The Future of Cyber Security

Prof. Ravi Sandhu
Executive Director and
Endowed Chair

ravi.sandhu@utsa.edu
www.profsandhu.com
www.ics.utsa.edu

Cyber Security Status

- Cyber technologies and systems have evolved
- Cyber security goals have evolved
  - Computer security
  - Computer security + Communications security
    - Separate and never shall meet TO
    - Coupled and integrated
  - Information assurance
  - Mission assurance
- Cyber security research/practice have not kept up
  - The gap is growing

Cyber Security Status

- ➢ Mission assurance = Application assurance
- ➢ Latest technology: Cloud Computing

  Dominant issues:
  - ❖ Cost and productivity
  - ❖ Focus on core competence
  - ❖ Availability
  - ❖ Security
- ➢ Latest lesson (April-May 2011):
  - ❖ Amazon outage
  - ❖ 100s of companies with 24-72 hours downtime
  - ❖ Netflix unaffected

Cyber Security Doctrine

- Old think: protect the network, protect the information, protect the content
  - Design to isolate and protect the network in face of system and security failures
- New think: protect the mission, protect the application, protect the service
  - Design to operate through system and security failures
  - Not possible without application context
- Most important recommendation
  - Cyber security needs to be a proactive rather than reactive discipline

Fundamental Premise

- Cyber security is all about trade-offs
  - confidentiality
  - integrity
  - availablity
  - usage
  - privacy
  - cost
  - usability
  - productivity
- Application context is necessary for trade-offs

Productivity-Security

- Cyber Security is all about tradeoffs

Productivity | **Security**

Let's build it
Cash out the benefits
Next generation can secure it

Let's not build it
Let's bake in super-security to make it unusable/unaffordable
Let's sell unproven solutions

There is a middle ground
We don't know how to predictably find it

The ATM Paradox

- The ATM (Automatic Teller Machine) system is
  - secure enough
  - global in scope
- Not attainable via current cyber security science, engineering, doctrine
  - not studied as a success story
- Similar paradoxes apply to
  - on-line banking
  - e-commerce payments

Why is the ATM System Secure?

- Monetary loss is easier to quantify and compensate than information loss
- Security principles
  - stop loss mechanisms
  - audit trail (including physical video)
  - retail loss tolerance with recourse
  - wholesale loss avoidance
- Technical surprises
  - no asymmetric cryptography
  - no annonymity

Why is the ATM System Secure?

- Monetary loss is easier to quantify and compensate than information loss
- Security principles **Application Centric**
  - stop loss mechanisms
  - audit trail (including physical video)
  - retail loss tolerance with recourse
  - wholesale loss avoidance
- Technical surprises
  - no asymmetric cryptography
  - no annonymity

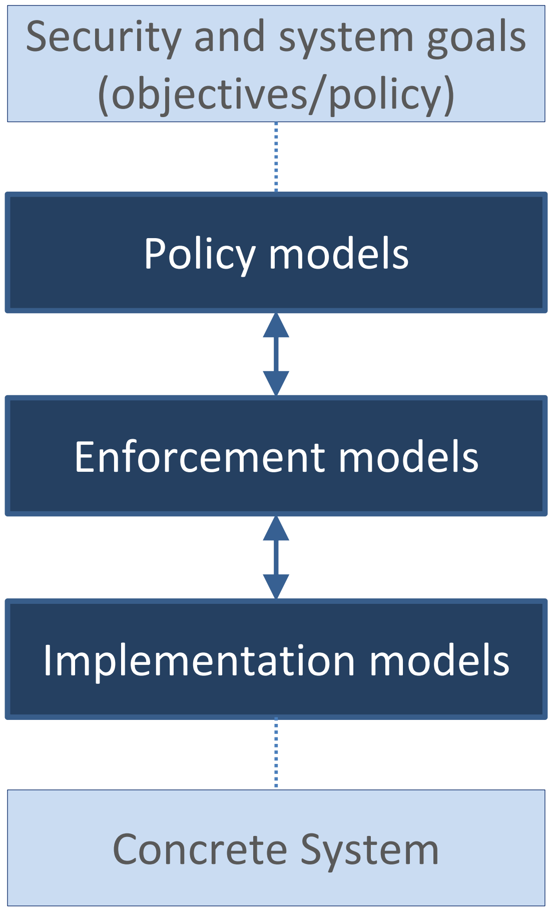
PEI Models

PEI MODELS

WHAT

HOW

HOW



Necessarily informal

Specified using users, subjects, objects, admins, labels, roles, groups, etc. in an ideal setting.

Security analysis (objectives, properties, etc.).

Approximated policy realized using system architecture with trusted servers, protocols, etc.

