Modern Threats
2014
SOFTWARE
SYMPOSIUM
Modern Solutions

Agile Development in Support of DoD Information Assurance

THE VALUE OF PERFORMANCE.
NORTHROP GRUMMAN

April 1, 2014

Keith Conway

Software Engineer

Unclassified

Acknowledgements

- Max Padilla
- David Loring
- Devang Parekh
- Richard Schlarb
- Frank Fullen

Introduction

- Cyber security is a growing industry for a reason

- If the DoD is going to buy a product to connect to a network the DoD has be sure the product is not going to contaminate the network.

- IA (Information Assurance) is a science because of the gray area – not black and white
  - We want to take as much of the science out and make it a process – standardization

- Need to secure a system with fewer resources and a constrained schedule

Agenda

- C&A – Certification and Accreditation
- Information Assurance Areas
  - Hardware
  - Network
  - Physical
  - Software
  - Database
  - Documentation
- Agile Development
- Agile in Support of DoD IA

The End Goal – C&A

- DD250 – The Gov't buys your product
- ATO – Authority to Operate
- IATT – Interim Authority To Test
- DAA – Designating Accrediting Authority
- DAA Rep – Designating Accrediting Authority Representative

Information Assurance (IA) Areas

- Hardware
- Network
- Physical
- Software
- Database
- Documentation

Hardware - Windows

- WASSP – Windows Automated Security Scanning Program
  - XP, 2003, Vista, Win7, Win2008
  - Generic tool to look for known vulnerabilities in Windows O/S.
  - Vulnerability levels: High, Medium, Low, Unknown
  - Group Policy Objects (GPO's) from Domain Controller on Server (Win2008 R2) to push security to domain members

Hardware - SECSCN

- SECSCN – Security Scanner
  - Solaris 2.6 – 9 (SPARC), Solaris 10, Red Hat Enterprise Linux 4 – 6, Mac OS X v10.6
  - Generic tool to look for known vulnerabilities in UNIX O/S.
  - Vulnerability levels: High, Medium, Low, Unknown

Hardware - Patching

- Patch O/S
- Patch products: COTS and GOTS
  - Custom built software
  - Database: SQL Server, Oracle, PostgreSQL, MySQL
  - Web Server
  - Virus Definitions
- What is the cycle for patching? Once a year, twice a year, quarterly
- What about site specific critical patches?

Hardware - Image

- We want a hardware image with a CM (Configuration Mgmt) version number
    - O/S is hardened
        - Files are removed
        - Services are turned off
        - Patches are up to date
        - Work that is not part of the GPO’s

Network

- Network devices must be hardened
  - Switch, router, firewall, KVM, NTP, printers
    - Verify default passwords have been changed
    - Verify strong passwords are used
    - Verify logging / auditing is enabled
    - Verify that high risk services like TELNET and / or FTP are not turned on
    - Verify SSH v2 is used
    - Disable web interface
    - Enable NTP

Physical

- Gates / Guards / Dogs / Guns
- Access to Servers
- USB enabled?
- CD burner enabled?
- Location of different security caveats: Unclassified, Secret, Top Secret
  - What is the separation required
- Labeling of physical devices: hard drives, monitors
- Color coding of network cabling

Software – STIG's

- DoD STIGs (Security Technical Implementation Guidance)
  - http://iase.disa.mil/stigs/
  - This guidance is generic but valuable because of the breadth of DoD programs that have contributed to the STIGs
  - Vulnerability levels: CAT I, CAT II, and CAT III
    - CAT I is the highest with CAT III the lowest

Software

- Strong passwords – we have O/S users, Active Directory users, database user, and network device users
  - Do we enforce the same strong passwords (password complexity) everywhere?
- AAA – Authentication, Authorization, Accounting
- RBAC – Role Based Access Control
  - Once a user is authenticated what are they authorized to do – least privilege. Roles can be assigned to a user or a group.
- Encryption – HTTPS, LDAPS, SSL
- Logging – this is part of the accounting for AAA
  - We want to know who did what
- Secure System Files – We need to identify files which are important and protect them. Configuration and logging files should be protected.

