Cyber Security:
Past, Present and Future

Prof. Ravi Sandhu
Executive Director and Endowed Chair
Institute for Cyber Security (ICS)
University of Texas at San Antonio

August 2009

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

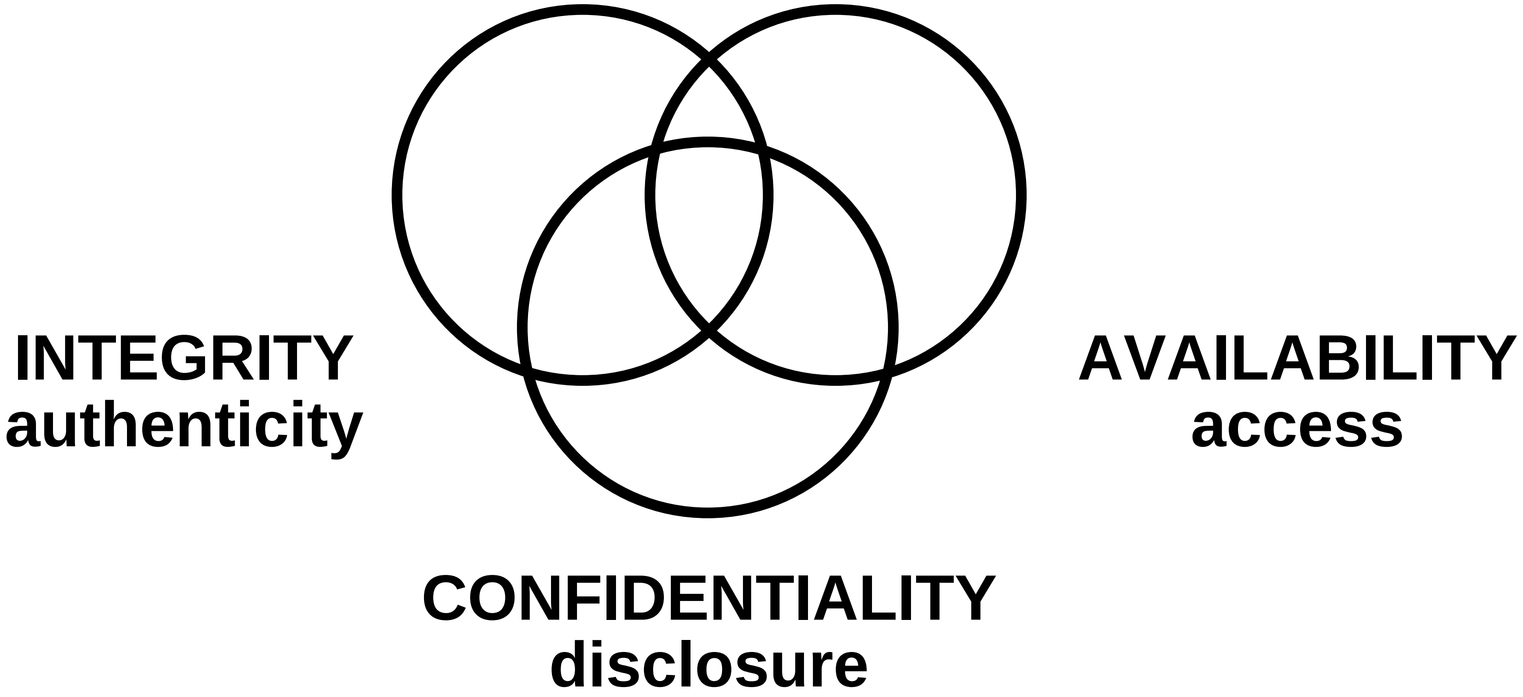
Institute for Cyber Security

- Founded June 2007: still in start-up mode

- World leading security modeling and analysis research
  - Role-Based Access Control (RBAC) Model: Commercially dominant model today
  - Usage Control (UCON) Model: Attribute-Based Access Control on Steroids
  - PEI Framework: Policy (what), Enforcement (how), Implementation (how exactly)
  - Group-Centric Information Sharing: Sharing metaphor of meeting room
  - Security for Social Networks
  - Botnet Analysis, Detection and Mitigation
  - Multilevel Secure Architectures
  - Secure Cloud Computing