Enforcement level security analysis (e.g. stale information due to network latency, protocol proofs, etc.).

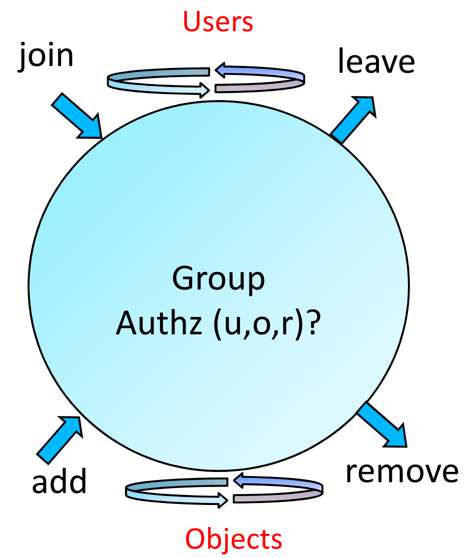
Technologies such as Cloud Computing, Trusted Computing, etc.

Implementation level security analysis (e.g. vulnerability analysis, penetration testing, etc.)

Software and Hardware

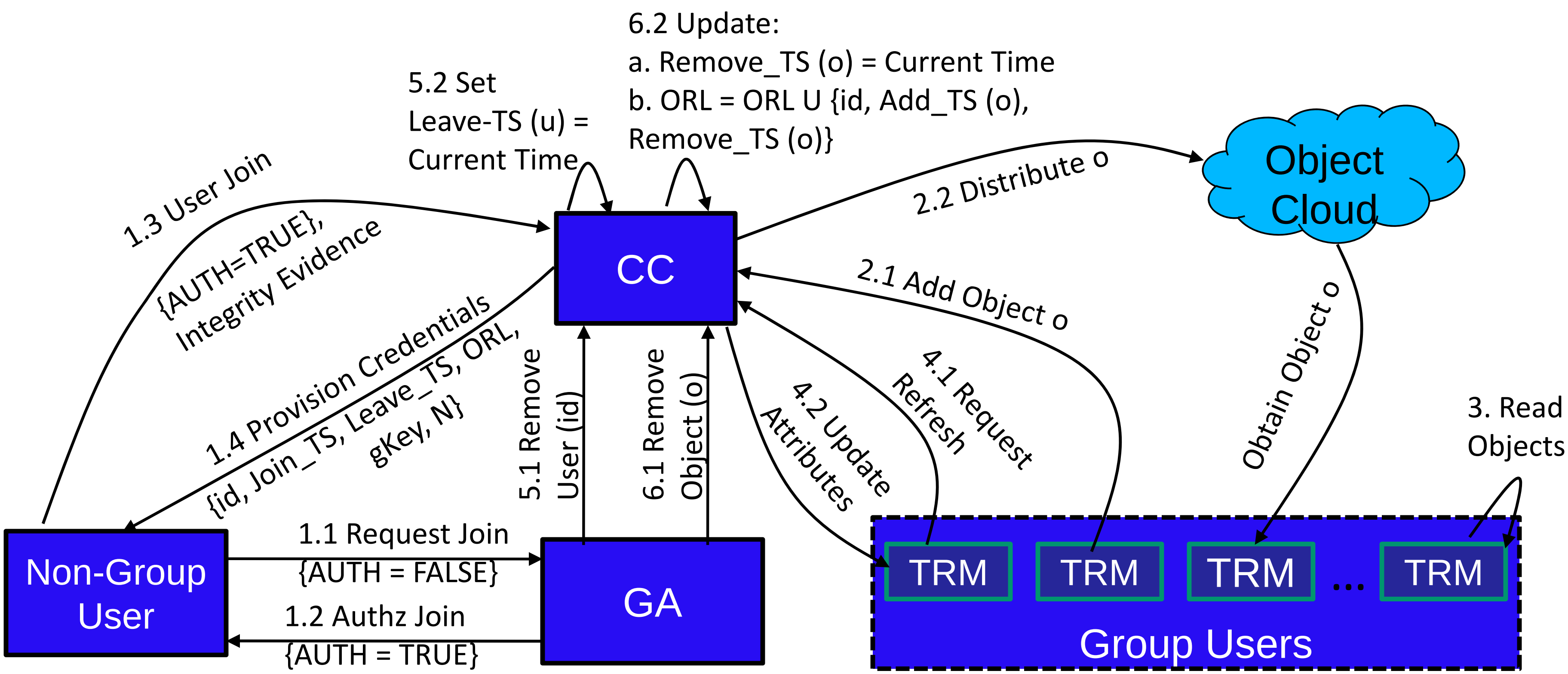
Group-Centric Secure Information Sharing Policy Models

- Operational aspects
  - Group operation semantics
    - Add, Join, Leave, Remove, etc
    - Multicast group is one example
  - Object model
    - Read-only
    - Read-Write (no versioning vs versioning)
  - User-subject model
    - Read-only Vs read-write
  - Policy specification



- Administrative aspects
  - Authorization to create group, user join/leave, object add/remove, etc.