Software – Secure Coding

- Secure coding standards – a guideline needs to be developed which is enforced / followed by developers

- Peer review before check-in

- Static code analysis
  - Checks code for known vulnerabilities
    - Grouped by severity and category
    - Because tools are generic you have to understand which categories pertain to your systems
  - Process to run static code analysis and enforce

Database

- Depending on your database you will have a manual STIG to follow or a scan
  - Vulnerability levels: CAT I, CAT II, and CAT III
  - AAA Authentication, Authorization, Accounting
    - Disable default users
    - Change default passwords – enforce strong passwords
    - Audit on security relevant events
  - Protect security relevant files:
    - Audit data
    - Configuration files

Documentation

- Certification and Accreditation package
- Test Procedure Document – what have you secured and does it work
- SSP – System Security Plan
  - Followed by IAM (Information Assurance Mgr)
- Patch Mgmt schedule
  - Once a system is delivered how will it be maintained – extremely important for security to include OS patches as well as COTS updates.
- Back up and recovery
- Passwords – expiration schedule and location

Agile Development

- Sprint
- Cross functional team
- Product backlog
- Sprint backlog
- Daily standup
- Sprint demonstration
- Velocity

Agile - Sprint

- Unit of time accomplish work
  - 3 to 5 weeks
- Should have a potentially shippable product at end of sprint
- Requirements
- Design
- Code
- Test

Agile – Cross Functional Team

- Programmers, testers, user experience, DB’s, ..
- If a task involves a modification to a user interface then you could possibly need the following skill sets on your team:
  - Requirements
  - Programming
  - DB
  - UI
  - Test
  - Installation
  - Documentation

Product Backlog

- This is work that needs to be accomplished
- Scrum Masters, Product Owners, team members can create tasking to be placed in the product backlog.
- The product backlog does not specify how to do the work – only identifies the work
- Could be identified up front, along the way, or a mix of the two
- As you are working you will see areas for work – put in the backlog

Sprint Backlog

- Highest priority work
  - Taken from the product backlog
  - Brought in by the product owner
- When you sign up for work from the sprint backlog you are signing up to finish that work in the sprint timeline
  - If too much work to finish in one sprint them modify task
- Try not to change priorities during sprint
  - Newly identified work can be accomplished following sprint
- Minimize pop-ups

Daily Standup

- Daily
- 15 minutes
- Same time / same place
- Not for solving problems
- Answer the following three questions
  - What you did yesterday
  - What you are doing today
  - Any issues

Sprint Demonstration

- A demonstration of the work that was accomplished during the sprint
- Invite the stake holders
  - This helps everyone see progression and make sure on the right track
- If there are issues it will make them visible so they can be fixed

Agile in support of DoD IA

- Product backlog
  - Shows work that has been accomplished
  - Shows outstanding work – by priority
    - Can get stakeholder concurrence on backlog and priority
    - Can get mgmt approval – resource / schedule
  - Can keep scope creep in check

Agile in support of DoD IA

- Resource constraints
  - Lab assets
  - Testers
  - Documentation
  - Engineers: programmer, DB, network, hardware
- Work the items from the product backlog that you have resources for
  - High priority items are visible every month – this will keep them on mgmt radar

Summary

- Information Assurance Areas
  - Hardware
  - Network
  - Physical
  - Software
  - Database
  - Documentation
- Agile in Support of DoD IA
- C&A – IATT / ATO / DD250

THE VALUE OF PERFORMANCE.

NORTHROP GRUMMAN

Author Biography

- 11+ years as a software engineer
  - Enterprise Architecture, SOA, Web Services (SOAP, REST), JMS

- 5+ years securing systems
  - Emphasis is on software security

- Relevant Certificates Related to Security
  - CEH – Certified Ethical Hacker
  - CISSP – Certified Information System Security Professional
  - SSCP – System Security Certified Practitioner
  - Security+
  - Network+
  - CCENT
  - Java Programmer

Abstract

- Mission Systems IPT has been using an agile development methodology in support of DoD IA. We understand that gaining an ATO (Authority To Operate) is crucial to the success of a program.

- The Agile methodology is a way to identify needed work, schedule the work properly, and keep track of work that has been accomplished. We have identified the following areas in support of Agile and DoD IA.
  - Hardware
  - Network
  - Physical
  - Software
  - Database
  - Documentation