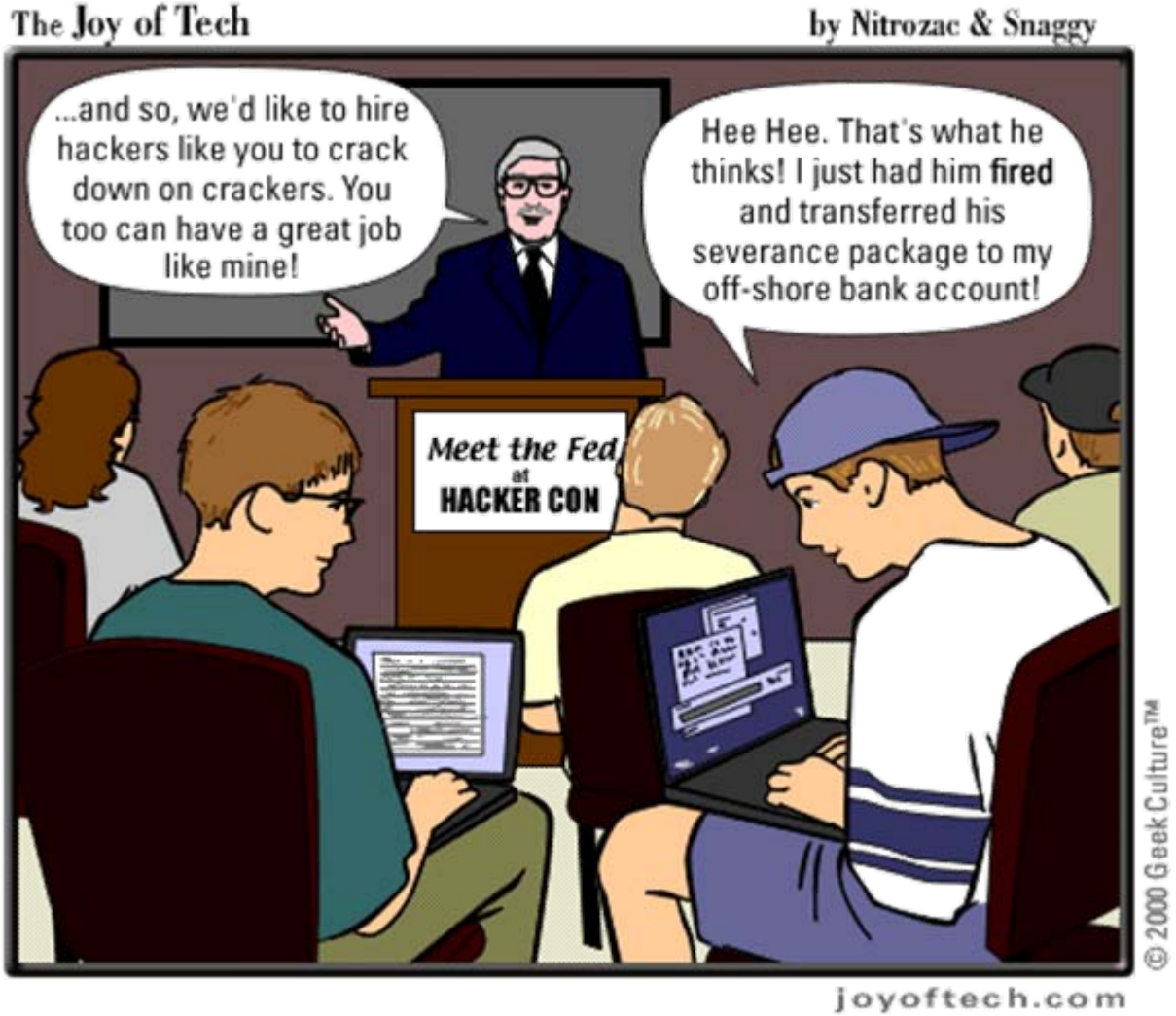
# Promoting Application Security within Federal Government


Dr. Sarbari Gupta, CISSP, CISA
Founder/President
Electrosoft
sarbari@electrosoft-inc.com
703-437-9451 ext 12


## AppSec DC

November 13, 2009

# Application Security is NOT A JOKE!




Courtesy of http://www.securitywizardry.com

Electrosoft

# Problem Statement

- Federal government takes information system security and assurance very seriously
- Focus areas for Federal security efforts include:
  - Platform Security
  - Network Security
  - Perimeter Security
  - Personnel Security
  - Physical Security
  - Acquisition Security, and so on ...
- *HOWEVER, APPLICATION SECURITY HAS RECEIVED MEAGER ATTENTION!!*

