MIL-SPEC vs. COTS Standards: Necessary Harmony for Affordable Multilevel Secure Architectures

Dr. Ben A. Calloni, P.E.
“MILS Chief Evangelist”
Research Program Manager and Principle Investigator
“Affordable Safe and Secure COTS Software Initiative”
Overview

- Introduction
- MIL-SPEC: Great “-ilities” but with a cost
  - Commercial Off the Shelf and DoD
- MILS and Benefits
- Conclusion
“Some Anecdotal Stories”

McDonnell Douglas F-4J Phantom II

This one-of-a-kind photo was shot by Mr. Harry Gunn, of McDonnell Douglas, at the Point Mugu Naval Air Station on 23 October 1971. The aircraft, a McDonnell Douglas F-4J Phantom II, "Black Beauty" from Navy flight test squadron VXE-4, was captured on film while flying at near supersonic velocity. However, the frontal velocity on parts of the aircraft were supersonic, causing the two distinctive, diamond-shaped shock wave cones around the leading and trailing edges of the aircraft. A photograph like this is rare, it required split-second timing and a large amount of luck. "At the time, I was using a motorized Nikon F-2 camera with a 300mm lens," states Mr. Gunn. "I shot about four frames. The film was Ektachrome 400. As I remember, I was standing about 70 yards from the taxiway during the pass."
Chicken Cannon
Birds Pose Problems to more than Airplanes.

- Sometimes Major League Pitchers don’t fare well with birds!
  - AKA: Randy Johnson
Mil-Spec Standards

• An “Elephant” is what you get when you design a “Mouse” using MIL-SPEC!

• $500 Toilet Seats
• $100 Hammers and,
• $7000 Coffee Makers on C-5 Galaxy (plus other A/C)
  – Stainless Steel
  – Low Pressure Certified
  – Fire Rated
  – Rated to 50 G’s (Air Force Magazine - 1980’s)!!!
  – Etc.

– http://www.tsgc.utexas.edu/archive/general/ethics/galaxy.html
MIL Standards Finally Come Through !!!

“A hot cup of coffee to calm the nerves!”
Vietnam Era Pilot’s Wrist Watch


• Hand Wound, 15 Jewel Movement
• Radium Dial (glow in dark)
• +/- 60 Sec accuracy (Daily)
  – Morning update from Base Ops GMT Atomic Clock
• Water Proof to -30 feet
• Low Pressure
  – 35,000 feet for minimum of 60 minutes
• Shock Resistant
• Magnetic Protection
  – 14.5 to 15.5 gauss protection
• H3 & Radiation Markings (Tritium)
• Test for Radiation Leakage
• Order placed for Hundreds of Thousands
  – Warehouse the spares

WATCH, WRIST: GENERAL PURPOSE
MIL-W-46374A
HAMILTON
6645-952-3767
MFG. PART NO. 39988
DAAA25-72-00458
APRIL 1973
US
Casio Calculator Watch ($14.95 in 1985)

- Digital Display
- 8-Digit Calculator
- Dual Time
- 1/100 Second Stopwatch w/ Net Times, Split Time, 1st-2nd Place Times
- Daily Alarm
- Auto-Calendar
- Water Resistant
- Accuracy: +/- 1 Seconds
- Band Type: Resin
- Color: Black
- Battery Life: Approx. 1 Year

Flashing Blue Light
K-Mart Special: $9.95
MIL STD Version

- Same as commercial

- **PLUS**
  - Water Proof to -30 feet
  - Low Pressure
    - 35,000 feet for minimum of 60 minutes
  - Magnetic Protection
    - 125±1 gauss
  - ±0.7 seconds per day (@ 75°F)
- Battery Life: 5 Years Minimum

Instead of < $9.95 - $127.93 (1985)

