



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

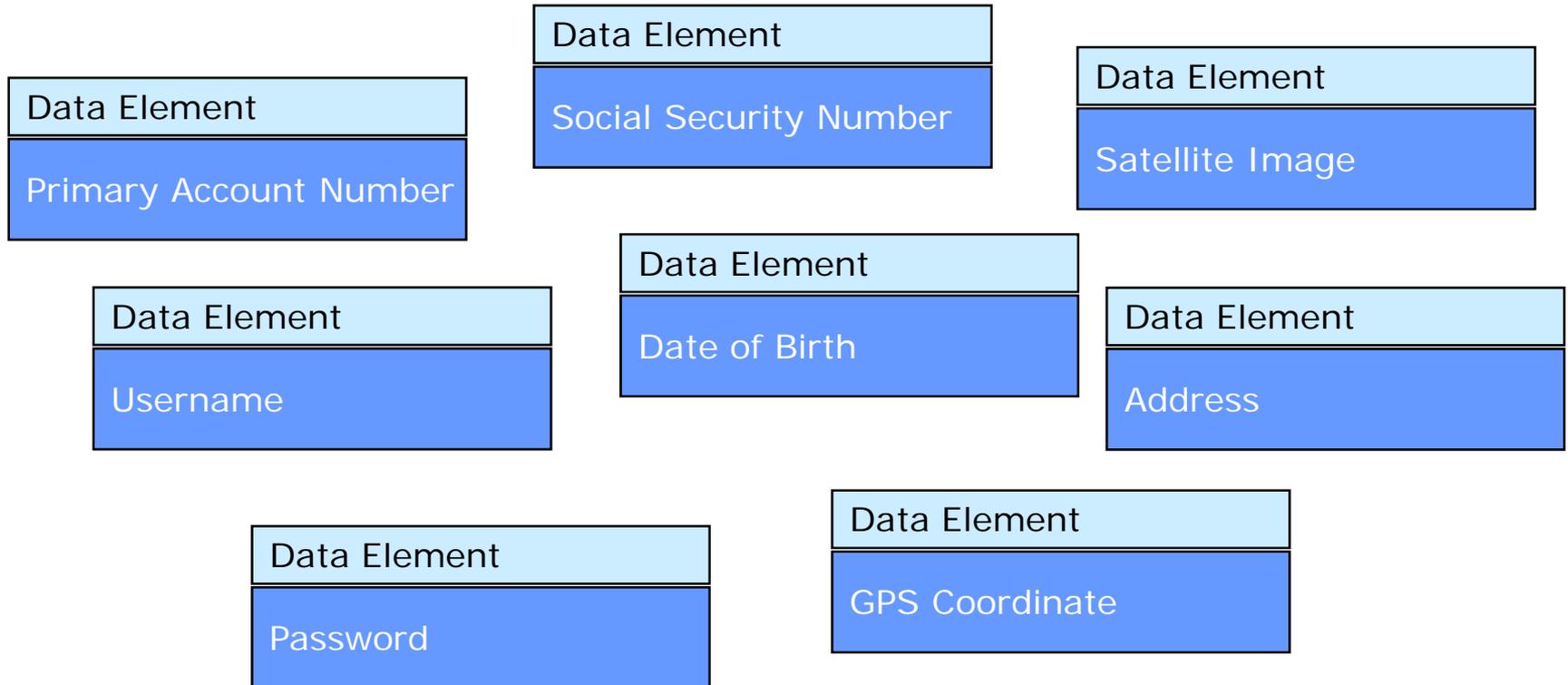
Scope	Product X enterprise security server and access gateway
Goal	Go/No go security evaluation based upon data defined criteria
Team	Alice and Bob are evaluators. Charlie is sole decision maker.
Preexisting conditions	Successfully passed functional testing. Must meet NERC. Users want it and don't care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

- Do not underestimate the importance of this step
 - Missed deadline, team miscommunications, poor deliverables, etc
- Formality can increase from here

