The Dual-EE Approach

The Dual-Execution-Environment Approach: Analysis and Comparative Evaluation

Mohamed Sabt[1,2]

[1]Orange Labs, France

[2]Sorbonne Universités, UTC, France

IFIP SEC, May 2015

Outline

1. Introduction

Outline

1. Introduction
2. Background
   - Separation Kernel
   - Secure Execution Environment

Outline

Outline

Outline

1. Introduction
2. Background
   - Separation Kernel
   - Secure Execution Environment
3. Dual-Execution-Environment
   - Introduction
   - Core Properties
4. Comparative Evaluation
5. Conclusion
   - Summary
   - Perspectives

The Trust Problem

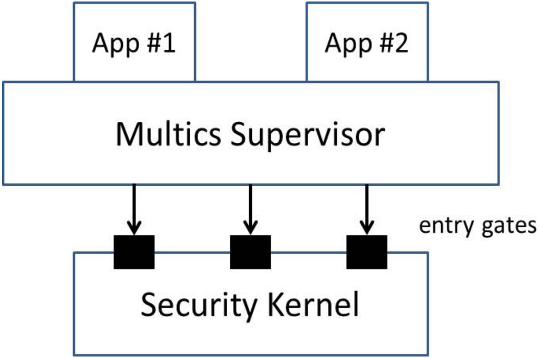
Description

How the execution of an application can be secured in the face of a compromised operating system ?

Motivation

- The rise of services requiring trusted platforms with proved security;
- Operating systems of real-world systems are inherently insecure:
  1. Complexity and unsafe languages;
  2. Poor isolation.

The Multics Project – SOSP '75



The Security Kernel

Where should it be placed ?

1. monolithic operating system: Unix-like systems;

The Security Kernel

Where should it be placed ?

1. monolithic operating system: Unix-like systems;
2. special hardware processor: AEGIS and XOMOS;

The Security Kernel

Where should it be placed ?

1. monolithic operating system: Unix-like systems;
2. special hardware processor: AEGIS and XOMOS;
3. micro-kernel: SeL4;

The Security Kernel

Where should it be placed ?

1. monolithic operating system: Unix-like systems;
2. special hardware processor: AEGIS and XOMOS;
3. micro-kernel: SeL4;
4. specialized OS: TLR.

The Security Kernel

Where should it be placed ?

1. monolithic operating system: Unix-like systems;
2. special hardware processor: AEGIS and XOMOS;
3. micro-kernel: SeL4;
4. specialized OS: TLR.

Outline

Definition

j'aurais mis Design à la place de definition

Design Purpose

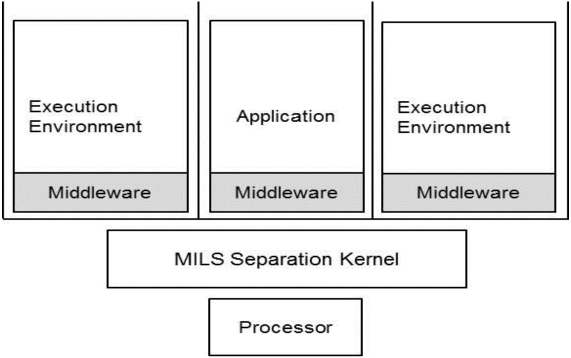
To enable the coexistence of different systems requiring different levels of security on the same platform.

requests ?

Design Requirements

- *tamper proof*: it cannot be modified or disabled by rogue application;
- *always invoked*: all inter-partition communication request must go through it;
- *evaluable*: its correctness can be validated.

Overview of the SK Architecture



Outline

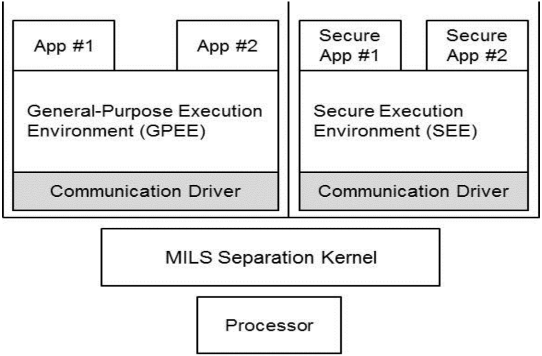
Definition

SEE is a processing environment that guarantees the following properties:

- *authenticity*: the code under execution should not have been changed;
- *integrity*: runtime states should not have been tampered with;
- *privacy*: code, data and runtime states should not have been observable by unauthorized applications.