Group-Centric Secure Information Sharing Enforcement Models



User Attributes: {id, Join-TS, Leave-TS, ORL, gKey}
Object Attributes: {id, Add-TS}

ORL: *Object Revocation List*
gKey: *Group Key*

Trusted Computing

- 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
  - Mitigate Trojan Horses and bugs by legal and reputational recourse

Trusted Computing

- Basic principles
  - Protect cryptographic keys
    - At rest
    - In motion
    - In use
  - Control which software can use the keys
- Marriage of cryptography and access control

Cyber Security Research

- Foundations
  - Security Models
  - Formal methods
  - Cryptography
- Application-Centric
  - Secure information sharing
  - Social computing
  - Health care
  - Data provenance
  - Critical infratructure
- Technology-Centric
  - Cloud computing
  - Smart grid
  - Trusted computing
  - Mission-aware diversity
- Attack-Centric
  - Botnet and malware analysis
  - Complex systems modeling
  - Zero-day defense
  - Moving target defense

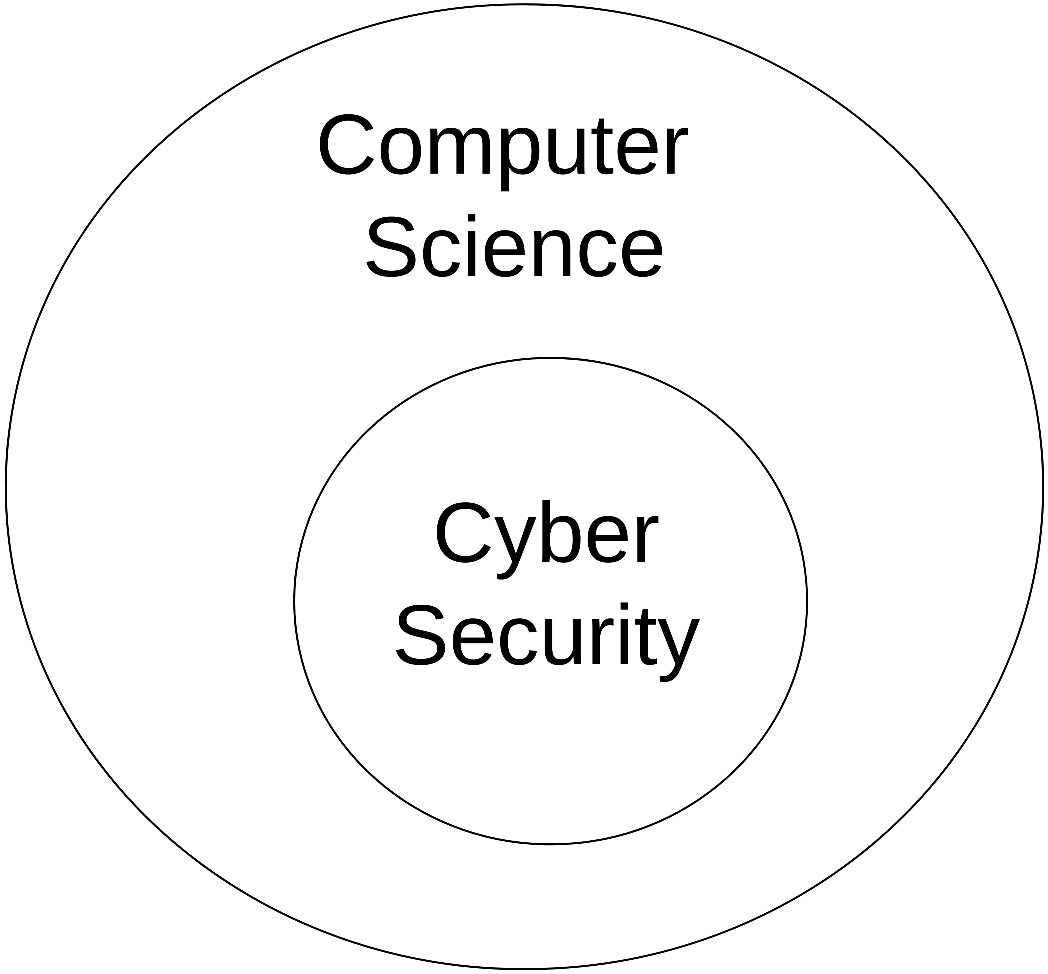
Microsec vs Macrosec

- Most cyber security thinking is microsec
- Most big cyber security threats are macrosec