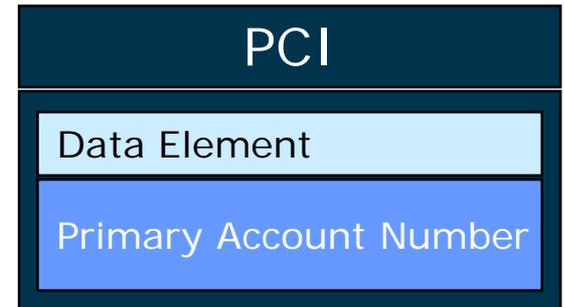
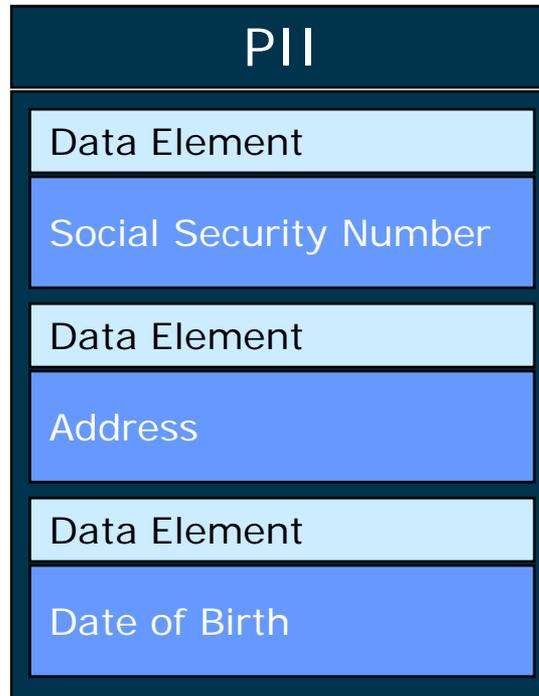
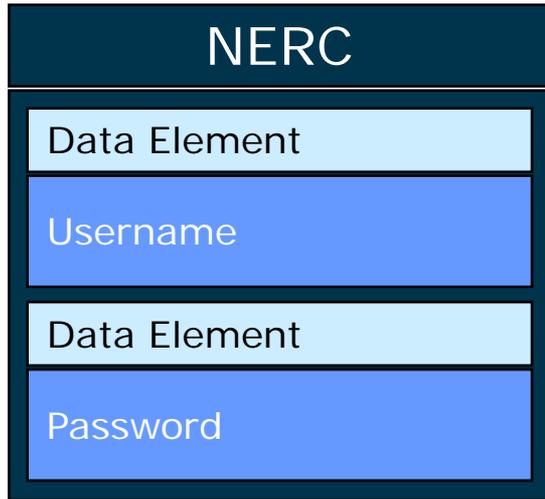
Phase 2: Identify criteria

