



F-22 Requirements for Strong Access Control

Gary W. Smith, Ph.D.
Science Applications International Corporation

Workshop on Innovations in Strong Access Control
September 25-27, 2000

Air Intelligence Agency
Air Force Information Warfare Center
San Antonio, Texas



F-22 Weapon System

- Air Vehicle (A/V)
- Mission Planning System
- Maintenance System
- System/Software Engineering Environment (S/SEE)
- Contractor Logistics Support (CLS)
- Miscellaneous
 - Tech Order Data Authoring System (TODAS)
 - Operational Flight Program (OFP) Build System (OBS)

F-22 SAC Requirements Summary



- Derive from an MLS Air Vehicle as well as the MLS world
- Most subsystems operate in system high environment, thus the drivers are the need to
 - reliably export data (via media and electronic) at a classification lower than the direct users' clearance
 - produce a multilevel output for another subsystem
 - have the export decision made at the application level
- Some subsystems need to drive Type I crypto devices
- One subsystem actually has direct users with different clearances
- Most subsystems require multilevel windowing

3

Air Vehicle (A/V)



- There is no expectation that COTS will support the A/V
- Has integrated avionics with the computing capacity of several Cray computers
- Processes data in a range from U to Top Secret with multiple Special Access Required (SAR) categories
- All classified data stored encrypted
- During flight unclassified files created for export
- Differs from tradition MLS systems in that the design is fixed at "build" time (i.e., at software release)
 - All objects and their security properties are static
 - All processes and their security properties are static

4

Mission Planning System



- All users (pilots) cleared to TS/SAR
- All systems in TS/SAR approved facilities
- Pilots want to logon to their workstation at TS/SAR, plan missions using data from U to TS/SAR, and output products at their actual classification including unclassified or encrypted files on an unclassified Data Transfer Cartridge (DTC) used by the A/V
 - Many of the classified (encrypted) files on the DTC are just copied from the system
 - Other files, including unclassified files, on the DTC are created during mission planning
- Multilevel windowing required

5

Mission Planning System (Con't)



- Data must be imported from single-level sources with classifications from U to TS/SAR
- Data must be exported at unclassified and Secret (future)
- Current solution
 - All interfaces are via removable media
 - Mission planning done on system high system
 - Back-end high assurance guard (WANG XTS-300) does data content checking for re-grading data, drives the crypto, and creates lower level outputs
- Future requirements include electronic interfaces to Secret and Unclassified systems

6

TOD Authoring System



- Builds electronic TOD for use by maintainers
- All users cleared to S/SAR
- All systems in S/SAR approved facilities
- Contractor system--one instance
- Technical Order Data created at U and S/SAR
- System must create a multilevel media (CD-ROM) for use in the maintenance system
- Multilevel windowing required
- Current System: SCO CMW+ (migrating to Trusted Solaris)

7

OFP Build System (OBS)



- Creates the software load for the A/V
- All users cleared to TS/SAR
- System in TS/SAR approved facilities
- Contractor system--one instance
- System functions
 - Inputs files from two S/SAR classified systems
 - Re-grades files to correct classification (U, C, S, S/SAR)
 - Encrypts the S and S/SAR files
 - Creates a multilevel media (CD-ROM) with U and encrypted classified files used by the maintenance system
- Current System: DGUX

8

CLS Database



- Repository for data from U-S/SAR needed for CLS (e.g., depot function)
- All users cleared to S/SAR
- All systems in S/SAR approved facilities
- Contractor system--one instance
- Electronic interfaces from U-S/SAR external systems
- Multilevel windowing required
- Current System: being designed to use SCO CMW+ (migrating to Trusted Solaris) and Trusted Rubix

9

Maintenance System



- Maintainers are the A/V system administrators
- Used for all organizational maintenance tasks
- Portables attach to A/V to do maintenance
 - Install OFP
 - Download files
 - Trouble shoot problems
 - All tasks use electronic TOD (multilevel)
- For servers, some workstations, and some portables: data ranges from U to S/SAR
- Many workstations and some portables are U
- Users clearances: TS/SAR, S/SAR, and S

10

Maintenance System (Con't)



- Electronic interfaces
 - at S/SAR for CSFDB
 - at U for Base-level AF systems
 - potentially U-S/SAR to mission planning
- Multilevel windowing required
- Current system:
 - SCO CMW+ (migrating to Trusted Solaris)
 - Maxsix networking
 - Trusted Rubix
 - All internal networks closed (using VPN)
 - All external U interfaces controlled by system

11

Summary of SAC Requirements



- Separate direct users with a range of clearances from data with a range of classifications
- Reliable export data (via media) at lower classifications
- Interface to networks with data at a range of classifications
- Interface to single level networks at different classifications
- Create multilevel (labeled) output media
- Provide multilevel windowing
- Provide trusted applications that export decisions (to both media and electronic interfaces)

12