# Multiple Independent Levels of Security Architecture (MILS)

Ashley Ma & Miliano Mikol

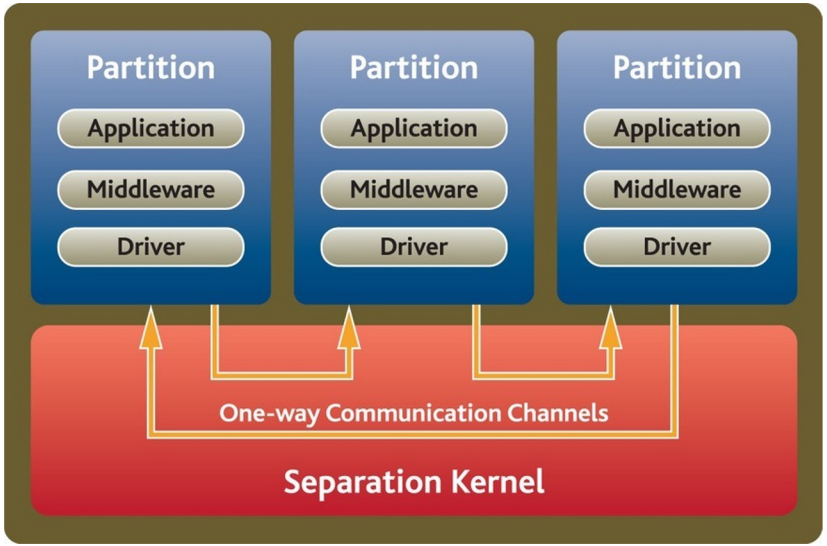
# Different Needs, Different Security Systems

*Multi-level secure systems have been built using multiple physically separated computers, networks, and displays costing money, power, and time*

- Single-level secure system
  - One security domain that processes information
- Multi-single level secure system (MSLS)
  - Two or more security domains are being processed but are always separated in time or space
- Multi-level secure system (MLS)
  - Two or more security domains are processed within the same time and space

# Multiple Independent Levels of Security Architecture (MILS)

- A “divide-and-conquer” approach that creates an environment indistinguishable from a physical one
  - Trusted hardware
  - Separation Kernel
  - Middleware
  - Application



# MILS Separation Kernel Security Policies

- Data Isolation
  - Partitions do not access resources in other partitions
- Periods Processing
  - Applications in partitions execute only for a specified duration in the system’s schedule
- Information Flow
  - Definitions for permitted information flow between partitions
- Fault Isolation
  - Failure of one partition does not affect any other partitions in the system

# NEAT is the Goal

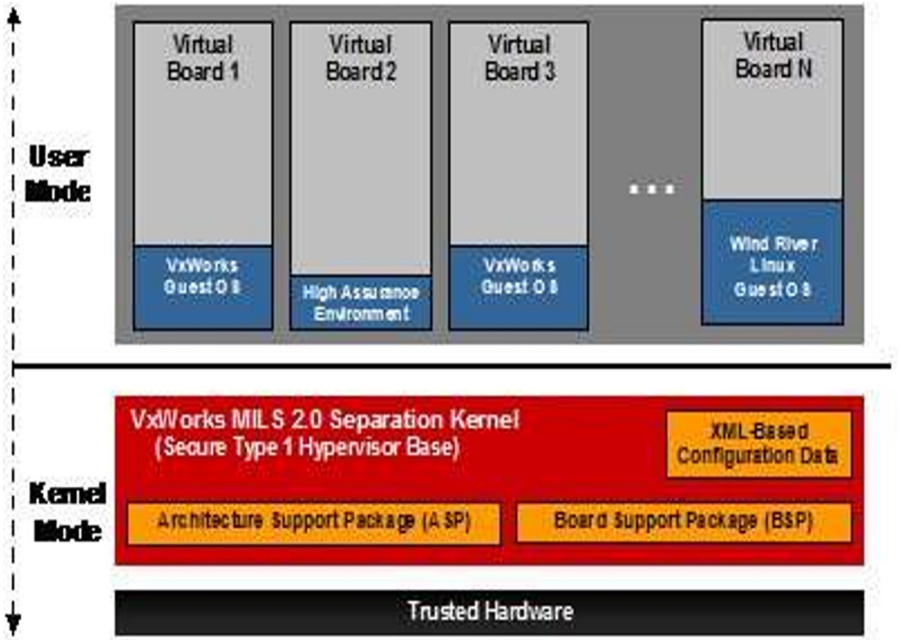
*Based on class discussion, do these principles sound familiar?*

- **N**on-bypassable, **E**valuable (verifiable), **A**lways invoked, **T**amperproof
- Useful for crucial applications
  - Control of nuclear power generation
  - Control of sewage control systems
  - F-35 Joint Strike Fighter Communications, Navigation, Identification (CNI) system


