Simplifying Complex Security Assessments

Dr. Robert W. Baldwin
Plus Five Consulting, Inc.

Baldwin@PlusFive.com

Outline

- Goals vs. Reality in Assessments
- Case Study: Secure Distributed Application Execution Platform
- Relevant & Missing Security Criteria
- Decomposition & Layering
- Limitations of Assessments
- Benefits of Assessments

Goals of Assessments

- Proof the Product is Secure
- Product Ensures the Integrity of the System
- Product Enforces Access Policy
- No Way to Circumvent the Policy

Realities of Assessments

- Few Relevant Assessment Criteria
- Never Enough Time for Custom Assessment
- Hard to Formally State “Security Criteria”

Case Study: InfoScape Product

- Powerful Trusted Computer Uses PC for I/O, Network, Bulk Storage
- Biometric Authentication
- Small Trusted User Interface
- Large Persistent Memory
- Multiple Separate Application Domains
- Application Control Infrastructure

Layers of Functionality

- Application Development Platform
- Secure Domain Enrollment and Setup
- Domain Specific Applications and Data
- Policy Based Access Controls
- Infrastructure for Auditing & Escrow
- Secure Communication and RPC

Layers of Functionality

- Cryptographic Protocols for Communication and Life Cycle Steps
  - Enroll Device, Register User, Download Applications, Manage Access Controls, Remote Method Calls, etc.
- Biometric Authentication
- High Performance Encryption and Integrity Verification Algorithms
- Attack Resistant Hardware
  - Passive, Internal, and Active

Relevant and Missing Criteria

- FIPS-140: Crypto Module
- Common Criteria: Trusted OS
  - No Profile for Domain Separation
- Missing Criteria for Authentication, Protocols and Infrastructure Services
- Many Cryptographic Standards
  - SSL, S/MIME, X9.17, etc.
  - Most Irrelevant to This Device

Formal Security Criteria

- FIPS-140 version 2
- Levels of Assurance for Software and Hardware
- Compliance for Algorithms & Key Management
  - 3DES, AES, SHA1, HMAC-SHA1
  - RSA, DSS
  - PRNG with FIPS-186 Appendix 3.1
- Better Algorithms May Not Be Allowed
  - RSA, ECC, AES, HMAC

FIPS-140-2 Process

- Hire Consultant to Write Documents for Low Level, and Assist in Design for High Levels
  - Acts as Your Defense Attorney
- Hire National Certification Lab
  - Acts as Prosecutor for the State
- Submit Results to Government
  - Acts as Judge

Formal Security Criteria

- Trusted Operating Systems, Databases, Networks:
  - Orange, Red and other Rainbow Books
  - Common Criteria
- Common Criteria Profiles for:
  - Smart Cards
  - OS with Discretionary Access Controls
  - OS with Mandatory Access Controls
  - No Profile For This Type of Device

Common Criteria Process

- Hire Team Familiar With Process
- Fulltime Work Upfront and Ongoing
- Hire National Certification Lab
- Large Amount of Negotiation
- Very Long Process

Recognized Security Standards

- No Evaluation Criteria or Certification Labs
- Must Check Appropriate and Correct Use
  - SSL/TLS, SSH, IPSec
  - S/MIME, PGP, PKCS #7, PKCS #15
  - X9.17, X9.42, etc.
  - Signed XML, SHTTP
  - SNMP v3, Radius, Kerberos

Missing Security Standards

- Secure Application Development Platform
  - OS, Network and File System, Remote Services
  - Web Servers, Databases, Access Policies
- Programming Language
  - Java and Ada

Missing Security Standards

- Record and File Encryption
- Creating and Using Audit Records
- Key Storage, Key Recovery,
  Control Use Of Recovered Keys
- Authentication & Biometrics
- Tempest (Hardware Level Attacks)

Missing Cryptographic Standards

- Very Fast, Key-Agile, Cipher for High Throughput and Transaction Rates
- Very Fast Public Key, Small Public Key
  - NTRU
- Tiny Code Size, Tiny RAM, Low Power
  - XTEA, Skipjack, RC4

Evaluating Custom Security

- State Objectives
- Must Link Objectives to Higher Goals
- Hire Layer Expert
- Correct and Appropriate Use of Standards?
- Sound Engineer Discipline/Approach for Custom Mechanisms?

New Cryptography

- Hard to Get Experts Interested
  - Always Find Some Area of Concern
- Can Take Decades for Academic Consensus
  - NIST: DES, SHA1, DSS and AES
- Can Skip Academic Consensus
  - GSM's A5 cellphone encryption -- Disaster
  - IEEE 802.11 With RC4 & CRC -- Disaster
  - RSA, MD5, RC4 -- Good
  - Netscape's SSL (v3+) -- Good
  - Sony's M6 for DRM -- Maybe
  - Intel's DTCP Video for DRM -- Maybe

Decomposition & Layering

- What must I assume about the lower layer to convince myself this layer works?
  - Write These Down!
- Ex: Crypto Layer Assumes that Hardware Layer Resists Passive and Active Attacks
- Usually Need Upward Signaling
  - Indicate When Hardware Attacked.
- Examine Internal (Same-Layer) Attacks

Layering Problems

- Lower Layer Discovers New Assumption About Upper Layer Behavior
- Upper Layer Creates New Assumption on Lower Layer Security
- Layer Integration: Check Upward and Downward Assumptions

Limitations of Assessments

- Compliance to FIPS-140 or Common Criteria Appears Deterministic
  - Actually Many Fine Points Get “Argued”
- Assessment Evaluations Always Find Something to Improve
  - Clear Objectives Help
  - Must be Driven Top Down to Match Higher Level Goals

Limitations of Assessments

- Limited Time and Lack of Formal Process means that Results are “Best Guess”
- Buying “Reputation Credit” from Independent Expert
- Can Loop on Breaking and Improving
  - Loss of Independence for Expert

Overall Benefit of Assessments

- Required in Some Markets (FIPS-140)
- Helps with Funding and Marketing
  - Gain Reputation Capital from Experts
- Avoid Silly Mistakes
- Discipline of Preparing for Assessment Improves Quality

Questions?

- Baldwin@PlusFive.com