The PEI Framework for Application-Centric Security

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

May 2009

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

PEI = Policy, Enforcement, Implementation

Presented by:
Ram Krishnan, GMU

Application Context

- Our Basic Premise
  There can be no security without application context

- Orange Book and Rainbow Series era (1983-1994)
  Opposite Premise
  Application context makes high assurance security impossible to achieve
  - May need to settle for "reasonable" assurance or "good-enough" security
  - Its about "mission assurance" not "information assurance"

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”

Application Context

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

- What precisely is Secret?
  - There exists a SecureWin7 project
  - Alice works on SecureWin7
  - Alice's effort on SecureWin7 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

Orange/Rainbow Fatal Flaws

- Enforcement of 1-way information flow in a lattice is not the dominant concern for most applications
- Avoiding covert channels is not the highest priority for most applications
- Exclusion of cryptography probably not the right decision for securing distributed systems

Post-Orange Era

- Firewalls, patch cycle, vulnerability scanners, intrusion detection, intrusion prevention, Identity Management, Federation, SSL, VPNs, PKI, etc
- Emergence and dominance of RBAC over MAC/DAC
- Emergence of highly motivated, sophisticated and innovative attackers

Emerging Application-Centric Era (ACE)

ECE

**Enterprise-Centric Era
(Orange/Rainbow Era
Post-Orange Era)**

Applications are cyber analogs of previously existing enterprise-centric applications

- **on-line banking**
- **brokerage**
- **e-retail**
- **auctions**
- **search engines**

ACE

Application-Centric Era

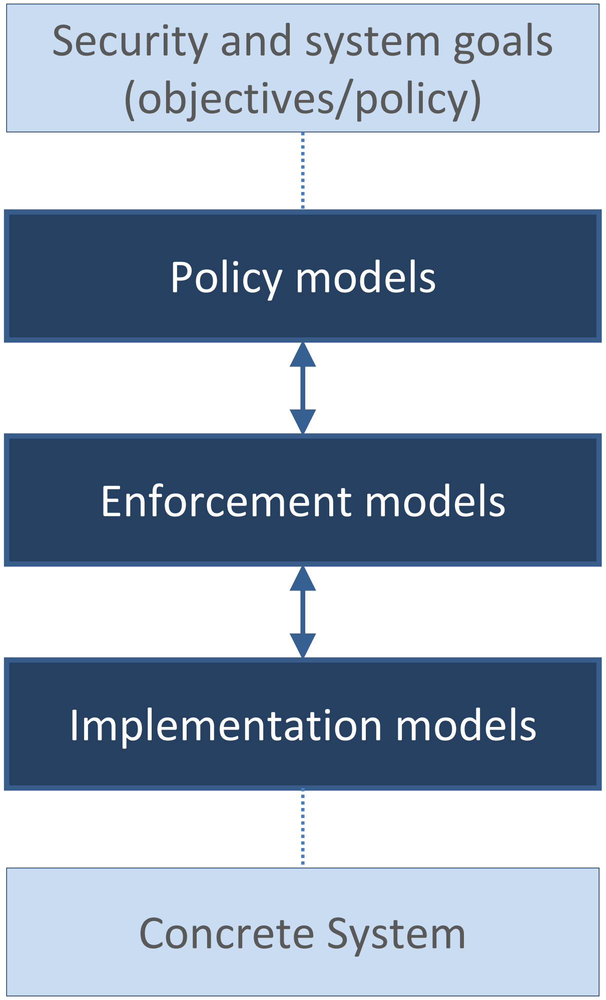
Future applications will be fundamentally different

- **?**
- **?**
- **?**
- **?**
- **?**
- Social Networking Websites?

ACE Characteristics

- Multi-party interests
- Fuzzy security objectives
- Attack/threat models

PEI Models



Security and system goals (objectives/policy)

Policy models

Enforcement models

Implementation models

Concrete System

- 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