$222.10 (2004)
**Mil-Std vs. COTS Watches**

*5 year Cost of Ownership!*

<table>
<thead>
<tr>
<th></th>
<th>Service Life</th>
<th>Unit Cost</th>
<th>Total Units</th>
<th>5 year cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>COTS</td>
<td>1 year</td>
<td>$9.95</td>
<td>15,750</td>
<td>$156,712.50</td>
</tr>
<tr>
<td>MIL STD</td>
<td>5 years</td>
<td>$127.93</td>
<td>3,000</td>
<td>$383,790.00</td>
</tr>
</tbody>
</table>
“The problem is that programmable logic controllers, digital control systems, and supervisory control and data acquisition, or SCADA, systems were never designed with security in mind”

- “SCADA vs. the hackers”, Mechanical Engineering, December 2002

• Existing SCADA systems lack authentication of administrators and operators

¹SCADA: Supervisory Control And Data Acquisition
Why Security in Commercial Embedded Systems? (cont’d)

    • Network protected but contractor used modem (with Infected PC) : not deliberate
  – *Dept of Interior computer in Portland, OR, gaining access over computers controlling every dam in Northern California*: Early 1990’s
  – *Amundsen-Scott South Pole Station’s Life Support System*: 2003
  – *Sewage & Water treatment plant in Queensland, Australia*: 2000

• Alan Paller, Director of Research, SANS Institute:
  – “*We will never know about most of the break-ins because the victims will never tell the public!*”
The MultiLevel Security (MLS) Challenge

• We need to achieve “commodity” MLS
• MILS is about making it possible for application level processes to enforce the policy semantics specific to an organization
  – … without trust concerns regarding the infrastructure upon which they operate
• MILS does this by distributing high confidence trusted enforcement mechanisms across multiple layers
  • OS, Middleware, Applications
• These independent layers must compose
  – … preserve independent component properties
  – … achieve desired emergent system properties
  – … prohibit undesired emergent system properties
What is the MILS Architecture?

- A “layered” architecture concept targeted at enabling the composition of system properties from trusted components
  - **Layered functionality & assurance**
- Defines 4 conceptual layers based on the 3-level Rushby* architecture (*John Rushby, PhD)
  1. **Separation Kernel & Hardware (single node)**
  2. **Distributed Communication (multiple nodes)**
  3. **Middleware Services (single node)**
  4. **Trusted Applications (as required) (single node)**
MILS Concept Objectives

• At the component level
  – Accommodate trusted components evaluable to the level of high robustness
  • Reduce the amount of security critical code
  • Increase the scrutiny of security critical code
MILS Project—An Enabling Technology

- Leverage the **Synergy** between:
  - *DoD, Contractors, COTS Vendors, Academia*
- Developing Common Criteria **Protection Profiles**
  - towards compliance with **NSTISSP #11**,
  - **within Open Standards Consortia** (OMG, Open Group, NCOIC)
- Developing and aggregating **NIAP Validated COTS components**
- Allowing **Cost Sharing** of
  - Evaluation & Certification costs of **appropriate COTS products**
  - to provide an appropriate infrastructure for MLS, CDS, etc.

Enabling secure, dependable GIG / WWW IA
MILS Program
Where We Are Today

F/A-22, JSF, J-UCAS, CV-22 (USAF / Navy / DARPA / SOCOM)
OSD (NII)
JTRS, FCS, DDX, MMA, Others

Certified COTS MILS RTOS & Middleware Products

AFCA Cross Domain Solutions
Army Cross Domain Solutions
NSA Information Assurance Directorate

AFRL Information Directorate

OSJTF (OUSD-ATL)

PMW 160 Cross Domain Solutions

DISA

Platform Integrators (LM Aero, Raytheon, Boeing)

RTOS Vendors
Tool Vendors
Middleware Vendors

NIAP Laboratories

NIAP Labs
Artifact

Certified COTS MILS RTOS & Middleware Products

AFCA Cross Domain Solutions
Army Cross Domain Solutions
NSA Information Assurance Directorate

