Collecting Industry Best Practices for Software Assurance (SwA)

David A. Wheeler

September 7, 2005

IDA

Outline

- Existing Best Practices information
  - MITRE Survey (4 March 2005)
  - Microsoft
  - Prescriptive/Menu sources
    - Common Criteria, SSE-CMM, FAA/DoD SSE, TSDM, CLASP, books
- Discussion
  - What are types/examples?
  - Who does them? Why? Sufficient?

MITRE Survey

- Industry attention in several areas matches DoD needs, should be closely monitored and opportunities for DoD collaboration encouraged at the highest levels
  - Defect reduction through static analysis, annotation/specification, test case generation and management
  - Autonomic computing and the implications of delegating authority to increasingly autonomous software
  - Education and training shortfalls
  - Application of embedded system safety techniques and virtual machine technology to broader classes of software and SwA
- Some tendencies in Industry are at cross purposes with DoD interests
  - Increasing "arms length" outsourcing focused on better control over specifications and resulting code
    - Doesn't address malicious code

Microsoft Security Development Lifecycle (SDL)

- Requirements: Consider security “up front”
- Design: Architecture/design guidelines (inc. least privilege), doc. attack surface, threat models, supplemental ship criteria
- Development: Coding/testing standards, fuzz testing, static analysis tools, code reviews
- Verification: “Security push” for new and legacy code
- Release: Final Security Review (FSR)
- Final Security Review (FSR) Response
- Support/Service: Respond, adapt processes

Implementation: SDL mandatory; education mandatory; metrics; central security team

Results: Vast decrease in #security bulletins in same time period

http://msdn.microsoft.com/security/default.aspx?pull=/library/en-us/dnsecure/html/sdl.asp

Common Criteria

- "Common Criteria" (ISO/IEC 15408) defines selectable set of security functions & security assurance measures
- Evaluation Assurance Levels (EAL 1-7) group assurance measures
  - Configuration Management, delivery & operation, development, guidance documents, life cycle support test, vulnerability assessment
- Users specify requirements in "Protection Profiles"
- Suppliers specify what they do in "Security Targets"
- Focus on security products, not general products
- Much effort in evaluation of evidence (documentation)
  - Higher levels increase testing & vulnerability analysis
  - Highest levels involve proofs of models
- Presume no intentionally malicious code
  - Vendor provides all evidence
- Version 3 upcoming

Systems Security Engineering CMM (SSE-CMM)

- Focused on IT security system requirements
- Security Base Practices:
  - Administer Security Controls, Assess Impact , Assess Security Risk, Assess Threat, Assess Vulnerability, Build Assurance Argument, Coordinate Security, Monitor Security Posture, Provide Security Input, Specify Security Needs, Verify and Validate Security
- Project/Org Best Practices:
  - Ensure Quality, Manage Configurations, Manage Project Risk, Monitor and Control Technical Effort , Plan Technical Effort , Define Organization's Systems Engineering Process, Improve Organization's Systems Engineering Processes, Manage Product Line Evolution, Manage Systems Engineering Support Environment, Provide Ongoing Skills and Knowledge, Coordinate with Suppliers

http://www.sse-cmm.org

FAA/DoD Safety and Security Extensions for iCMMs (SSE, "16 practices")

- Goal 1. An infrastructure for safety and security is established and maintained.
  - Ensure Safety and Security Competency; Establish Qualified Work Environment; Ensure Integrity of Safety and Security Information; Monitor Operations and Report Incidents; Ensure Business Continuity
- Goal 2. Safety and security risks are identified and managed
  - Identify Safety and Security Risks; Analyze and Prioritize Risks; Determine, Implement, and Monitor Risk Mitigation Plan
- Goal 3. Safety and security requirements are satisfied
  - Determine Regulatory Requirements, Laws, and Standards; Develop and Deploy Safe and Secure Products and Services; Objectively Evaluate Products; Establish Safety and Security Assurance Arguments
- Goal 4. Activities and products are managed to achieve safety and security requirements and objectives.
  - Establish Independent Safety and Security Reporting; Establish a Safety and Security Plan; Select and Manage Suppliers, Products, and Services; Monitor and Control Activities and Products

FAA/DoD work; see http://www.faa.gov/ipg

Trusted Software (Development) Methodology (TSDM, TSM, TCMM)

- SDIO-created, vs. malicious developers & unreliable sw
- 5-level (T1..T5) increasing rigor, e.g.:
  - T1: Peer review of all requirements, design, source code, tests; placed under CM prior to review
  - T2: CM must be able to determine modification history
  - T3: Code analysis by tools, limited peer review rates
  - T4: Two-person knowledge/responsibility for each component
  - T5: Formal methods to specify/verify requirements/ design/ implementation
- Categories & Principles:
  - Management Policy: Planning, risk mgmt, security policy, reuse integrity, prototyping, shared knowledge
  - Environment Controls: CM, I&A, auditing, access control
  - Environment Management: Admin, integrity, intrusion detection, trusted distribution
  - Software Engineering: Standards, doc, traceability, peer review, formal review, CASE tools, code analysis, testing approach/responsibility, reliability engr, formal methods

TSM Fife et al. Survey

- IDA papers P-2829 and P-2999, April 1993
  - Surveyed 15 organizations vs. TSM
  - 5 DoD contractors, 5 TCSEC, 5 commercial
- Commercial/TCSEC similar to T1
- DoD contractors close to T2 because of DoD-STD-2167A (now abandoned)
- Feedback: Not concerned with insider threat, reuse, cost, too many standards

CLASP

- CLASP: Comprehensive, Lightweight Application Security Process
- Developed by Secure Software
- Process guide that helps organizations incorporate security into their application development lifecycle
- “Menu” to be selected into process

Books

- **Design/implementation books:**
  - **[Howard 2002] Howard, Michael and David LeBlanc. 2002. *Writing Secure Code*. Redmond, Washington: Microsoft Press.**
  - **[Wheeler 2003] Wheeler, David A. *Secure Programming for Linux and Unix HOWTO*, March 2003. http://www.dwheeler.com/secure-programs/**
  - **[Viega 2002] Viega, John, and Gary McGraw. 2002. *Building Secure Software*. Addison-Wesley.**
  - **Draft DISA Application Development STIG (unpublished)**

Discussion Time!

- Please propose/discuss:
  - What are the types of best practices?
  - What are examples of each?
  - Who does them (or not)?
  - Why (or why not) do they do them?
  - Are they sufficient for industry? DoD?
  - Are these general? Contra-indicators?
  - How could others be motivated to do them?
- Goal: A collection of these answers