high assurance
- Bigger than (but includes)
  - Retail DRM (Digital Rights Management)
  - Enterprise DRM

What is Information Sharing?

	Strength of Enforcement		
Content type and value	Weak	Medium	Strong
Sensitive and proprietary	Password-protected documents	Software-based client controls for documents	Hardware based trusted viewers, displays and inputs
Revenue driven	IEEE, ACM digital libraries protected by server access controls	DRM-enabled media players such as for digital music and eBooks	Dongle-based copy protection, hardware based trusted viewers, displays and inputs
Sensitive and revenue	Analyst and business reports protected by server access controls	Software-based client controls for documents	Hardware based trusted viewers, displays and inputs

Roshan Thomas and Ravi Sandhu, "Towards a Multi-Dimensional Characterization of Dissemination Control." POLICY04.

	Functionality		Strength of enforcement	
	Simple	**Complex**	**Weak/Medium**	**Strong**
Legally enforceable versus system enforced rights.			Reliance on legal enforcement; Limited system enforced controls.	Strong system- enforceable rights, revocable rights.
Dissemination chains and flexibility.	I… c…	…i-	Mostly legal enforcement;	System enforceable controls.
Object types supported.	S… s…	…ersion	Reliance on legally enforceable rights.	System supported and enforceable rights and sanitization on multiple versions.
Persistence and modifiability of rights and licenses.	Immutable, persistent and viral on all disseminated copies.	Not viral and modifiable by recipient.	Reliance on legally enforceable rights.	System enforceable.
Online versus offline access and persistent client-side copies	No offline access and no client-side copies.	Allows offline access to client-side copies.	Few unprotected copies are tolerated.	No unprotected copies are tolerated.
Usage controls	Control of basic dissemination.	Flexible, rule-based usage controls on instances.	Some usage abuse	No potential for usage
Preservation of attribution.	Recipient has legal obligation to give attribution to disseminator.	System-enabled pr… trace- back of the … back to original dis…		… is system
Revocation	Simple explicit revocations.	Complex policy-ba…		…d to take … effect.
Support for derived and value-added objects.	Not supported.	Supported.		…forceable rights … and valued- added objects.
Integrity protection for disseminated objects.	Out of band or non-crypto based validation.	Cryptographic schemes for integrity validation.	Off-line validation.	High-assurance cryptographic validation.
Audit	Audit support for basic dissemination operations.	Additional support for the audit of instance usage.	Offline audit analysis.	Real-time audit analysis and alerts.
Payment	Simple payment schemes (if any).	Multiple pricing models and payment schemes including resale.	Tolerance of some revenue loss.	No revenue loss; Objective is to maximize revenue.

With current state of knowledge the information sharing space is too complex to characterize in a comprehensive manner

Look for sweet spots that are of practical interest and where progress (and killer products) can be made

Roshan Thomas and Ravi Sandhu, "Towards a Multi-Dimensional Characterization of Dissemination Control." POLICY04.

Classic Approaches to Information Sharing

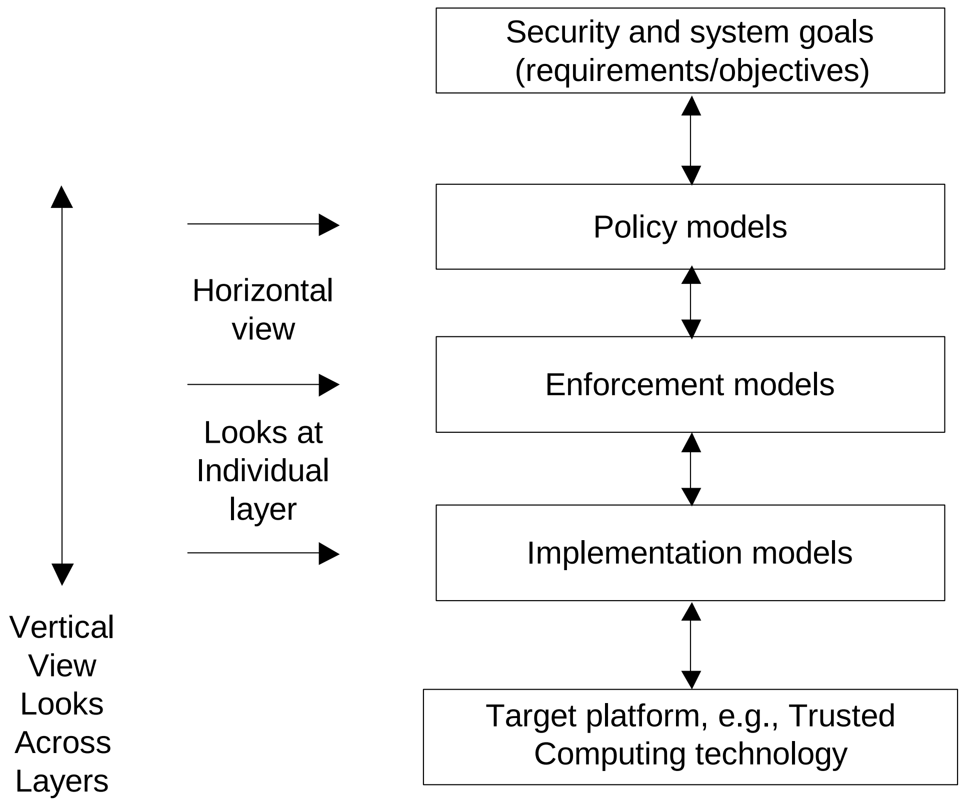
- Discretionary Access Control (DAC), Lampson 1971
  - Fundamentally broken
  - Controls access to the original but not to copies (or extracts)
- Mandatory Access Control (MAC), Bell-LaPadula 1971
  - Solves the problem for coarse-grained sharing
    - Thorny issues of covert channels, inference, aggregation remain but can be confronted
  - Does not scale to fine-grained sharing
    - Super-exponential explosion of security labels is impractical
    - Fallback to DAC for fine-grained control (as per the Orange Book) is pointless
- Originator Control (ORCON), Graubart 1989
  - Propagated access control lists: let copying happen but propagate ACLs to copies (or extracts)

