The Challenge of Data and Application Security and Privacy (DASPY)

Ravi Sandhu
Executive Director and Endowed Professor
March 23, 2011

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

Fundamental Premise

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

Outline

- The ATM (Automatic Teller Machine) paradox
- Lessons from the Orange Book era
- Data security and privacy
- Application security
- The DASPY system challenge
- DASPY research thrusts

The ATM Paradox

- The ATM 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 Enough?

- 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 Enough?

- 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

Lessons from the Orange Book Era

- Our Basic Premise
  - Security is fundamentally about tradeoffs
  - There can be no security (no tradeoffs) without application context
- Orange Book/Rainbow Series (1983-94)
  - Security is all about high assurance
  - Application context makes high assurance security impossible to achieve

Rainbow Series

- 34 titles listed in Wikipedia as the "most significant Rainbow series books"
  - Only 1 addresses applications
  - Trusted Database Interpretation (TDI)
  - Scope: "Trusted Applications in general and database management system in particular"

I·C·S
The Institute for Cyber Security

The Polyinstantiation Wars

UTSA

Software Architect	Project	% Time	Label
Alice	Win7	25%	U
Alice	SecureWin7	75%	S
Bob	Vista	100%	U

- What precisely is Secret?
  - There exists a SecureVista project
  - Alice works on SecureVista
  - Alice's effort on SecureVista is 75%
  - All or some of the above
- How do we maintain integrity of the database?
  - Depends

Much work and $$$ by researchers and vendors, late 80's-early 90's

Data Security and Privacy

- Familiar term used for over 3 decades
- Fundamental problems identified in the first decade continue to dominate
  - covert channels
  - inference and aggregation
  - homomorphic encryption
- "The general understanding of the term data security and privacy is probably not significantly changed since these early days, although of course in the details and nuances there have been considerable advances." -- Sandhu, CODASPY11

Application Security

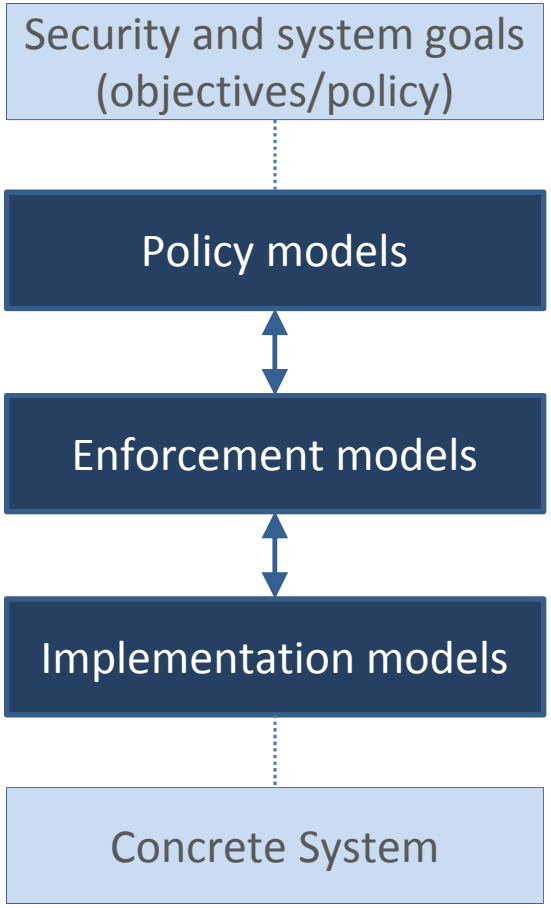
- Has come into use relatively recently
  - Remains amorphous
- The How interpretation: (currently prevalent in industry)
  - scanning for software vulnerabilities such as buffer overflow
  - run time application firewalls to prevent/detect application layer attacks
- The What interpretation: (the bigger challenge)
  - security policy and trade-offs in existing applications such as on-line banking: relatively straightforward and relatively well understood
  - security policy and trade-offs in newer applications such as social networks, secure information sharing, smart grid, secure data provenance, location-based services, electronic helath records: much fuzzier, less familiar and a major challenge to understand

The DASPY 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 DASPY system challenge is how to develop a systems perspective on DASPY

The DASPY System Challenge

PEI MODELS



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.).

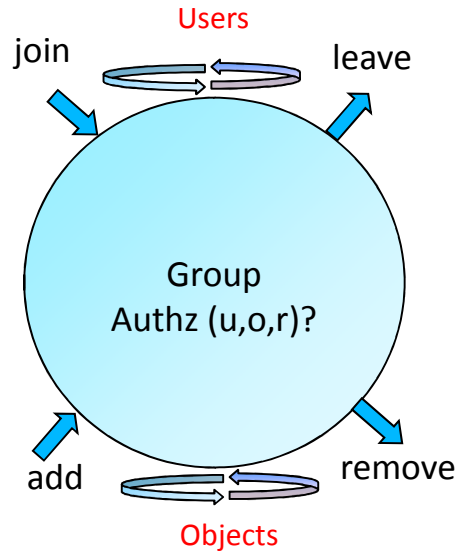
Technologies such as Cloud Computing, Trusted Computing, etc.

