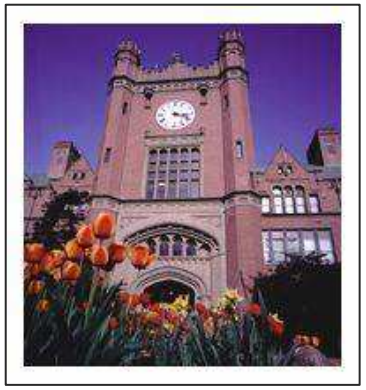
MILS Multiple Independent Levels of Security



Carol Taylor & Jim Alves-Foss
University of Idaho
Moscow, Idaho

United states

Outline

- Introduction and Motivation
- MILS History
- MILS Architecture
- Common Criteria (CC) Certification
- MILS Certification Progress
- Conclusion

Introduction

- MILS is an evolving component based high assurance architecture
  - MILS = Multiple Independent Levels of Security
- Under development by industry, government and academia
- Intended for high assurance environments
  - Multi-level data communications
  - Safety critical systems

Introduction

- Current and past practice in CC Certification
  - No methodology for Common Criteria certification of components or much
  - Reuse of certification efforts
- Common Criteria focused on certification of single systems or products
  - Not easy to certify composed system

Introduction

- Also, entire certification process is not “open”
  - Access to information on CC process not readily available at higher EAL levels
  - Evaluation methodology is proprietary since labs compete with each other for certification business

Motivation

- Need to do component CC certification for MILS
  - Reuse of certification artifacts
  - Publish findings in order to clarify the process
  - Investigate higher assurance levels for trusted MILS components

Motivation

- Area in need of further work
  - Composing Protection Profiles of certified products
  - Show composition of components will work
    - Brian Snow, December 5, 2005 - ACSAC

MILS History

- High assurance systems require proof that system meets critical security requirements
  - Proof = formal methods analysis
- Past high assurance systems relied on
  - Security Kernel +
  - Trusted Computing Base (TCB)

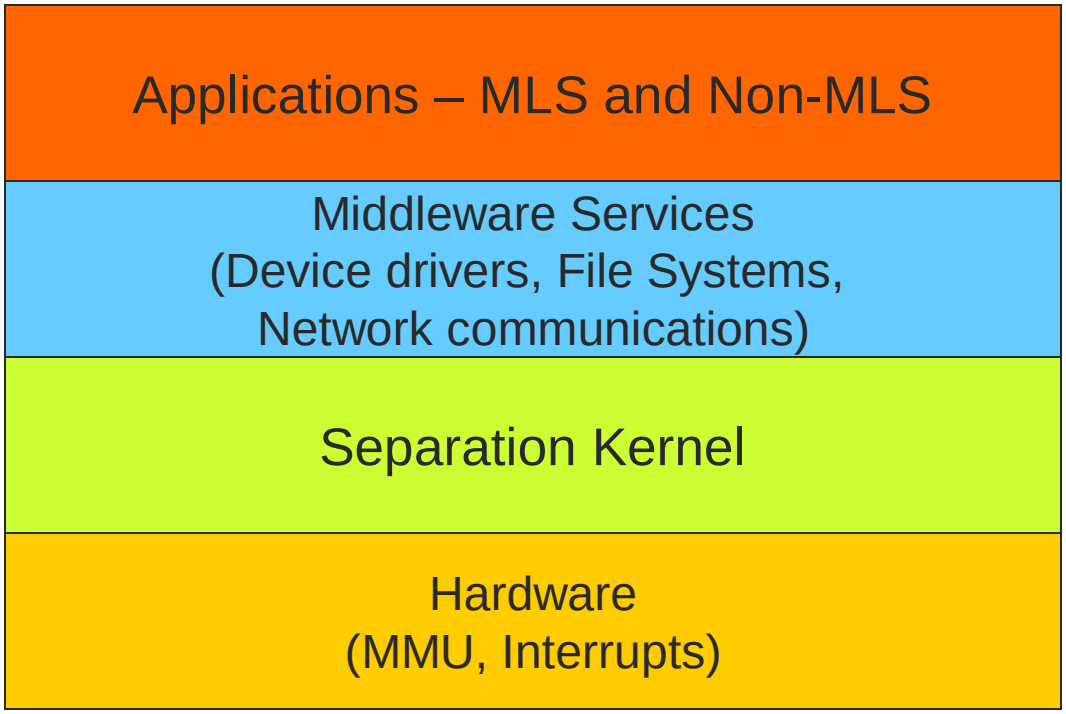
MILS History

- As high assurance systems evolved
  - Difficult to separate security functionality from other system functions
  - TCB became very large
  - Impossible to formally verify correctness of system with many 1000's lines of code
    - Security policy complex
    - High level design also complicated and large

MILS History

- MILS is an alternative *vision* for high assurance systems
  - MILS is a layered approach with lower layers providing security services to higher layers
  - Each layer is responsible for security services in its own domain and nothing else
  - Limits the complexity and scope of security mechanisms
  - Makes evaluation possible
  - Fits in with *small is beautiful* thinking