AFRL Information Directorate

OSJTF (OUSD-ATL)

PMW 160 Cross Domain Solutions

DISA

COTS Vendors

Standards Bodies
OMG, The Open Group, NCOIC

Evaluation (EAL6/7)
Funding
Collaboration
Consulting

NIAP Laboratories

F/A-22, JSF, J-UCAS, CV-22 (USAF / Navy / DARPA / SOCOM)
OSD (NII)
JTRS, FCS, DDX, MMA, Others

Certified COTS MILS RTOS & Middleware Products

AFCA Cross Domain Solutions
Army Cross Domain Solutions
NSA Information Assurance Directorate

AFRL Information Directorate

OSJTF (OUSD-ATL)

PMW 160 Cross Domain Solutions

DISA

COTS Vendors

Standards Bodies
OMG, The Open Group, NCOIC

Evaluation (EAL6/7)
Funding
Collaboration
Consulting

NIAP Laboratories

F/A-22, JSF, J-UCAS, CV-22 (USAF / Navy / DARPA / SOCOM)
OSD (NII)
JTRS, FCS, DDX, MMA, Others

Certified COTS MILS RTOS & Middleware Products

AFCA Cross Domain Solutions
Army Cross Domain Solutions
NSA Information Assurance Directorate

AFRL Information Directorate

OSJTF (OUSD-ATL)

PMW 160 Cross Domain Solutions

DISA

COTS Vendors

Standards Bodies
OMG, The Open Group, NCOIC

Evaluation (EAL6/7)
Funding
Collaboration
Consulting

NIAP Laboratories

F/A-22, JSF, J-UCAS, CV-22 (USAF / Navy / DARPA / SOCOM)
OSD (NII)
JTRS, FCS, DDX, MMA, Others

Certified COTS MILS RTOS & Middleware Products

AFCA Cross Domain Solutions
Army Cross Domain Solutions
NSA Information Assurance Directorate

AFRL Information Directorate

OSJTF (OUSD-ATL)

PMW 160 Cross Domain Solutions

DISA

COTS Vendors

Standards Bodies
OMG, The Open Group, NCOIC

Evaluation (EAL6/7)
Funding
Collaboration
Consulting

NIAP Laboratories
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,

Evaluation and C&A Processes

- **Product Assurance**
  - *Common Criteria Evaluation & Validation Scheme (CCEVS)*
    - Administered by the National Information Assurance Partnership (NIAP)
    - Evaluation activities executed by Common Criteria Testing Laboratories (CCTLs)
    - Evaluation oversight provided by NIAP representatives ( Validators)

- **System Assurance**
  - *DoD Information Technology Security Certification & Accreditation Process (DITSCAP)*
    - Process executed by the Program Manager leading a team that includes
      - Designated Accreditation Authority (DAA)
      - Certifier and certification team(s)
      - User Representative
    - Commercial via CIP and the CISSP IA personnel
Robustness Compared to EALs

- DoD 8500 defined assurance in terms of Robustness Levels
  - Basic, Medium, High
- NSA has translated Robustness Levels into EALs
  - Basic Robustness
    - EAL2 augmented
  - Medium Robustness
    - EAL4 augmented
  - High Robustness
    - EAL6 augmented
    - Will include elements of EAL7
Key High Robustness Assurance Properties

- Confidence that Trusted Security Functions (TSF) are
  - Non-bypassable
  - Evaluable in regards to design/implementation
  - Always invoked
  - Tamper-proof

- Mathematical Verification of security policy model and external interfaces

- Reduction of size and complexity of the TSF

- Modular/layered approach to s/w component development, evaluation, integration
Orange Book Approach

==

MIL-STD

Monolithic Applications

MLS Requires Evaluatable Applications!