Not very successful

Modern Approach to Information Sharing

- Prevent leakage by binding information to Trusted Viewers on the client
  - Use a mix of cryptographic and access control techniques
- Cryptography and Trusted Computing primitives enable encapsulation of content in a Trusted Viewer
  - Trusted Viewer cannot see plaintext unless it has the correct keys
- Access control enables fine-grained control and flexible policy enforcement by the Trusted Viewer
  - Trusted Viewer will not display plaintext (even though it can) unless policy requirements are met
  - Enables policy flexibility and policy-mechanism separation

PEI Models Framework for Information Sharing



The Future: Three Megatrends

- Fundamental changes in
  - Cyber-security goals
  - Cyber-security threats
  - Cyber-security technology

Cyber-security goals are changing

USAGE
purpose

INTEG
modific

USAGE

LABILITY
access

Cyber-security attacks are changing

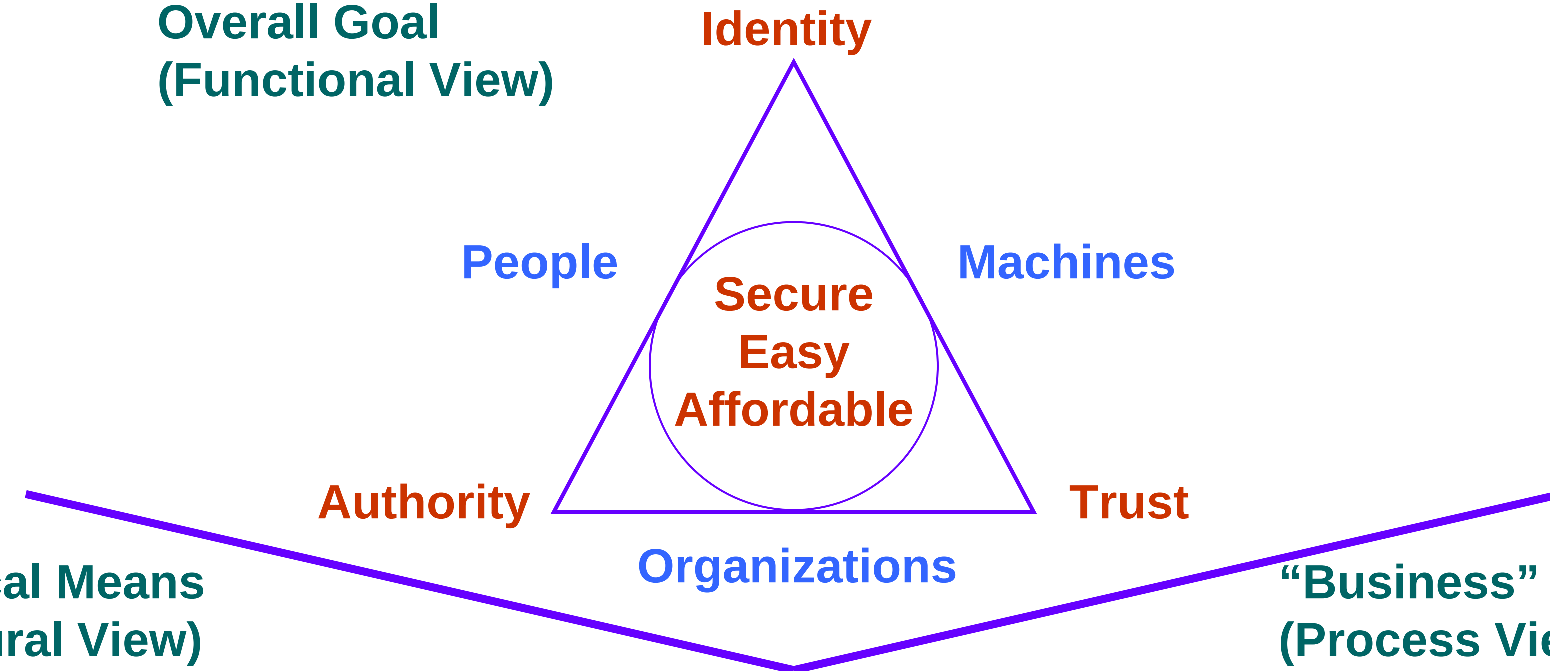
- The professionals have moved in
  - ~~Hacking for fun and fame~~
  - Hacking for cash, espionage and sabotage

Cyber-security technology is changing

- Trusted computing on the client
- Virtualization
- Massive parallelism on the desktop
- Computation-and-power challenged mobile devices
- etcetera

Cyber-Identity, Authority and Trust Systems

Overall Goal
(Functional View)



Technical Means
(Structural View)

UCON (Usage Control)

RBAC (Role-Based Access Control)

Info Sharing

PKI (Public-Key Infrastructure)

TC (Trusted Computing)

TM (Trust Management)

TONs (Trusted Overlay Networks)

DPM (Distributed Policy Management)

DRM (Digital Rights Management)

SA (Situational Awareness)

ETC (……………)

PEI Layered Models

“Business” Means
(Process View)

Business Models
Legal, Social
Regulations
Reputational
Risk, Liability
Privacy
Cost
Recourse
etc

Information Assurance: A Personal Perspective

Ravi Sandhu
www.list.gmu.edu

Q&A