Demo of ELISA

Enterprise Level Information System Assurance

Nina Tang and Pascal Meunier
Purpose

• Implement partial support for Patch and Vulnerability Groups (PVGs)

• PVGs recommended and defined in NIST special publication 800-40
Duties of PVGs

• 1. Create An Organizational Software Inventory.
• 2. Identify Newly Discovered Vulnerabilities and Security Patches.
• 3. Prioritize Patch Application.
• 4. Create an Organization-Specific Patch Database.
• 5. Conduct Generic Testing of Patches.
• 6. Distribute Patch and Vulnerability Information to Local Administrators.
• 7. Verify Patch Installation Through Network and Host Vulnerability Scanning.
• 8. Train System Administrators in the Use of Vulnerability Databases.
• 9. Perform Automatic Deployment of Patches (When Applicable).
Implementation

- Based on Cassandra system
- Profiles:
  - Lists of applications and keywords
- Vulnerabilities are found by matching profiles to ICAT database, which is based on MITRE’s CVE
Inheritance in ELISA Profiles

- Profiles can be children of other profiles (unlimited hierarchy)
- Inherit applications and keywords, and therefore vulnerabilities
- Inherit recommended and mandated patches
- PVG profiles are parents of regular (system administrator, SA) profiles
- SAs can add more applications and keywords
Implementation goal: Confidentiality

- Every PVG has a domain of confidentiality
- SAs must belong to that domain to create children profiles and benefit from the work of PVGs
- PVGs get reports of patching states for their domain only
- Hierarchical domains
Extended Resolution States

• Installed patch on all systems.
• Installed the patch on servers only.
• Installed the patch on desktop systems only.
• Patch could not be applied.
• Patch not applied because vulnerability is not exploitable.
• Removed offending software.
• Disabled offending software.
• Equivalent patch applied instead.
On to the Demo…