

# Application Security

From Code to Cloud

Joe Cupano  
[consigliere@cupano.com](mailto:consigliere@cupano.com)

16 March 2011

---

---

---

---

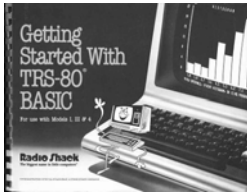
---

---

---

---

## Way back when . . .



---

---

---

---

---

---

---

---

## Way back when . . .



---

---

---

---

---

---

---

---



---

---

---

---

---

---

---

---

- Compute Stack
- Hardware
  - OS
    - DOS, OS/2, Win 3.1, System 6.X/7.X
  - Languages
    - Batch/Shell
  - Application
    - Input validation
  - Connectivity
    - None, Terminal Servers, Dial-up, Local LAN

---

---

---

---

---

---

---

---

- Early Threats (pre-Internet)
- Virus
    - Sharing Disks
    - Dial-up systems
    - Files across local LANs
  - Weak Passwords
  - Physical Security

---

---

---

---

---

---

---

---

**Today's threats to the Stack**

- Chips
  - Firmware
  - BIOS
- OS
  - Kernels, Libraries
  - Virtualization: Hypervisors
- Languages/Platforms
  - Interpreted, Compiled
- Application
  - Input validation
- Connectivity
  - LAN, WAN, 3<sup>rd</sup> Party, Internet

---

---

---

---

---

---

---

---

**Where does your "ROOT of TRUST" begin?**

---

---

---

---

---

---

---

---

**Information Security Concepts**

- Confidentiality
  - Prevent unauthorized disclosure
- Integrity
  - Prevent unauthorized modification
  - Non-repudiation
- Availability
  - BC/DR
  - SLAs

---

---

---

---

---

---

---

---

### Information Security Concepts (2)

- Authentication
  - Identity
- Authorization
  - Credentials
- Accountability
  - Logging, Trust but verify

---

---

---

---

---

---

---

---

### Information Security Concepts (3)

- Least Privilege
  - Need to know
  - Minimum amount of credentials to perform role
- Defense in Depth
  - Layered Security

---

---

---

---

---

---

---

---

### Risk Analysis

- Asset
  - What we are protecting
- Threat
  - What we are protecting against
- Vulnerability
  - Weakness exploited by threats
- Risk
  - Potential for loss/damage/destruction of an asset resulting of threat exploiting vulnerability
- Countermeasures
  - Efforts to reduce risk by addressing vulnerability and/or reducing threat opportunity

**RISK = THREAT x VULNERABILITY**

---

---

---

---

---

---

---

---

Where do we start?

---

---

---

---

---

---

---

---

**Threats**

- Input Validation
  - Buffer overflow, cross-site scripting, SQL injection
- Impersonation
  - Brute force, dictionary, eavesdropping, cookie and credential attacks
- Authorization
  - Privilege Elevation
- Change/Configuration Management
  - Privilege Elevation
- Key management & weak crypto
- OWASP Top Ten Web Application Security Risks 2010
  - [www.owasp.org](http://www.owasp.org)

---

---

---

---

---

---

---

---

**Mitigation**

- Vulnerability Scanners
- Static Code Analysis
- Penetration Testing
- Development Methods
  - NIST 800-14 “Generally Accepted Principles and Practices for Securing Information Technology systems”
  - NIST SP-800-64 Revision 2 “Security Consideration in the SDLC”
  - Microsoft SDL

**Use multiple tools for each category**

---

---

---

---

---

---

---

---

### NIST SP 800-14

- Prepare a Security Plan
- Initiation
  - Conduct a Sensitivity Assessment
- Development/Acquisition
  - Determine Security Requirements and incorporate controls and assurances
- Implementation
  - Testing of controls
  - Certification & Accreditation
- Operation & Maintenance
  - Security Operations, Assurance, Audit & Monitoring
  - Disposal

---

---

---

---

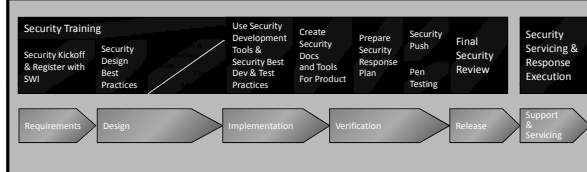
---

---

---

---

### Security Deployment Lifecycle Tasks and Processes



\* The Security Development Lifecycle - Microsoft

---

---

---

---

---

---

---

---

### Languages/Platforms

- Machine Code, Source Code, Assemblers
- Compilers, Interpreters, and Bytecode
- Object Oriented Languages

**Show Chain of Custody**

---

---

---

---

---

---

---

---

**Operating Systems**

- Proprietary and Open Source
  - Kernels, Libraries, and other re-usable objects
  - Patch Management, Updates
- End Point Security
  - Personal Firewall, Anti-Virus
- Virtualization
  - Platform catalogs

**Show Chain of Custody**

---

---

---

---

---

---

---

---

**Connectivity**

- Few Protocols
- Assume open network
  - LAN, WLAN, WAN, Internet, any
- Zones of Trust
- Federation

---

---

---

---

---

---

---

---

**Cloud**

- Software as a Service (SaaS)
  - Use provider's applications over a network
- Platform as a Service (PaaS)
  - Deploy customer-created applications on provider platform
- Infrastructure as a Service (IaaS)
  - "Rent" Compute/Storage/Network resources from provider
  - Virtual Data Center

---

---

---

---

---

---

---

---

### Hardware

- Required of certain entities
- Chips
- Adapter Cards
- Motherboards
- Storage
- All Associated BIOS and Firmware

**Show Chain of Custody**

---

---

---

---

---

---

---

---

### Questions?

Thank You!

Joe Cupano  
[consigliere@cupano.com](mailto:consigliere@cupano.com)

---

---

---

---

---

---

---

---