- World-leading research infrastructure
  - FlexCloud
  - FlexFarm

Cyber Security Objectives

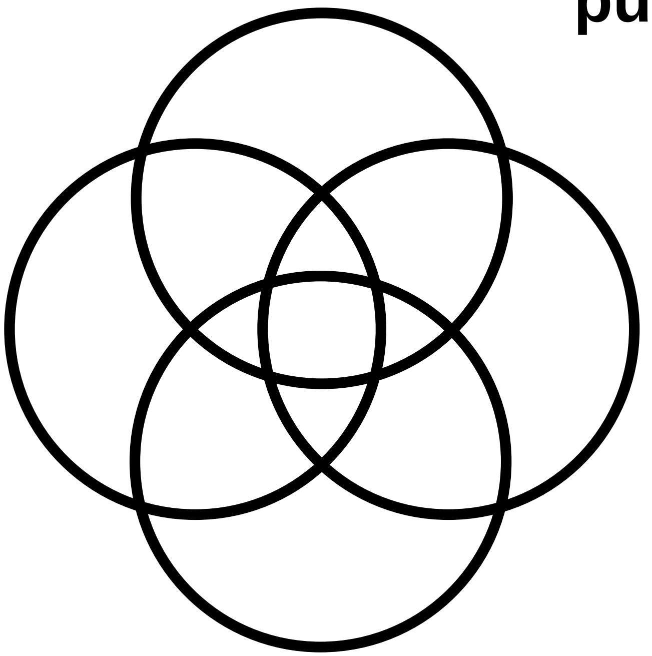


INTEGRITY
authenticity

AVAILABILITY
access

CONFIDENTIALITY
disclosure

Cyber Security Objectives



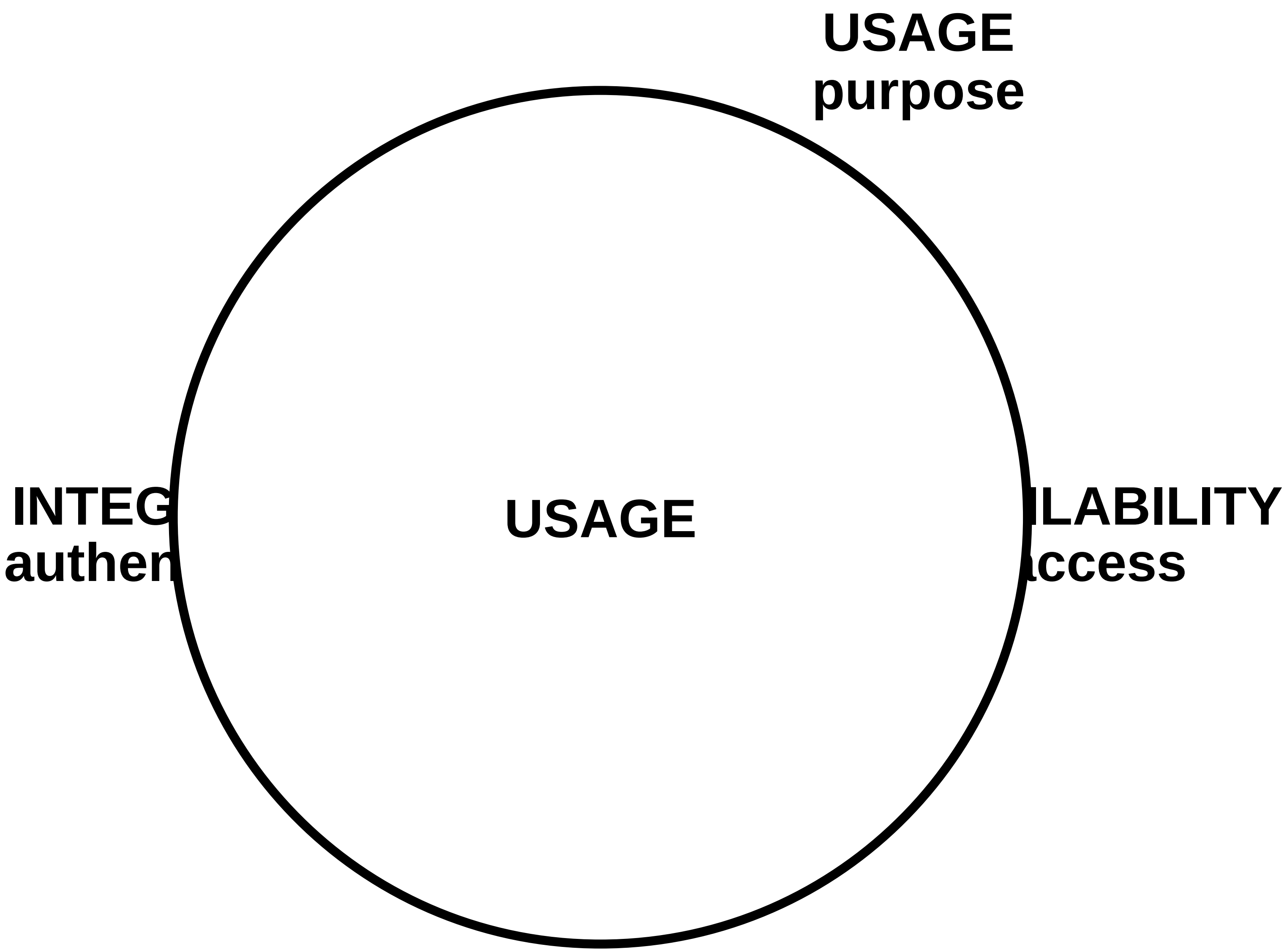
USAGE
purpose

INTEGRITY
authenticity

AVAILABILITY
access

CONFIDENTIALITY
disclosure

Cyber Security Objectives



USAGE
purpose

INTEG
authen

USAGE

ILABILITY
ccess

Cyber Security: Major Trends

- Major driver is the **Internet** which itself is in continuous transition
- **Attackers**: Morphed from
  - A nuisance

  to

  - Highly organized criminal ecosystem motivated by money
  - Stealthy infiltrators, spies and saboteurs driven by nation states and terrorists
- **Defenders**: Morphed from
  - Closed Enterprise-Centric era

  to

  - Open Application-Centric/Technology-Centric era
- **Dinosaurs**: Mired in old-think
  - Industry: mired in FUD (fear, uncertainty, doubt)
  - Academia: mired in fairy tales

Internet Architecture

Layer 5+	IM email web social nw VOIP collaboration twitter ……
Layer 4 **Layer 3**	Transport: TCP, UDP Routing: IP
Layer 2 **Layer 1**	Ethernet WiFi Cable-modem Wide-area network ……

