Superior Products Through Innovation

COTS, Subversions, and the Foreign Supply Chain issues for DoD Systems

Advanced Development Programs

Dr. Ben A. Calloni, P.E.

Lockheed Martin Fellow, Software Security

Research Program Manager and Principle Investigator

Introduction

- ***There is no perfect security!!!***
- ***Only levels of Trust or Assurance!***

- **C-I-A Triad**
  - ***Confidentiality -*** *secret or private information remains that way*
  - ***Integrity -*** *refers to the completeness, correctness, and trustworthiness of the information*
  - ***Availability -*** *authorized persons (entities) may access the information in a timely manner*

Safety and Security have I and A in common!

- **Must have solid balance between C-I-A**
  - ***Traditional IT Information Assurance (IA) tends to Overemphasize "C" at the expense of "I" and "A"***

Common Criteria (ISO/IEC 15408)

- **Common Criteria the only multinational agreed sharing mechanism for Computer / Software Security**
  - ***Common security requirements definition (Protection Profiles)***
  - ***Common evaluation scheme (CCEVS)***
  - ***Product based (COTS) flavor***
- **Component Requirements defined by:**
  - ***Functional Requirements***
  - ***Assurance Requirements***
- **Evaluation Assurance Levels 1 through 7**
- **Must know what the Protection Profile specifics**

NSTISSP #11 (National Security Telecommunications and Information Systems Security Policy)

- National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products
- IA shall be considered as a requirement for all systems used to enter, process, store, display, or transmit national security information.
- Effective 1 July 2002, the acquisition of all COTS IA and IA-enabled IT products
  - *Limited only to those evaluated and validated via NIAP or FIPS*
  - *Initially interpreted to mean Desktop IT Centric Systems*
- Latest direction includes DoD Platforms

"The appropriate certification routing for Commercial Products for use in DoD systems is through a NIAP lab under Common Criteria. NSA does not certify products, the NIAP labs do.", July 2004

-- Mike Fleming, Deputy Director IAD

" NO WAIVERS!" : DHS-OSD Software Assurance Workshop, Oct 3, 2005

-- Daniel Wolf, Director IAD,

- http://niap.nist.gov/cc-scheme/nstissp11_factsheet.pdf

Microsoft and SELINUX

- **Both OS's claim NIAP evaluations**
- **Controlled Access Protection Profile (EAL-3)**
- **Windows Server 2003 and Windows XP**
  - ***ALC assurances to EAL-4+***
- **SELINUX – same.**
- **The "CATCH".**
  - ***The profile does not address the processing nodes on a network.***
  - ***Neither Security Target addresses the network vulnerabilities***

COTS SW Supply Chain Issues (Real Examples)

- **Foreign Nationals with access to product SW at supplier**
  - ***Foreign national with prior connections to a foreign intelligence service at a trusted unclassified SW supplier***
- **Foreign sourced code incorporated into another product**
  - ***Purchased display processor driver SW from a domestic source and discovered it was actually sourced from a foreign country***
- **Foreign sourced Intellectual Property (IP) embedded into SW or firmware**
  - ***Purchased FPGA IP components from domestic supplier and subsequently learned that they were sourced from a foreign country***
- **Foreign sourced HW and SW that was purchased from another foreign source**
  - ***Purchased Nokia Checkpoint firewall appliances only to learn they were an indigenous Israeli design purchased by Nokia***

Open Source Software – Pedigree of Developers

- **Subversion**
  - ***System subversion is '... the covert and methodical undermining of internal and external controls over a system lifetime to allow unauthorized or undetected access to system resources and/or information.' - (Myers 1980).***

- **Naval Post Graduate School Study[1] (e.g. LINUX)**
  - ***Traditional techniques will NOT find nation-state funded adversaries.***
    - Source Code Inspection
    - Security Test and Evaluation
    - GOOGLE - "security thousand eyes source code"

- **Must be able to find "What is it ***NOT*** supposed to do?"**
  - ***Need Requirements and Design Documents***
  - ***Documents HAVE to be maintained w.r.t. the fielded implementation***
  - ***Full Traceability to the Documents***
  - ***Validate the trusted development process employed***

- **Substantial TCO for high robustness safety/security in OSS[3]**
  - ***"Free is not Exactly Inexpensive"***

[1]http://cisr.nps.edu/downloads/04paper_subversion.pdf
[2]http://www.nsa.gov/selinux/info/faq.cfm
[3]http://pdf.aiaa.org/jaPreview/JACIC/2007/PVJA23080.pdf

Summary

- **Security is a “buyer beware”!**
  - ***Understand the CCEVS process and PP assurances***
- **Not all companies and software products come from sources friendly to a given country!**
- **Open Source can be a real nightmare at higher security robustness levels totally obviating any “benefit” from its initial cost!**