# Data Isolation

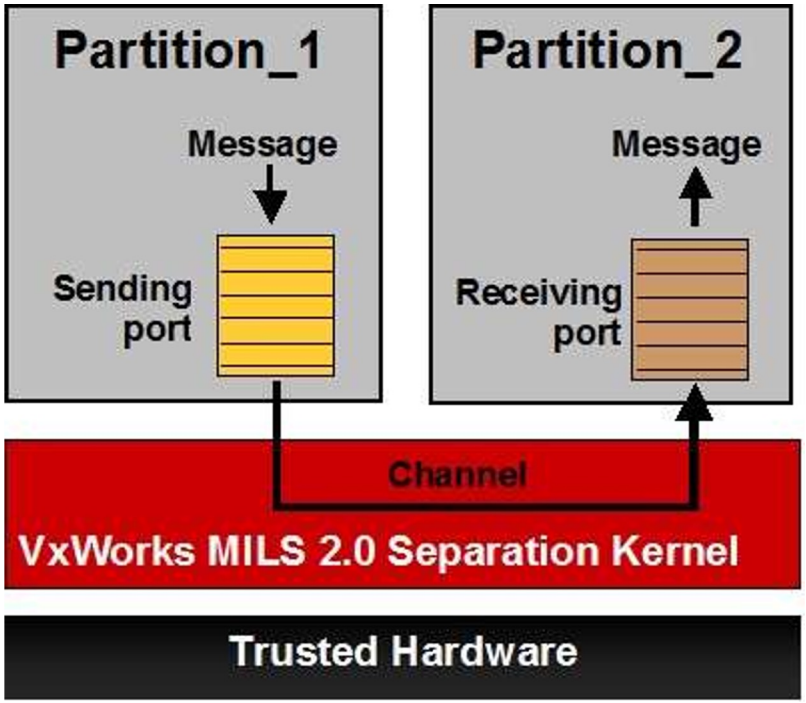
*An application of the VxWorks MILS 2.0 Hypervisor by Wind River*

- Relies on separation kernel in kernel mode that provides partitions (virtual boards); each partition contains different guest OS's
- Virtualization entails that guest OS cannot access physical memory outside of its virtual machine and is not reliant on cooperation of other partitions



# Information Flow

- The VxWorks MILS 2.0 hypervisor can define, implement, and enforce information flow policies between partitions
- It uses two transport mechanisms:
  - Secure IPC (message passing via a buffer)
  - Shared memory (implemented ad hoc by applications)



# Fault Isolation

- Separation kernel contributes to the implementation of fault isolation
- By preventing fault propagation and/or illegal accesses beyond a partition
- VxWorks MILS 2.0 implementing a security-management architecture that provides a configurable framework
  - includes a comprehensive set of security management functions
- Access to the security management functions is determined by the predefined security policy
  - implemented in conjunction with a security audit
  - determine the appropriate action to be taken in response to an event or an attempted security violation
- Enable the security management architecture to be configured in an appropriate manner for the deployed system, depending on the threat environment

# Secure Application Development

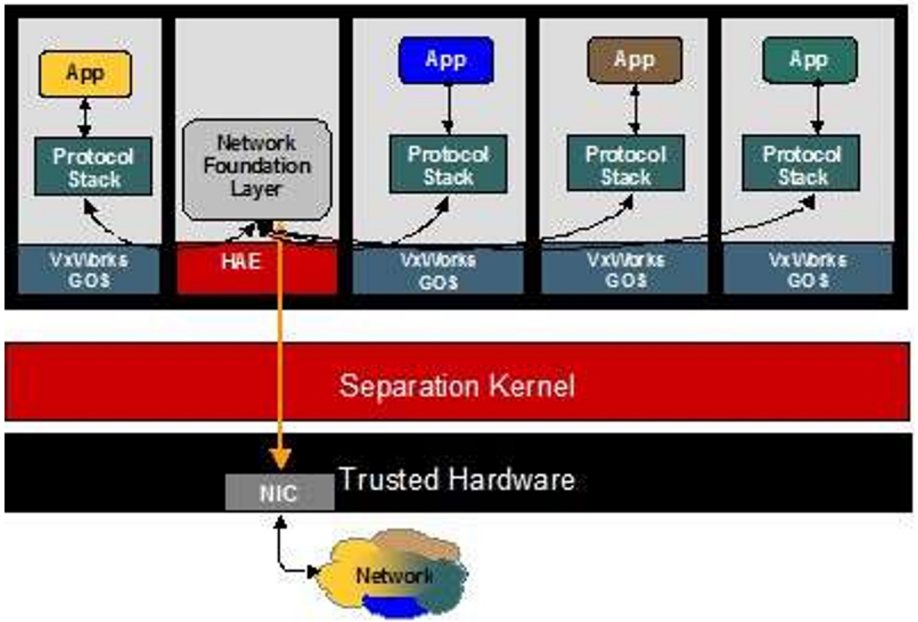
- High Assurance Environment (HAE)
  - provides a single-threaded, minimal runtime environment, using a small code footprint
    - The Vxworks Guest OS
    - The Linux Guest OS
- High Assurance Network Stack (HANS)
  - Implements an IPv4-based UDP and TCP networking stack
- Development and debugging tools (not covered)
  - The quality of development and debugging tools can have a dramatic effect on development timescales
  - tools for single-level secure development may not be suited to MILS development
  - Wind River Workbench