Internet Architecture

INNOVATION

Layer 5+ IM email web social nw VOIP collaboration twitter ……

Layer 4 Transport: TCP, UDP
Layer 3 Routing: IP

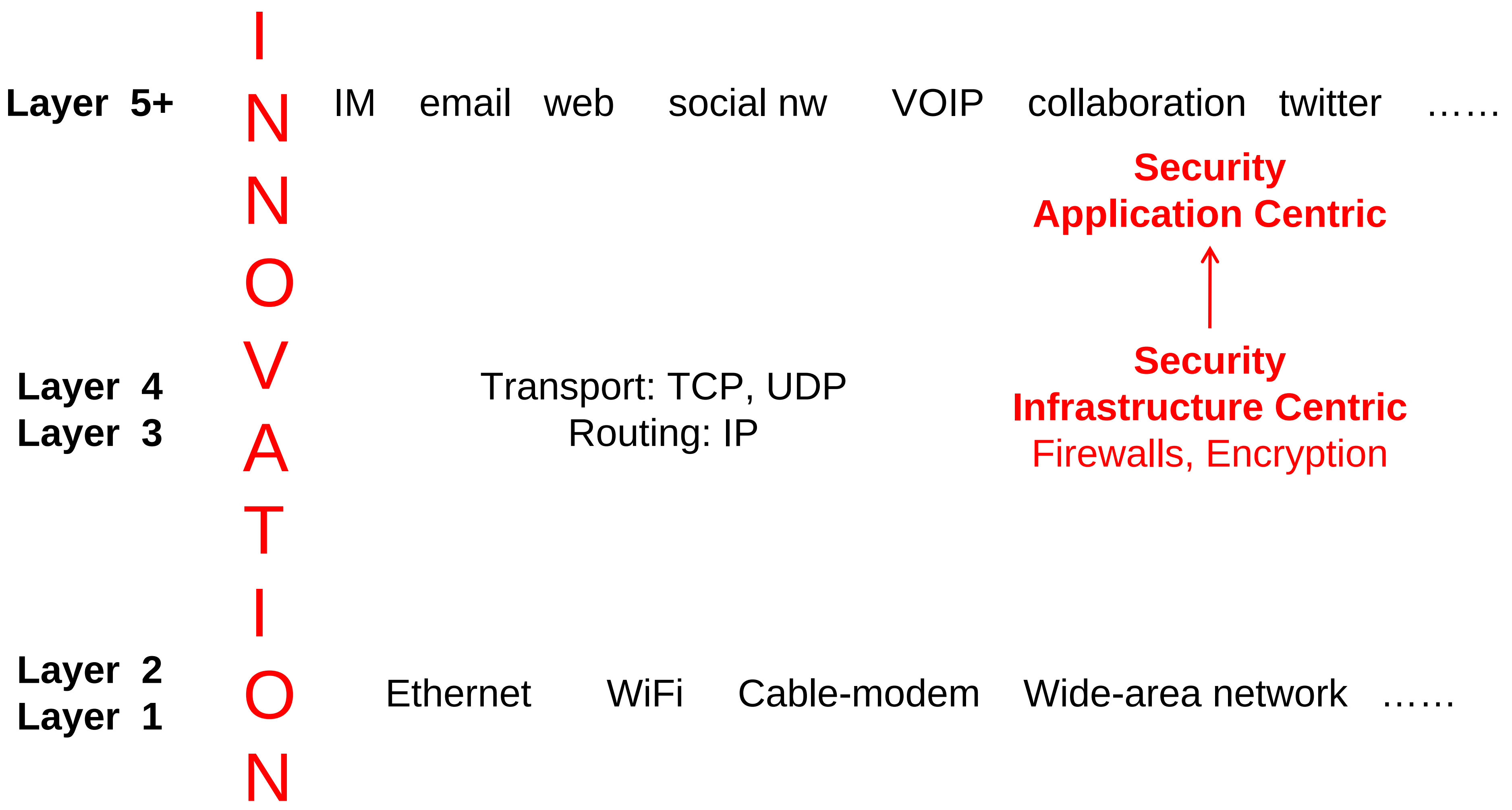
Layer 2
Layer 1 Ethernet WiFi Cable-modem Wide-area network ……

Internet Architecture

INNOVATION

Layer 5+	IM email web social nw VOIP collaboration twitter ……	
Layer 4 **Layer 3**	Transport: TCP, UDP Routing: IP	**Security** **Infrastructure Centric** Firewalls, Encryption
Layer 2 **Layer 1**	Ethernet WiFi Cable-modem Wide-area network ……	

