Challenges of Secure Solutions

Cross Domain Solutions on Trusted Linux

Chad Hanson
Manager, Trusted OS Development Lab
chanson@TrustedCS.com
All TCS application software products require a trusted operating system as the mechanism for security policy enforcement.

“Current security efforts suffer from the flawed assumption that adequate security can be provided in applications with the existing security mechanisms of mainstream operating systems. In reality, the need for secure operating systems is growing in today’s computing environment due to substantial increases in connectivity and data sharing.”

The Inevitability of Failure: The Flawed Assumption of Security in Modern Computing Environment

-National Security Agency, USA
Current Approach
Information Access and Transfer

Courtesy of NSA
Assessment Methodologies

- Hurdles to create a Trusted Operating System
  - Evaluation
    - “Orange Book” - Historical
    - Common Criteria - Current

- Hurdles to field Cross Domain Solutions
  - Certification & Accreditation
    - What is it?
    - DIACAP
    - DCID 6/3
    - SABI/CDS
    - TSABI
    - NIST
Common Criteria

- Current Versions 2.2, 3.1
- International Standard (Recognized by at least 19 Countries)
- Common Criteria Documents
  - Security Functional Requirements
  - Security Assurance Level
  - Security Targets
    - Describes Security Requirements and Rationale for meeting the requirements
  - Protection Profiles (*optional*)
    - *Example*: Labeled Security Protection Profile (LSPP)
  - Standardized PPs and STs for all DoD entities
    - Overseen by NSA
Linux
Common Criteria Evaluation Landscape

Evaluation Assurance Levels

EAL 5
EAL 4
EAL 3
EAL 2
EAL 1

Red Hat
Enterprise Linux v.5
(RHEL 5)
Includes TCS Trusted Linux

Protection Profiles

CAPP
RBAC
LSPP
PP_MLOS-MR
Certification and Accreditation (C&A)

• What is C&A?
  – Certification — Evidence that proves the system security features work
  – Accreditation — Approving Authority “approves” the system

• DIACAP
  – DoD Information Assurance Certification and Accreditation Process
  – Formerly called DITSCAP
    • DoD Information Technology Security Certification and Accreditation Process

• DCID 6/3
  – Director of Central Intelligence Directive 6/3
  – SSAA — Describes the set of documentation for TSABI
Certification and Accreditation (C&A)

- **SABI/CDS** — Secret and Below Interoperability/ Cross Domain Solution
  - DIACAP (DITSCAP) documentation format
  - Oversight by CDTAB/DSAWG (NSA, DISA)

- **TSABI** — Top Secret and Below Initiative
  - DoDIIS implementation of DCID 6/3 Format
  - Oversight by DICAST (DIA)

- **NIST** — National Institute for Standards and Technology
  - NIST Format for Civilian agencies
  - Currently under development
Final Thoughts

- Many different certifications and processes
  - Varies by technology
  - Requirements differ by industry
  - Creates challenges

- Open Source Software
  - Meeting checkmarks
  - Combination of Industry and Academia
  - Increasing Security
  - Available to different methods of assessment
Thank You

For Additional Questions:

Chad Hanson
Trusted Computer Solutions, Inc.
2021 South First St. Suite 207
Champaign, IL 61820

chanson@TrustedCS.com

www.TrustedCS.com