# High Assurance Environment (HAE)

- Provides a single-threaded, minimal runtime environment, using a small code footprint
  - Enables the cost-effective development of high EAL(Common Criteria Evaluation Assurance Level)/high robustness applications that require a high degree of scrutiny
  - Can also be used in conjunction with medium robustness guest OS environments to partition new or existing applications into security-critical and non-critical components
- The VxWorks Guest OS
  - provides a multi-threaded environment, medium-assurance components of high-assurance systems, using divide-and-conquer approach
  - provides familiar functionality and API
- The Linux Guest OS
  - provides a Wind River Linux 3.0.2 environment on top of the MILS separation kernel

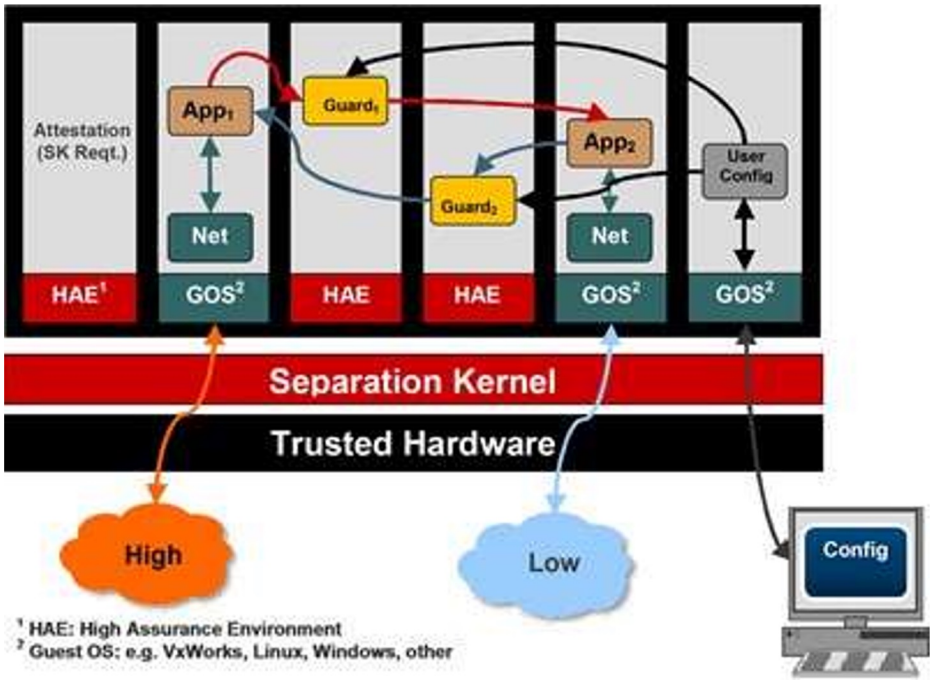
# High Assurance Network Stack (HANS)

- Implements an IPv4-based UDP and TCP networking stack
- Using separate partitions to enable multi-single level secure (MSLS) network communications
  - Multiple levels of data can be carried on the network, but are always separated
- HA partition is used to ensure that the packets destined for different partitions are kept separate within the MILS system's partitions
  - Ingress
  - Egress
- The MSLS security requirements for this network architecture are focused on the HA partition



# High Assurance Network Stack (HANS)

- Develop sophisticated CDS and MLS systems
  - Example: a notional MILS-based gateway
  - The system is connected to two networks of different security classifications, filtering and routing data between them
  - A Separate partition for each network interface, containing a network stack and device driver running in user mode
  - Dedicated guards which filter the traffic in each direction
  - Using secure IPC (SIPC) to implement communication between partitions



# System configuration and security certification

- Require configuration data and security policy for each partition are defined correctly
  - MILS enables building complex systems, comprising multiple partitions, communications channels, and interfaces
- CDS and MLS systems will be developed using a role-based approach
  - Developers of an application within a partition can only access to pertinent information at the appropriate security classification and the external interfaces of the partition

# System configuration and security certification

- Uses modular XML-based configuration and data security policies
  - To support the role-based approach
  - Independently define the configuration of each partition
  - A system can be constructed in a modular and incremental manner
- Advantage of the modular approach
  - Simplify the initial development of a MILS system
  - Assist the migration of Single Level Secure (SLS) Linux or VxWorks applications to MILS architecture

# Reference


- MILS architecture simplifies design of high assurance systems – Part 1
  - https://www.eetimes.com/mils-architecture-simplifies-design-of-high-assurance-systems-part-1/
- MILS architecture yields high assurance systems – Part 2
  - https://www.eetimes.com/mils-architecture-yields-high-assurance-systems-part-2/
- Open standards ease Multi-Level Security (MLS) systems integration
  - https://militaryembedded.com/cyber/encryption/open-mls-systems-integration