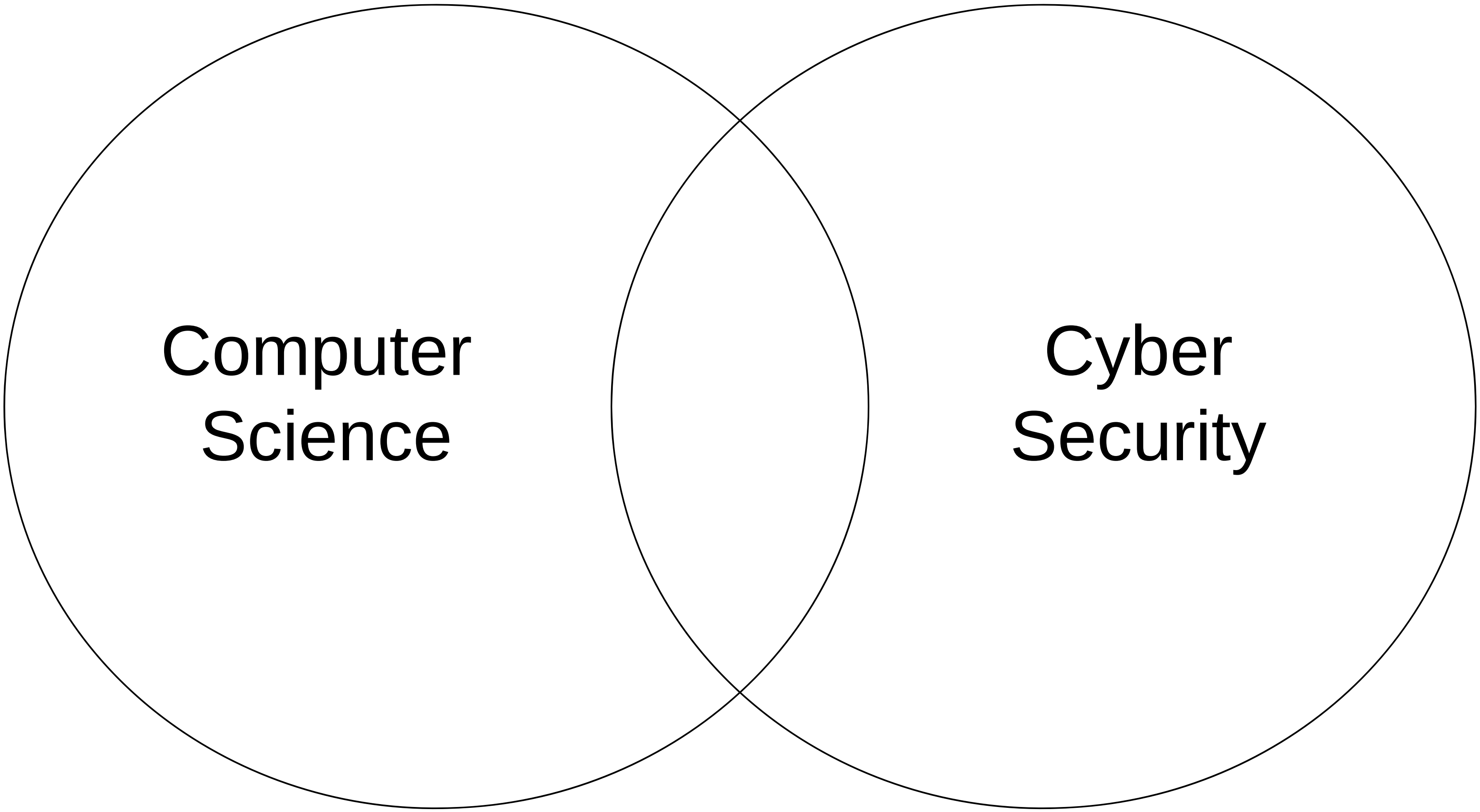
- Microsec
  - Retail attacks vs Targeted attacks
  - 99% of the attacks are thwarted by basic hygiene and some luck
  - 1% of the attacks are difficult and expensive, even impossible, to defend or detect

- Rational microsec behavior can result in highly vulnerable macrosec

Cyber Security as a Discipline



Cyber Security as a Discipline



The Cyber Security System Challenge

- Wisdom from the past:
  - "Generally, security is a system problem. That is, it is rare to find that a single security mechanism or procedure is used in isolation. Instead, several different elements working together usually compose a security system to protect something." R. Gaines and N. Shapiro 1978.
- The challenge is how to develop a systems perspective on cyber security