# Agenda

- Application Security Best Practices
- Federal IT Security Landscape
- Mapping AppSec Best Practices to FISMA
- Observations
- Wrap-Up

# Application Security Best Practices

- Application Security Training  for Developers/Managers
- Documented Secure Coding Standards
- Formalized SDLC Processes
- Application Threat Modeling
- Documented Security Design/Architecture
- Automated Security Testing
- Manual Code Review
- Vulnerability and Penetration Analyses
- Continuous Monitoring for New Vulnerabilities
  - OWASP Top Ten Vulnerabilities
  - SANS Top 25 Coding Vulnerabilities
  - NVD, Other lists ...

# Agenda

- Application Security Best Practices
- Federal IT Security Landscape
- Mapping AppSec Best Practices to FISMA
- Observations
- Wrap-Up

# Information Security – Federal Landscape

- Federal Practices in Information Security is driven by REGULATORY COMPLIANCE

- Compliance with What?
  - Title III of E-Government Act of 2002
    - Federal Information Security Management Act (FISMA)
  - Privacy Act of 1974
  - OMB Circular A-130, Appendix III
  - Homeland Security Presidential Directives
    - HSPD-7, HSPD-12, etc.
  - OMB Memos
    - FISMA Reporting
    - Privacy
    - Data Encryption
    - FDCC, etc.

# FISMA Documentation

- NIST Standards and Guidelines
  - FIPS 199 – Standards for Security Categorization of Federal Information and Information Systems
  - SP 800-37 Rev 1 – DRAFT Guide for Security Authorization of Federal Information Systems: A Security Lifecycle Approach
  - SP 800-53 Rev 3 – Recommended Security Controls for Federal Information Systems and Organizations
  - SP 800-53A - Guide for Assessing the Security Controls in Federal Information Systems

# NIST Special Pub 800-53 Revision 3

| ID | FAMILY | CLASS |
|---|---|---|
| AC | Access Control | Technical |
| AT | Awareness and Training | Operational |
| AU | Audit and Accountability | Technical |
| CA | Security Assessment and Authorization | Management |
| CM | Configuration Management | Operational |
| CP | Contingency Planning | Operational |
| IA | Identification and Authentication | Technical |
| IR | Incident Response | Operational |
| MA | Maintenance | Operational |
| MP | Media Protection | Operational |
| PE | Physical and Environmental Protection | Operational |
| PL | Planning | Management |
| PS | Personnel Security | Operational |
| RA | Risk Assessment | Management |
| SA | System and Services Acquisition | Management |
| SC | System and Communications Protection | Technical |
| SI | System and Information Integrity | Operational |
| PM | Program Management | Management |

- **Title**: Recommended Security Controls for Federal Information Systems and Organizations
- **Published:** August 2009
- **Approach**: Risk Management Framework
  - Categorize Information System
  - Select Security Controls
  - Implement Security Controls
  - Assess Security Controls
  - Authorize Information System
  - Monitor Security Controls
- **18 families** of Security Controls

# Agenda

- Application Security Best Practices
- Federal IT Security Landscape
- Mapping AppSec Best Practices to FISMA
- Observations
- Wrap-Up

# AppSec Best Practices – Map to FISMA Controls

| Application Security Best Practices | NIST 800-53 Rev3 Controls |
|---|---|
| Application Security Training for Developers/Managers | AT-3: Security Training<br>SA-8: Security Engineering Principles |
| Documented Secure Coding Standards | SI-3: Malicious Code Protection |
| Formalized SDLC Processes | SA-3: Life Cycle Support<br>SA-8: Security Engineering Principles<br>SA-13: Trustworthiness |
| Application Threat Modeling | RA-3: Risk Assessment |
| Documented Security Architecture | SA-5: Information System Documentation |
| Automated Testing | SA-11: Developer Security Testing<br>CA-2: Security Assessments |
| Source Code Review | RA-5: Vulnerability Scanning<br>SA-5: Information System Documentation |
| Vulnerability and Penetration Analyses | CA-2: Security Assessments<br>RA-5: Vulnerability Scanning |
| Continuous Monitoring | CA-7: Continuous Monitoring |