- 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

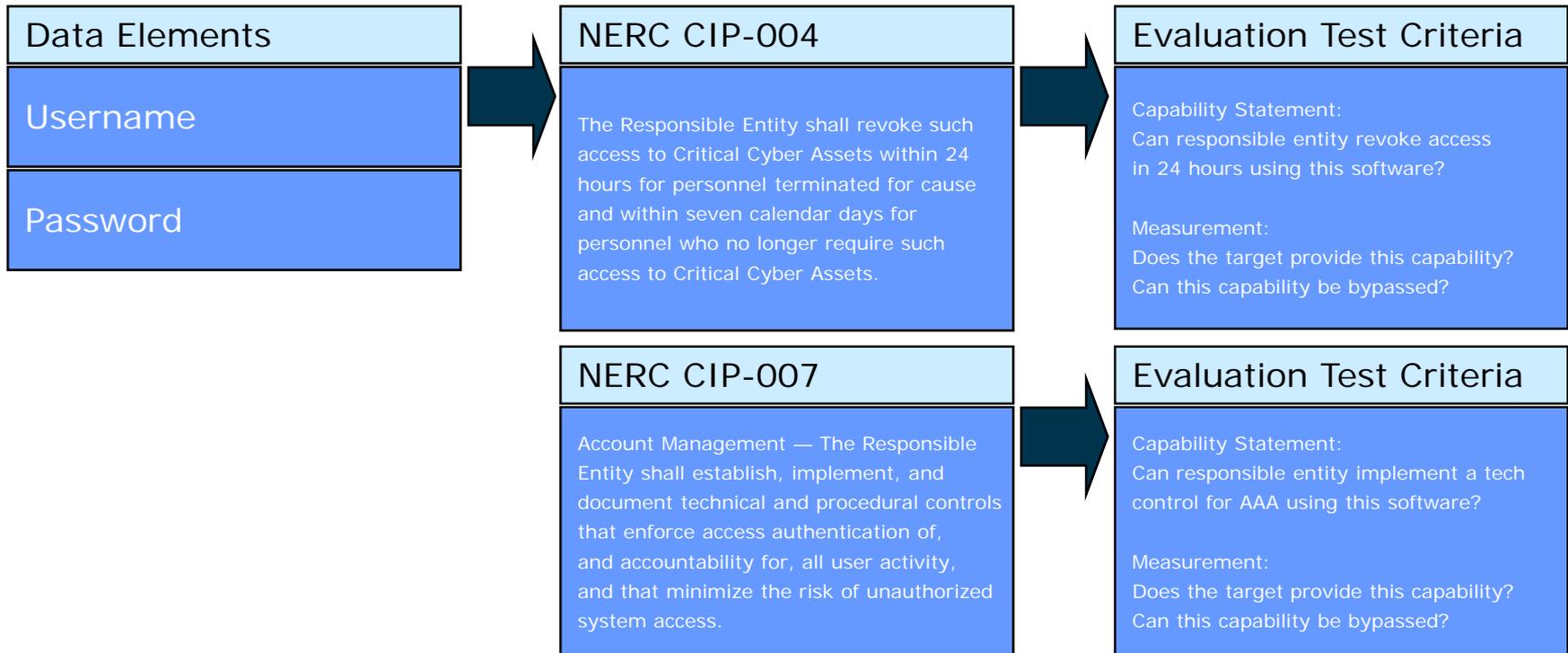
Data elements



Data taxonomy



Requirements and criteria



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

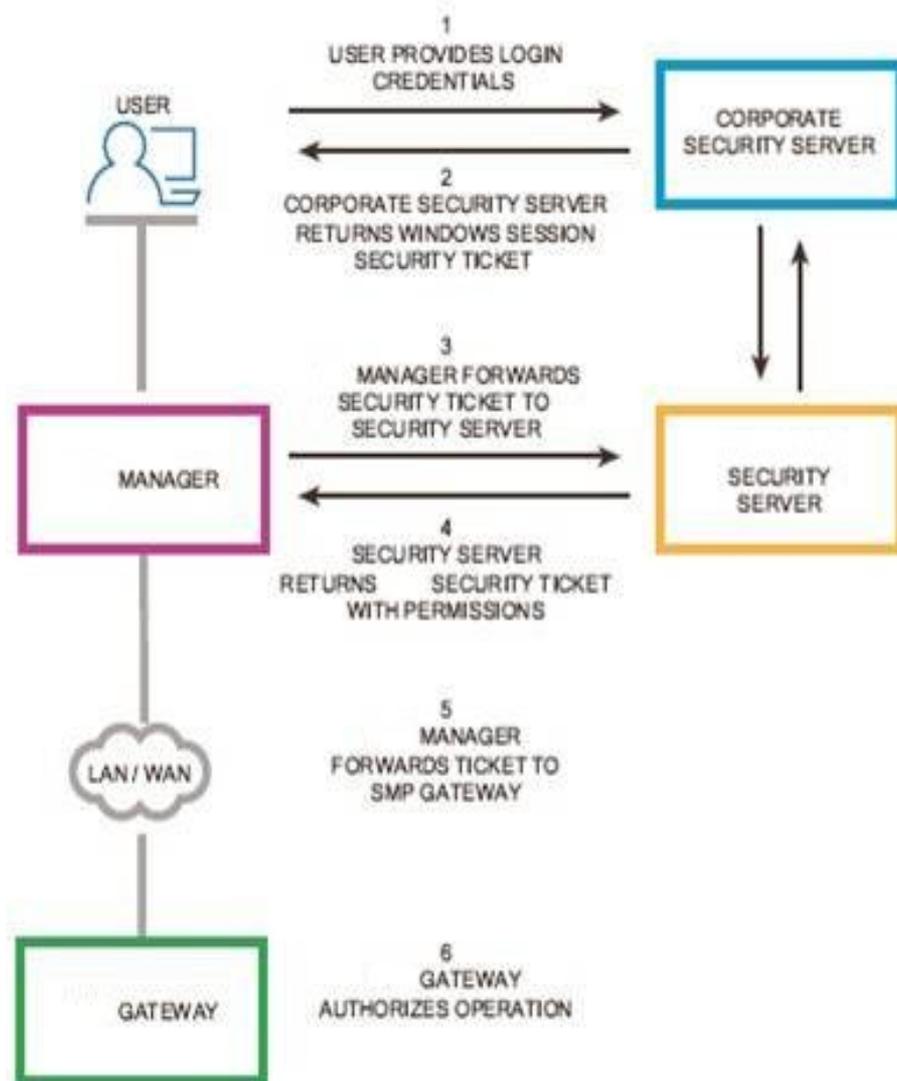
- COTS software is non-trivial, lab testing will be required to:
 - Verify vendor claims
 - Identify assumptions made by product
 - Determine the security posture in production context
 - Integrity, Reliability, Availability, Serviceability, Confidentiality
- Levels of testing
 - Test beds
 - Ideally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

	Yes	No
Criteria		
Does Target Provide AAA		X
Can target revoke access in 24 hours		X

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 cited 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

EDS
5400 Legacy Drive
Plano, TX 75024
Richard.MacVarish@eds.com

EDS and the EDS logo are registered trademarks of Hewlett-Packard Development Company, LP. HP is an equal opportunity employer and values the diversity of its people. ©2008 Hewlett-Packard Development Company, LP.

Behind success there's