Conceptual View MILS Layers



MILS Architecture

- Separation underlies all of MILS
  - Long used in avionics world for safety critical systems
  - Safety features
    - Space partitioning
      - Well defined, separate address space
      - Damage Limitation
        - Application errors only affect the application partition
    - Time partitioning
      - Only one application runs in mostly static time allowance

MILS Architecture

- Separation Kernel
  - Simplified to provide partitioning, partition scheduling and secure communication between partitions
  - An EAL 6+ Protection Profile has been written
  - Vendors developing separation kernels
    - Green Hills, LynuxWorks, Wind River
  - Others developing MILS components
    - Lockheed Martin, Objective Interface, University of Idaho, Navel Research Lab

MILS Architecture

- Separation Kernel
  - Security Policy
    - Data isolation – enforces space partitioning
    - Periods Processing – enforces time partitioning
    - Sanitization – clears shared resources, system buffers and micro processor registers
    - Information flow – permits communication between authorized partitions

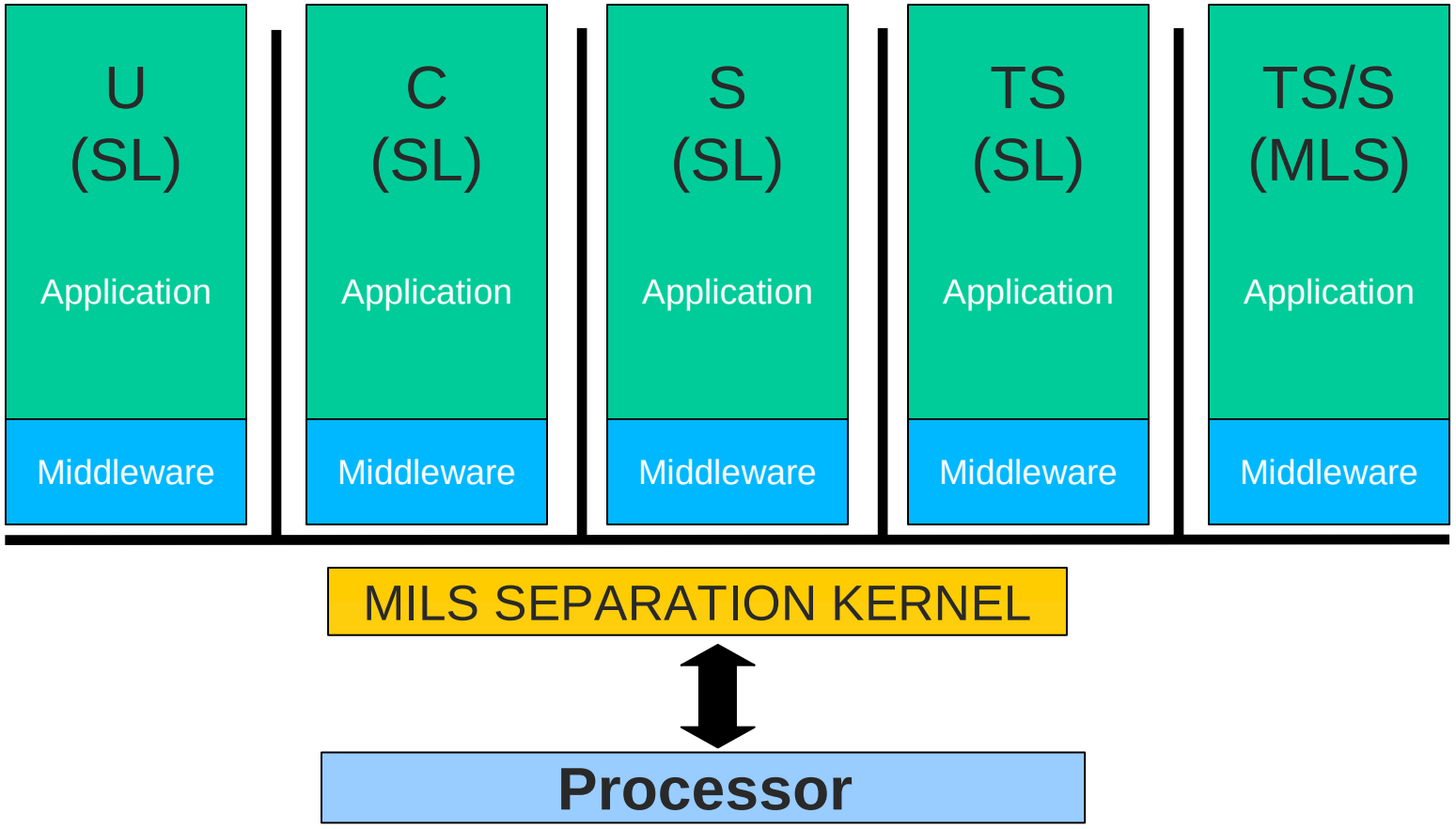
MILS Architecture

- Middleware Services
  - Functionality previously in kernel now in OS Middleware layer
    - File systems, network services, device drivers
  - Added new functionality for security
    - Partitioning Communication System
      - Provides trusted, MLS, network communication
    - MILS Message Router
      - Data switch for partitions, handles multiple classification levels

