COTS PRODUCT SECURITY EVALUATION
Richard C. MacVarish, CISSP, IAM/IEM
EDS U.S. Public Sector
Why are we here?

• COTS software use is increasing rapidly
• COTS product assurance levels are in question
• Common Criteria may be insufficient to meet your needs
  – Are you using the same protection profile as the CC evaluation?
  – Common Criteria serves a different purpose
• Assurance is moving into the acquisition lifecycle
  – Assurance must extend beyond vendor SDLCs questionnaires
  – How will you validate the COTS product meets criteria?
  – How will you define your COTS delivered product criteria?
• Security defects in COTS introduce significant risk
  – Breaches
  – Patching and maintenance
The end game

• A data driven security evaluation process for COTS products
  – Criteria specific to your data
  – Testing specific to your environment
• Identification and reduction of COTS product introduced risk
  – Proper evaluation will expose defects in design and implementation
  – Provides metrics for risk management strategies
    • Avoid, reduce, transfer, retain
COTS

- Commodity off the shelf
  - COTS
  - Internals non-modified
  - Intellectual property retained by vendor
  - Vendor maintained, supported and enhanced
  - Sold, leased or licensed to the public for profit

- “COTS-ish”
  - Embedded
  - Middleware
  - Modifiable COTS
  - Freeware / shareware
  - Non-vendor supported open source
Assurance

- Assurance
  - Measure of confidence

- Software assurance
  - Integrity
    - Confidence level data cannot be modified without authorization
  - Reliability
    - Confidence level software will continue to processed data correctly
  - Availability
    - Confidence level data will be available when it is needed
  - Serviceability
    - Confidence level that software is maintainable
  - Confidentiality assurance
    - Confidence level that data cannot be disclosed without authorization
Performing an evaluation

- PICAR Process
  - Plan evaluation
  - Identify criteria
  - Collect data
  - Analyze data
  - Report findings
Phase 1: Planning the evaluation

- Form the evaluation team
  - Technical and domain subject matter experts
  - Business and contract subject matter experts
  - Regulatory subject matter experts
  - Security subject matter experts
  - Stake holder representatives

- Create a charter
  - Formal or informal
  - Scope of the evaluation
  - Mission and goal statement
  - Team members and responsibilities
  - Statement of preexisting decisions and constraints
  - Statement of commitment from evaluators and management
Charter example

<table>
<thead>
<tr>
<th>Scope</th>
<th>Product X enterprise security server and access gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>Goal</td>
<td>Go/No go security evaluation based upon data defined criteria</td>
</tr>
<tr>
<td>Team</td>
<td>Alice and Bob are evaluators. Charlie is sole decision maker.</td>
</tr>
<tr>
<td>Preexisting conditions</td>
<td>Successfully passed functional testing. Must meet NERC. Users want it and don’t care about security evaluation.</td>
</tr>
<tr>
<td>Commitments</td>
<td>Evaluators will collect and analyze data in one week. Draft report due mid week two. Final report end week two.</td>
</tr>
</tbody>
</table>

• Do not underestimate the importance of this step
  – Missed deadline, team miscommunications, poor deliverables, etc
• Formality can increase from here
Phase 2: Identify criteria

- PICAR is a data driven methodology
- Data elements
  - A discrete data that will be processed in the software
  - The fundamental building blocks of a security evaluation
- Data taxonomy
  - A classification system based on data properties and attributes
    - PII, PHI, Classified, CUI, MAC, etc
    - NIST, PCI, FISMA, HIPPA, DISA, organizational, etc
    - Listen to your subject matter experts
- Security requirement
  - Derived from the taxonomy
- Security capability
  - A clearly measurable capability needed to meet the requirement
Data elements

- Primary Account Number
- Username
- Social Security Number
- Satellite Image
- Date of Birth
- Address
- Password
- GPS Coordinate
Data taxonomy

NERC
- Data Element
  - Username
- Data Element
  - Password

PII
- Data Element
  - Social Security Number
- Data Element
  - Address

Classified
- Data Element
  - Satellite Image
- Data Element
  - GPS Coordinates

PCI
- Data Element
  - Date of Birth
- Data Element
  - Primary Account Number
Requirements and criteria

Data Elements
- Username
- Password

NERC CIP-004
The Responsible Entity shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.

Evaluation Test Criteria
- Capability Statement: Can responsible entity revoke access in 24 hours using this software?
- Measurement: Does the target provide this capability? Can this capability be bypassed?

NERC CIP-007
Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.

Evaluation Test Criteria
- Capability Statement: Can responsible entity implement a tech control for AAA using this software?
- Measurement: Does the target provide this capability? Can this capability be bypassed?
Phase 3: Collecting target data

- Vendor questionnaires
  - SDLC methodologies, outsourcing, ownership
- Vendor documentation and manuals
  - A great place to start for vendor claims
- Previous reviews and benchmarks
  - Typically more functional but can bear fruit
- Internet research
  - Often a gold mine
- Lab testing
Lab testing

• COTS software is non-trivial, lab testing will be required to:
  – Verify vendor claims
  – Identify assumptions made by product
  – Determine the security posture in production context
    • Integrity, Reliability, Availability, Serviceability, Confidentiality

• Levels of testing
  – Test beds
    • Ideally the lab is a production test bed used for system testing
  – Prototype
    • Small scale deployment can be used for effective product testing

• What’s done in the lab?
  – Test case creation, fault injection, stress testing, boundary testing, etc
Lab testing

- Scenario based test cases
  - Drives directly after the capability statement measurement
- 5 step process scenario based evaluation
  - Isolate a particular measurement and create a scenario
  - Define specific test cases for the scenario
  - Create simulated environment
  - Perform test cases
  - Record result
Scenario

- Capability statement
  - Target must provide AAA
- Measurement
  - Is AAA implemented?
  - Can AAA be bypassed?
- Scenarios
  - Traffic sniffing
- Test case
  - Can credentials be sniffed?
- Result
  - Yes/No
Phase 4: Analyzing Data

• Consolidate data
  – Translate data into useable information

• Gap analysis matrix of results
  – Criteria – Yes / No matrix
  – Direct way to isolate areas of strength/weakness

• Strive to remove bias
  – Often early results temper further findings
### Gap analysis

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Does Target Provide AAA</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Can target revoke access in 24 hours</td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>
Phase 5: Reporting

• Report
  – Summary
  – Recommendation
  – Evaluation findings
  – Evaluation activities
  – This document is the primary deliverable

• Evaluation Log
  – This document tracks the evaluation process
  – Provides information about steps performed
  – Team member skills and roles
  – Level of effort expended

• Product Dossier
  – Repository for all supporting material
  – Discovered or generated facts, etc
  – Interpretations of those facts
A few final notes

• Cost is often sited as prohibitive for independent evaluation
  – We aren’t talking about the common criteria process
  – We are talking about independent validation against your criteria

• Much of this work is leveraged
  – You are performing data classification before you buy right?
  – You are identifying data security requirements before you buy right?

• Some of this work is already being performed
  – We just formalize it a little bit and do it before product selection

• A data driven process to define criteria allows you to:
  – Measure, compare and reduce risk introduced by COTS
  – Evaluate software based on your organizations security needs
Questions / Comments