# OWASP Top Ten Vulnerabilities (2007) – Map to FISMA Controls

| OWASP Top Ten Vulnerabilities | NIST 800-53 Rev3 Controls |
|---|---|
| A1 - Cross Site Scripting (XSS) | SI-10: Information Input Validation |
| A2 - Injection Flaws | SI-10: Information Input Validation |
| A3 - Malicious File Execution | Not specified |
| A4 - Insecure Direct Object Reference | AC-3: Access Enforcement |
| A5 - Cross Site Request Forgery (CSRF) | Not specified |
| A6 - Information Leakage & Improper Error Handling | SI-11: Error Handling |
| A7 - Broken Authentication and Session Mgmt | SC-23: Session Authenticity |
| A8 - Insecure Cryptographic Storage | SC-13: Use of Cryptography |
| A9 - Insecure Communications | SC-9: Transmission Confidentiality |
| A10 - Failure to Restrict URL Access | AC-3: Access Enforcement |

# SANS Top 25 (1 of 3) - Insecure Interaction Between Components – Map to FISMA Controls

| Top 25 Coding Vulnerabilities | NIST 800-53 Rev3 Controls |
|---|---|
| CWE-20: Improper Input Validation | SI-10: Information Input Validation |
| CWE-116: Improper Encoding or Escaping of Output | Not specified |
| CWE-89: SQL Injection | SI-10: Information Input Validation |
| CWE-79: Cross-site Scripting | SI-10: Information Input Validation |
| CWE-78: OS Command Injection | SI-10: Information Input Validation |
| CWE-319: Clear-text Transmission of Sensitive Information | SC-9: Transmission Confidentiality |
| CWE-352: Cross-Site Request Forgery (CSRF) | Not specified |
| CWE-362: Race Condition | Not specified |
| CWE-209: Error Message Information Leak | SI-11: Error Handling |

# SANS Top 25 (2 of 3) – Porous Defenses – Map to FISMA Controls

| Top 25 Coding Vulnerabilities | NIST 800-53 Rev3 Controls |
|---|---|
| CWE-285: Improper Access Control (Authorization) | AC-3: Access Enforcement |
| CWE-327: Use of a Broken or Risky Cryptographic Algorithm | SC-13: Use of Cryptography |
| CWE-259: Hard-Coded Password | IA-5: Authenticator Management |
| CWE-732: Insecure Permission Assignment for Critical Resource | AC-3: Access Enforcement |
| CWE-330: Use of Insufficiently Random Values | Not specified |
| CWE-250: Execution with Unnecessary Privileges | AC-6: Least Privilege |
| CWE-602: Client-Side Enforcement of Server-Side Security | Not specified |

# SANS Top 25 (3 of 3) - Risky Resource Management – Map to FISMA Controls

| Top 25 Coding Vulnerabilities | NIST 800-53 Rev3 Controls |
|---|---|
| CWE-119: Memory Buffer Overrun | SA-8: Security Engineering Principles[1] |
| CWE-642: External Control of Critical State Data | SA-8: Security Engineering Principles[1] |
| CWE-73: External Control of File Name or Path | SA-8: Security Engineering Principles[1] |
| CWE-426: Un-trusted Search Path | SA-8: Security Engineering Principles[1] |
| CWE-94: Code Injection | SA-8: Security Engineering Principles[1] |
| CWE-494: Download of Code Without Integrity Check | SI-7: Software and Information Integrity |
| CWE-404: Improper Resource Shutdown or Release | SA-8: Security Engineering Principles[1] |
| CWE-665: Improper Initialization | SA-8: Security Engineering Principles[1] |
| CWE-682: Incorrect Calculation | SA-8: Security Engineering Principles[1] |

