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

  Opposite Premise
  Application context makes high assurance security impossible to achieve
  - May need to settle for “reasonable” assurance or “good-enough” security
  - It's about “mission assurance” not “information assurance”
• 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

<table>
<thead>
<tr>
<th>Software-Architect</th>
<th>Project</th>
<th>% Time</th>
<th>Label</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td>Win7</td>
<td>25%</td>
<td>U</td>
</tr>
<tr>
<td>Alice</td>
<td>SecureWin7</td>
<td>75%</td>
<td>S</td>
</tr>
<tr>
<td>Bob</td>
<td>Vista</td>
<td>100%</td>
<td>U</td>
</tr>
</tbody>
</table>

- **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**
- 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

- 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