MILS Architecture

- Applications
  - Traditional middleware such as CORBA
  - Guards
    - MLS or Single level
  - Encryption
  - Downgrader or Regrader

The MILS Architecture



Common Criteria Certification

- CC v. 2.2
  - Certification of single products
    - Application, OS, processor
  - Target of Evaluation (TOE)
    - Define or find a Protection Profile (PP)
    - Adapt PP to a Security Target (ST) at a given EAL level
      - ST specifies security functionality of TOE
    - Evaluated according to ST
      - NIAP Lab evaluates products up to EAL 4
      - Beyond EAL 4, NSA evaluates TOE

Common Criteria Certification

- CC v. 3.0
  - Allows certification of composed products
    - Involves combination of two or more evaluated products
    - Intent is to evaluate components developed by different organizations
      - Proprietary issues
      - Assumption is not all information is available for evaluation

Common Criteria Certification

- Composed CC v. 3.0 Certification
  - How to do it?
    - Independent evaluation of each component
    - Composed evaluation base component and dependent component
      - Use new class ACO: Composition - Five families
        - ACO-COR – Composition rationale
        - ACO-DEV – Development evidence
        - ACO-REL – Reliance of dependent component
        - ACO-TBT – Base TOE Testing
        - ACO-VUL – Composition vulnerability analysis

Common Criteria Certification

- Composed CC v. 3.0 Certification
  - Five families say
    - Ensure base component provides at least as high an assurance level as the dependent component
    - Security functionality in support of security requirements of dependent component is adequate
    - Description of interfaces used to support security functions of dependent component is provided
      - May not have been considered during component evaluation

Common Criteria Certification

- Composed CC v. 3.0 Certification
  - Five families say
    - Testing of base component as used in composed TOE is performed
    - Residual vulnerabilities of base component are reported and an analysis of vulnerabilities arising from composition are considered

Common Criteria Certification

- Composed CC v. 3.0 Certification
  - Composition Assurance Packages (CAPs)
    - Replace EAL levels for composed TOE's
    - Build on results of previously evaluated entities
    - CAP-A Structurally Composed
    - CAP-B Methodically Composed
    - CAP-C Methodically Composed, Tested and Reviewed

Common Criteria Certification

- Composed CC v. 3.0 Certification
  - CAP-A Structurally Composed
    - Developers or users require low to moderate levels of independently assured security
    - Security functional requirements are analyzed just using the outputs from the evaluations of the component TOE's
      - ST, and guidance documentation
      - No involvement of base TOE developer required

Common Criteria Certification

- Composed CC v. 3.0 Certification
  - CAP-B Methodically Composed
    - Developers or users require moderate levels of independently assured security
    - Security functional requirements are analyzed using outputs from TOE evaluations, specification of interfaces and high level TOE design of the composed TOE
    - Minimal involvement of base TOE developer required

Common Criteria Certification

- Composed CC v. 3.0 Certification
  - CAP-C Methodically Composed, Tested and Reviewed
    - Developers or users require moderate to high levels of independently assured security and are prepared to incur additional security-specific engineering costs
    - Security functional requirements are analyzed using outputs from TOE evaluations, specification of interfaces and the TOE design of the composed TOE
    - Involvement of base TOE developer required

Common Criteria Certification

- MILS Certification
  - MILS is ideally suited to a composed certification effort
    - MILS was designed as a component architecture
      - Components designed by multiple vendors
      - Components certified at multiple EAL levels
      - Components assist with security policy enforcement

Common Criteria Certification

- Composed MILS CC v. 3.0 Certification
  - Example: Separation Kernel and MMR
    - Base component
      - Separation Kernel
    - Dependent component
      - MILS Message Router (MMR)

Common Criteria Certification

- Steps for Composing MILS Components
  - Evaluation of Separation Kernel
  - Evaluation of MILS Message Router
  - Evaluation of Composed MILS Components
    - Define an ST for composed system
    - Decide on a Composition Assurance Level (CAP)

MILS Certification Progress

- Separation Kernel evaluation
  - Protection Profile, Security Target - done
  - Currently being evaluated
    - Formal methods artifacts under construction
    - Target EAL 6+
- MILS Message Router
  - No PP, Security Target – being created
    - Constructing artifacts
    - No actual NIAP Lab evaluation – review of artifacts
    - Target EAL 5

MILS Certification Progress

- Composed Certification
  - Next steps
    - Define a composed ST, Evaluation
    - Document all steps and publish results
    - Discuss strategy and methodology
    - Should be repeatable for other MILS components
    - Many certification artifacts should be reusable within MILS systems
      - Standard interfaces, consistent security policies

Conclusion

- MILS architecture provides layered, component-based approach to high assurance systems
  - Components certified at different assurance levels as needed
  - Saves cost, effort since entire system doesn't need to operate system "high"

Conclusion

- Newest CC version allows composed certification
  - MILS can use composition so that components can be developed by multiple venders
    - High assurance components designed to work together
  - Re-use of certification results now possible

The End

ctaylor@cs.uidaho.edu