Monolithic Kernel

Fault Isolation

Network I/O

Periods Processing

Auditing

Data isolation

DAC

MAC

Device drivers

Monolithic Application Extensions

User Mode

Privilege Mode

Feb 1, 2006

Unevaluatable!!!
MILS Architecture Evolution

Application Modules

Evaluatable Applications
On an Evaluatable Infrastructure

Rushby’s Middleware

Fault Isolation
Periods Processing

Kernel

Separation Kernel

Network I/O

Information Flow

Data isolation

Auditing

DAC

MAC

Device drivers

File systems

User Mode

Privilege Mode

ML Module 1

CSCI (Main Program)

SL (S) Application

SL (U) Application

SL (TS) Application

MLS Downgrader

Appropriate Mathematica Verification

Feb 1, 2006
Flow Policy Enforcement: User and Separation Kernel View

The user view of the Operational Policy to be enforced ...

... what the Separation Kernel enforces ...

Level

<table>
<thead>
<tr>
<th>BOD</th>
<th>FIN</th>
<th>MKT</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>B</td>
<td>D</td>
</tr>
</tbody>
</table>

Feb 1, 2006
MILS provides \textit{End-to-End}:

- Information Flow
- Data Isolation
- Periods Processing
- Damage Limitation

\textbf{System}

\textbf{Policy Enforcement Independent of Node Boundaries}

\textbf{CPU & Network}

- Registers
- Switches, DMA, …

\textbf{Red Data}

\textbf{Black Data}
# Notional MLS Architecture “Software Stack” Layering

<table>
<thead>
<tr>
<th>Hardware - MMU, Supervisor Mode, Privileged Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Separation Kernel - Isolation, Explicit Information Flow, Messages, Shared Mem, Synchronization</td>
</tr>
<tr>
<td>Security Attributes + Reference Validation Mechanism - MLS/MLI-MAC, DAC, Roles, Privileges</td>
</tr>
<tr>
<td>MLS Resources - Devices, Files, Pseudo-devices, Namespace(s)</td>
</tr>
<tr>
<td>MLS Console - Windows, Trusted Path</td>
</tr>
<tr>
<td>MLS Networking - Labels, Crypto, Routing</td>
</tr>
<tr>
<td>MLS Filesystem - Dir’s, Polyinstantiation</td>
</tr>
<tr>
<td>MLS Applications - DBMS, Web Server, Regrader, Guard, etc.</td>
</tr>
<tr>
<td>MLS Server Apps</td>
</tr>
<tr>
<td>MLS Desktop Apps</td>
</tr>
<tr>
<td>DownGrader</td>
</tr>
<tr>
<td>MILS CORBA/DDS</td>
</tr>
</tbody>
</table>

- **Product Cert Underway**
- **Profiles In Review**
- **Profiles in Start**

**Feb 1, 2006**
MILS Workstation: with Guest OS

Physical Display, Keyboard & Mouse

Trusted Path

Console Manager (MLS)
Token Service Driver (MLS)
File Sys. Driver (MLS)
Network Interface Unit (SL)
PCS (MLS)

LynxOS - Secure

Processor

S (SL)
RT CORBA/DDS/WEB

TS (SL)
RT CORBA/DDS/WEB

S, TS (MLS)
Minimal Middleware
Minimum Run-Time Library

Windows
Linux
Security will Cost More!

- CAN ANY ONE MAKE TOO MUCH PROFIT?
- Kindler Gentler Corporate America?!?!?

- “Field Guide to the New CEO” – Robert McGarvey
  - Desirable Traits
    1. Humble
    2. Inclusive
    3. Broad-Minded
    4. Intimate
    5. Values-Oriented
    6. Empathetic
    7. Absolutely Honest

“CEO’s need strongly held belief’s about how good business looks and acts. Profits can no longer come in First, Second, and Third on a CEO’s roundup of the three most important to-do’s.”
Historical Strategies for Warfare

Air Superiority

"Information Superiority"
in the 21st Century

Numerical Superiority

Sea Power

shore Force Projection
Let’s give them the affordable, verifiable IA technology necessary to do their jobs!