Internet Architecture



INNOVATION

Layer 5+ IM email web social nw VOIP collaboration twitter ……

Security
Application Centric

↑

Security
Infrastructure Centric
Firewalls, Encryption

Layer 4
Layer 3

Transport: TCP, UDP
Routing: IP

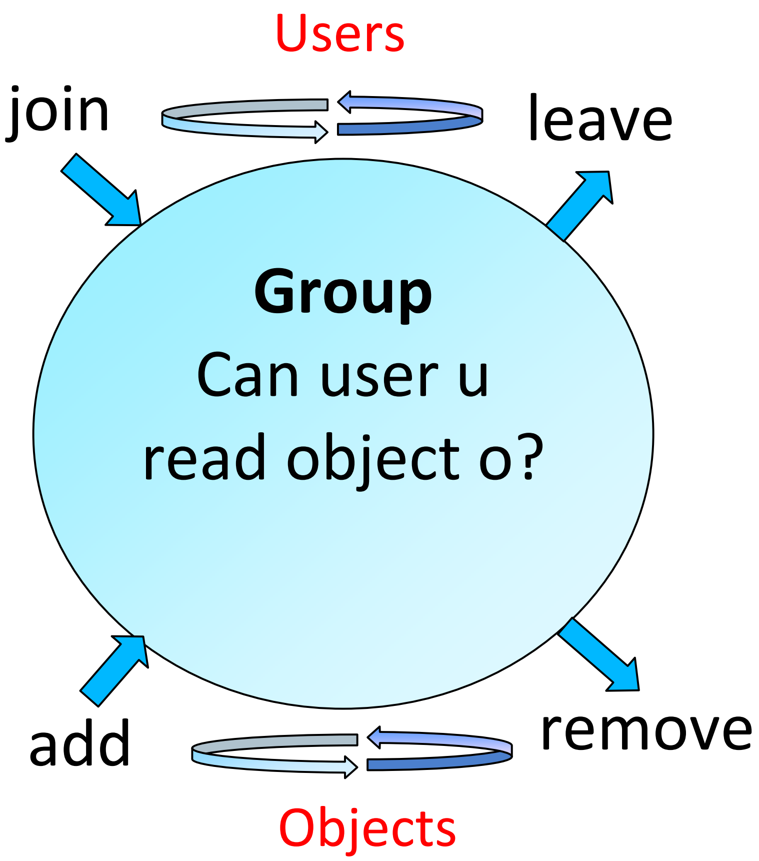
Layer 2
Layer 1

Ethernet WiFi Cable-modem Wide-area network ……

Policy (What)

Group-Centric Information Sharing

- Metaphor: Secure Meeting Room
- Operational aspects
  - What is authorized by join, add, etc.?
- Administrative aspects
  - Who authorizes join, add, etc.?
- Multiple groups
  - Inter-group relationship

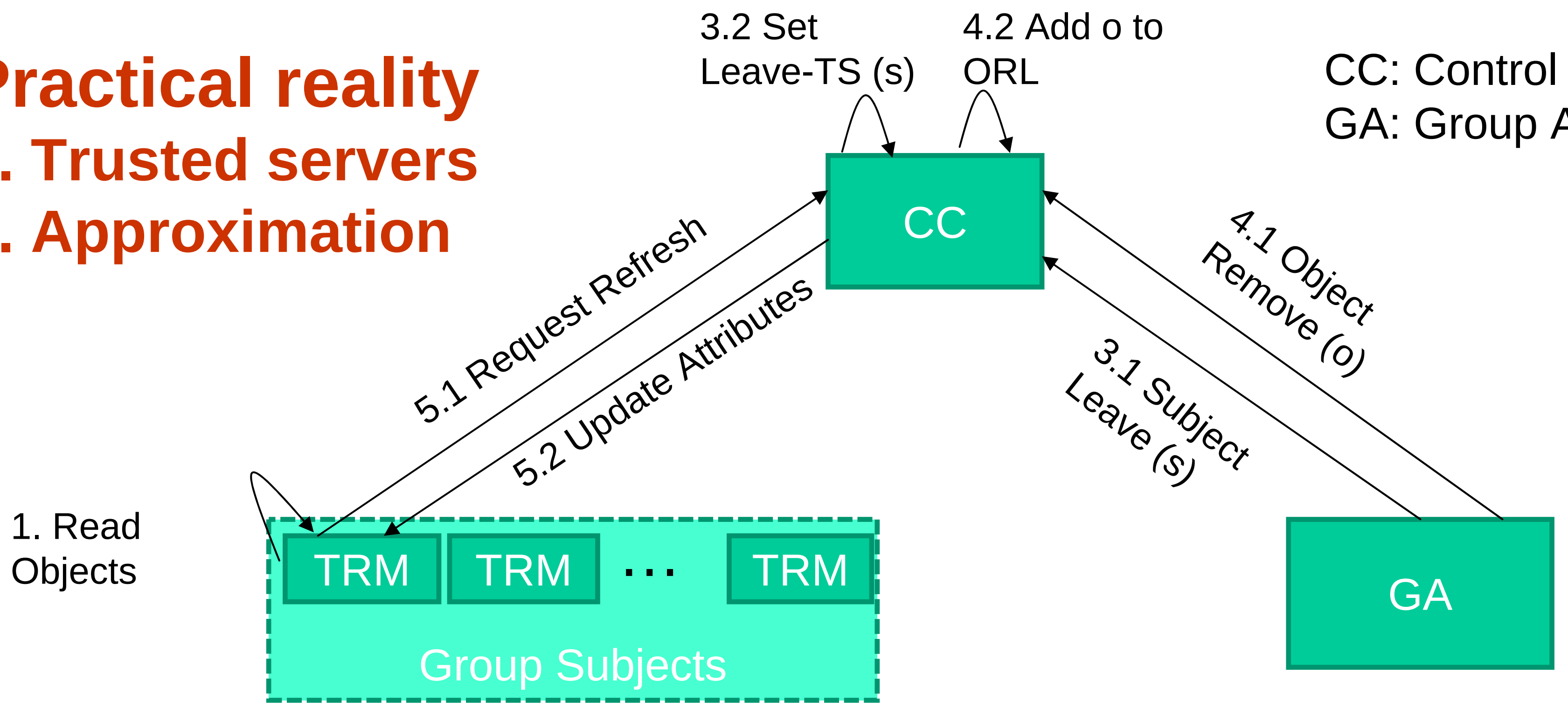


g-SIS Enforcement (How?)

