Building Trustworthy Systems with Cisco Secure Development Lifecycle
Foundation of Trust

Secure Process
- Lifecycle/Security Baseline
  - Product Security Requirements
  - Third Party Security
  - Vulnerability Testing
  - Detect Security Defects
  - Prevent Security Attacks
- Perform GAP Analysis
- Validate Requirements and Resiliency
- Register and Update Third Party Software
- Identify and Address Security Threats
- Secure Design
- Secure Coding
- CSDL

Trustworthy Systems Technology
- Common Modules and Hardware
  - Visibility and Control
  - Secure Communications
  - Platform Integrity

Secure Standards
- Information Assurance (IA)
  - Common Criteria
  - ISO 27034
  - FIPS/USGv6
  - TCG

Prevention
Detection
Recovery
Ensures consistent product security through proven techniques and technologies, reducing the number and severity of vulnerabilities in software.

Conforms with the guidelines of ISO 27034
Product Security Baseline (PSB)

Gap Analysis

PSB Architecture

- Administrative Access Security
- Application Security
- Authentication and Authorization
- Boot and System Integrity
- Cryptographic Support
- Development Process
- Hosted Services Hardening
- Logging and Auditing
- Operational Process
- Privacy and Data Security
- Session Management
- Threat Surface Reduction
- Traffic and Protocol Protection
- Vulnerability Management
- Web Security
Third Party Software Fundamentals

Minimize exposure by
• Perform gap analysis
• Establish maintenance plan
• Verify no backdoors
• Address all known vulnerabilities before FCS

Manages third party security alerts
• Register components with in a centralized database
• Contract support for critical security fixes

Planned response to security issues
• Follow established maintenance plan
Secure Design
Threat Modeling

Focus on how a feature can be attacked and how best to mitigate the attack
Secure Coding

- Boot Time Integrity with Run Time Defenses
  - ASLR
  - X-Space
  - OSC
- “Safe” libraries
- Input validation
- Best Practices Guidelines for each OS
- Signed Images
Static Analysis

- Security Checkers find key vulnerability types
  - Buffer overflow
  - Tainted input
  - Integer overflow
- Maximizes efficacy and reduce false positives
## Vulnerability Testing

Check Protocol Robustness
Duplicate Hacker Attacks

### CSDL Security Testing

#### Network Device Testing

<table>
<thead>
<tr>
<th>Codenomicon Protocol Robustness</th>
<th>Open Source “Hacker” Tools</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test Suites for 50+ Protocols, including: DNS, H.323, IKEv2, IPv4, IPv6, HTTP, SIP, SNMP, SSH, TLS and many more</td>
<td>20+ Open Source security tools, including: Amap, Curl, Dsniff, Hydra, Naptha, Nessus, Nikto, Nmap, Xprobe and many more</td>
</tr>
</tbody>
</table>

#### Application Testing

<table>
<thead>
<tr>
<th>IBM Rational AppScan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Family of application attack and test tools, including: risk analysis, security standard compliance testing, vulnerability scan and many more</td>
</tr>
</tbody>
</table>
ISO 27034 & CSDL

ISO 27034

• ISO 27034 is the standard for “Information Technology – Security Techniques – Application Security”

• Addresses Security Lifecycle for development and deployment

• Aligns with existing international, national, and industry standards

• Section 1 is adopted, sections 2-6 (implementation details) still in draft

CSDL conforms with the guidelines of ISO 27034

• Following CSDL is part of Cisco’s ISO compliance

• In 2013, Cisco used ISO/IEC 27034-1, as a baseline to evaluate CSDL.

  • “All current mandatory application security related policies, standards, and procedures along with their supporting people, processes, and tools meet or exceed the guidance in ISO/IEC 27034-1 as published in 2011.”
Security is Everyone’s Job
Accelerating to A Security Aware Culture
Cisco Security and Trust Spectrum
“Cradle to Grave”

Enterprise Security
Privacy and Data Protection

Security and Trust Built In

Design | Engineering | Manufacturing | Delivery / Deployment | Ongoing Operation

Cloud
Thank you.