1 – Weak Mapping

# OWASP Application Security Verification Std 2009 – Map to FISMA Controls

| ASVS Security Requirement Areas | NIST 800-53 Rev 3 Controls | Coverage |
|---|---|---|
| V1 - Security Architecture Documentation | RA-3 | 1 of 6 |
| V2 - Authentication Verification | AC-2, AC-3, AC-5, AC-7, AC-11, AC-14, AU-2, IA-2, IA-5, IA-6, IA-8, SC-24, SI-3 | 12 of 15 |
| V3 - Session Management Verification | AC-11, SC-10, SC-23, SI-3 | 9 of 13 |
| V4 - Access Control Verification | AC-2, AC-3, AC-6, SI-3, AU-2 | 10 of 15 |
| V5 - Input Validation Verification | SA-8, SI-3, SI-10, AU-2 | 7 of 9 |
| V6 - Output Encoding/Escaping Verification | SI-3, SI-10 | 5 of 10 |
| V7 - Cryptography Verification | IA-5, SC-12, SC-13, SI-3, AU-2 | 6 of 10 |
| V8 - Error Handling and Logging Verification | SI-3, SI-11, AU-3, AU-9 | 7 of 12 |
| V9 - Data Protection Verification | | 0 of 6 |
| V10 - Communication Security Verification | AC-4, AC-6, IA-3, IA-5, SC-8, SC-9, SC-24, AU-2 | 7 of 9 |
| V11 - HTTP Security Verification | SC-23 | 1 of 7 |
| V12 - Security Configuration Verification | CM-5, SI-6, SI-7, AU-2 | 3 of 4 |
| V13 - Malicious Code Search Verification | SI-3, SI-7 | 2 of 2 |
| V14 - Internal Security Verification | SC-4, SC-28 | 2 of 3 |

# Agenda

- Application Security Best Practices
- Federal IT Security Landscape
- Mapping AppSec Best Practices to FISMA
- Observations
- Wrap-Up

# Observations

- NIST SP 800-53 Rev 2 had little or no support for Application Security practices
  - HOWEVER, NIST SP 800-53 Rev 3 has built a solid level of support for Application Security
- Application Security requirements are sprinkled
  - Difficult to assemble to form complete picture
- SP 800-53 Rev 3 could be further refined for AppSec
  - Specific recommendations for change to existing controls
  - Specific recommendations for new requirements

# SP 800-53 Rev 1 – Recommended Refinements (I)

- AT-3: Security Training
  - Require training for software developers/integrators
- CA-2: Security Assessment
  - Require Red Team exercises targeted at Software Applications
- CA-7: Continuous Monitoring
  - Require Red Team exercises at HIGH baseline
- CM-4: Security Impact Analysis
  - Explicitly require security impact analysis for software changes

# SP 800-53 Rev 1 – Recommended Refinements (II)

- IA-5: Authenticator Management
  - Require check for unencrypted authenticators in code/scripts at MODERATE and HIGH
- PL-2: System Security Plan
  - Require Enhancements (CONOPS, Architecture) at HIGH
- SC-23: Session Authenticity
  - Require enhancements for session ID management at MODERATE/HIGH
- SI-3: Malicious Code Protection
  - Promote guidance on secure coding and monitoring practices to control description section

# SP 800-53 Rev 1 – Recommended Refinements (III)

- SA-5: Information System Documentation
  - Reword to apply to custom developed software systems; currently slanted for vendor/manufacturer developed systems
  - Move enhancement related to code reviews to CA-3 or RA-5
- SA-8: Security Engineering Principles
  - Move guidance on security training for developers/integrators to AT-3
- SA-11: Developer Security Testing
  - Require enhancements for independent code analysis and vulnerability analysis at HIGH

# Sp 800-53 Rev 3 – Extensions/Additions

- Sensitive Resource Identification (Data, URLs, Config Files, etc.)
  - SC-28: Protection of Information at Rest
    - Expand scope to require explicit identification of sensitive information
- Conditioning of Output Content/Data
  - SI-12: Information Output Handling and Retention
    - Expand scope to include checking outputs for valid syntax/semantics
- Server-Side Implementation of Security Services
  - Add new control requiring Common, Non-circumventable Implementation of server-side security checks

# Agenda

- Application Security Best Practices
- Federal IT Security Landscape
- Mapping AppSec Best Practices to FISMA
- Observations
- Wrap-Up

# Wrap-Up and Final Thoughts

- Time to focus on Application/Software Security
- NIST SP 800-53 Rev3 provides excellent boost to AppSec within FISMA
  - Refinements/Extensions could further strengthen AppSec practice under FISMA
- Updates to SP 800-53A could strengthen AppSec Testing
- OMB mandate could provide added impetus to AppSec
  - Let's not wait for a catastrophic AppSec breach
  - A memo in time could save nine!

*QUESTIONS??*

# Application Security – Federal References

- DISA
  - Application Security and Development STIG – July 2008
  - Application Security and Development Checklist Version 2 Release 1.5 - June 2009
- NIST
  - SP 800-53 Rev 3 – Recommended Security Controls for Federal Information Systems and Organizations
  - SP 800-64 Rev 2 – Security Considerations in the System Development Life Cycle – Oct 2008
  - SP 800-115 (draft) - Technical Guide to Information Security Testing – Nov 2007
  - Security Content Automation Protocol (SCAP)