Practical reality

1. Trusted servers

2. Approximation



CC: Control Center
GA: Group Administrator

Subject Attributes: {id, Join-TS, Leave-TS, ORL, gKey}

ORL: *Object Revocation List*

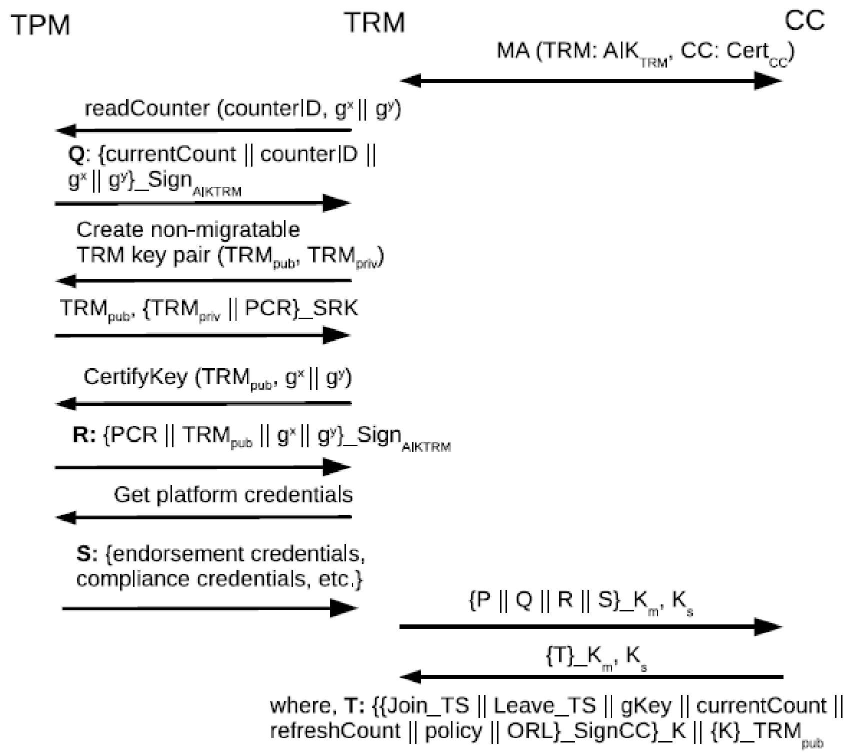
gKey: *Group Key*

Object Attributes: {id, Add-TS}

Refresh Time (RT): TRM contacts CC to update attributes

Implementation (How Exactly?)

- Detailed protocol and algorithm specifications



TPM

TRM

CC

MA (TRM: AIK_{TRM}, CC: Cert_{CC})

readCounter (counterID, g^x || g^y)

Q: {currentCount || counterID || g^x || g^y}_$\text{Sign}_{\text{AIKTRM}}$

Create non-migratable TRM key pair (TRM_{pub}, TRM_{priv})

TRM_{pub}, {TRM_{priv} || PCR}_SRK

CertifyKey (TRM_{pub}, g^x || g^y)

R: {PCR || TRM_{pub} || g^x || g^y}_$\text{Sign}_{\text{AIKTRM}}$

Get platform credentials

S: {endorsement credentials, compliance credentials, etc.}

{P || Q || R || S}_K_m, K_s

{T}_K_m, K_s

where, **T:** {{Join_TS || Leave_TS || gKey || currentCount || refreshCount || policy || ORL}_SignCC}_K || {K}_TRM_{pub}

Conclusion

PAST, PRESENT

- Cyber security is a young and immature field
- The attackers are more innovative than defenders
- Defenders are mired in FUD and fairy tales

FUTURE

- Cyber security will become a scientific discpline
- Cyber security will be application and technology centric
- Cyber security will never be “solved”