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

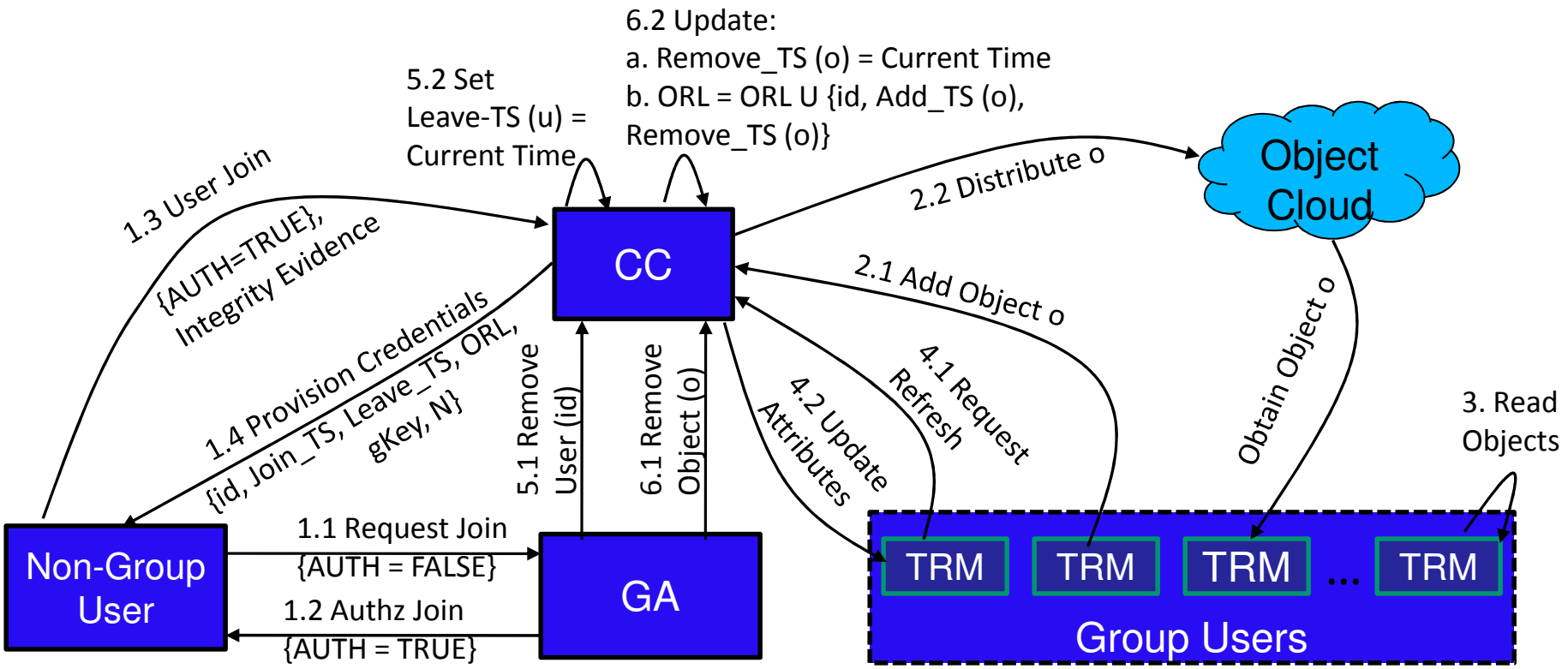
Software and Hardware

Group-Centric 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 Sharing Enforcement Models



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

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

DASPY Research Thrusts

- Continue to pursue
  - point solutions for various problems in data security and privacy
  - solutions on the how aspect of application security
- Embark on research to understand the what elements of application security
  - There are some excellent examples already but this thrust needs further and explicit encouragement.
- Embark on research to address the DASPY system challenge
  - Today this is largely ignored.

I·C·S
The Institute for Cyber Security

www.codaspy.org

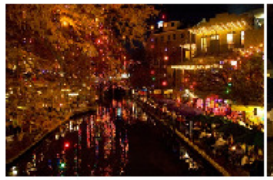
UTSA

First ACM Conference on Data and Application Security and Privacy

ACM CODASPY 2011

Feb 21-23, 2011 | Hilton Palacio Del Rio | San Antonio, TX, USA.

The deadline for early registration is January 22, 2011.




- Home
- Registration
- US Visa
- Hotel
- Program
- Keynote Speakers
- Call for Papers
- Camera Ready
- Organizers
- Program Committee
- Important Dates
- Submission Instructions

Maintained by:

Institute for Cyber Security UTSA

Announcement

ACM SIGSAC announces the creation of a new annual ACM Conference on Data and Applications Security and Privacy. The inaugural conference will be held **February 21-23 2011 in Hilton Palaci Del Rio, San Antonio, Texas.**

About

With rapid global penetration of the Internet and smart phones and the resulting productivity and social gains, the world is becoming increasingly dependent on its cyber infrastructure. Criminals, spies and predators of all kinds have learnt to exploit this landscape much quicker than defenders have advanced in their technologies. Security and Privacy has become an essential concern of applications and systems throughout their lifecycle. Security concerns have rapidly moved up the software stack as the Internet and web have matured. The security, privacy, functionality, cost and usability tradeoffs necessary in any practical system can only be effectively achieved at the data a application layers. This new conference provides a dedicated venue for high-quality research in thi arena, and seeks to foster a community with this focus in cyber security.

Best Paper Award Committee

Gail-Joon Ahn (Arizona State University)

Elena Ferrari (University of Insubria)

Dan Thomsen (Sandia National Labs)