

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

- 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”

- 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”

Software-Architect	Project	% Time	Label
Alice	Vista	25%	U
Alice	SecureVista	75%	S
Bob	XP	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

- 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 is not a smart decision for securing distributed systems

The Common Criteria, an ISO standard, and successor to the Orange Book has its own problems

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

ECE

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



ACE

Application-Centric Era

Applications are cyber analogs of
previously existing enterprise-centric
applications

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

Future applications will be
fundamentally different

- ?
- ?
- ?
- ?
- ?

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

PEI Models: 3 Layers/5 Layers