Outline

Overview


App #1
App #2
General-Purpose Execution Environment (GPEE)
Communication Driver
Secure App #1
Secure App #2
Secure Execution Environment (SEE)
Communication Driver
MILS Separation Kernel
Processor

Definition

The Dual-EE

The Dual-Execution-Environment is a security architecture where both a Separation Kernel and a Secure Execution Environment play the role of Security Kernel.

Theorem

Theorem

Let S be a system in which the security kernel is based on a separation kernel. If the requirements of all secure applications are equivalent, then all multi-execution-environment architecture can be reduced to a dual-execution-environment architecture.

Theorem

Theorem

Let S be a system in which the security kernel is based on a separation kernel. If the requirements of all secure applications are equivalent, then all multi-execution-environment architecture can be reduced to a dual-execution-environment architecture.

Sketch of proof

Let S be multi-EE architecture. Without loss of generality, we suppose that S is a system which contains 4 execution environments, 2 of which are non-secure and 2 are secure...

Outline

Isolation Properties

1. Data (spatial) separation. Data within one partition cannot be read or modified by other partitions;
2. Sanitization (temporal separation). Shared resources cannot be used to leak information into other partitions;
3. Control of information flow. Communication between partitions cannot occur unless explicitly permitted;
4. Fault isolation. Security breach in one partition cannot spread to other partitions.

Functional Properties

1. Protected Execution. no interference caused by malicious software;
2. Sealed Storage. protecting the integrity, secrecy and freshness of data;
3. Protected Input/Output. protecting the integrity and secrecy of input/output data;
4. Attestation. authentication to remote trusted parties.

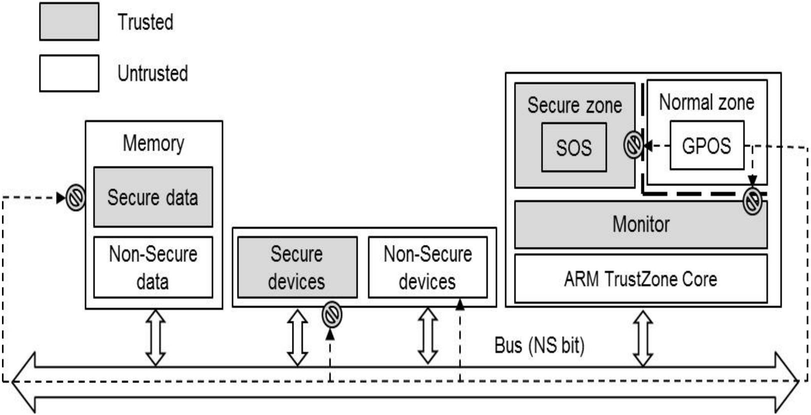
Ease-of-Deployment Properties

1. Support of Legacy Systems. required modifications for a system to run on a separation kernel;
2. Cost. extra silicon;
3. Overhead. separation kernel impact on performance;
4. SEE Performance. how fast complex operations are executed by SEE.

Dual-EE Technologies

- External hardware module: smart cards;
- Bare-metal hypervisor: KVM/ARM;
- Special processor extensions: ARM TrustZone.

ARM TrustZone



Summary of Evaluation

Comparison Category	Comparison Criteria	*Smart Card*	*KVM*	*TrustZone*
Security Requirements	Protected Execution	✓	✓	✓
	Sealed Storage	✓	×	✓*
	Protected Input	×	✓	✓
	Protected Output	×	✓	✓
	Attestation	✓	×	✓*
Isolation Properties	Data Separation	HW	SW	HW
	Information Flow Control	SW	SW	HW
	Sanitization	HW	SW	HW/SW
	Damage Limitation	HW	SW	HW
Deployability Criteria	Legacy Systems	✓	✓	✓
	Low Overhead	✓	×	✓
	Low Cost	×	×	✓*
	High Performance	×	✓	✓

✓: satisfies the criterion; ×: does not satisfy the criterion;
✓*: needs widely available additional hardware modules to satisfy the criterion;
HW: satisfied by hardware module; **SW**: satisfied by software implementation.

Discussion

- Bare-metal hypervisors achieve the lowest score;

Discussion

- Bare-metal hypervisors achieve the lowest score;
- External hardware modules do not fit to certain kind of applications that need user interaction and high processing speed;

Discussion

- Bare-metal hypervisors achieve the lowest score;
- External hardware modules do not fit to certain kind of applications that need user interaction and high processing speed;
- TrustZone provides a balanced compromise.

Outline

Summary

- The dual-EE is an interesting approach related to the trust problem;
- We provided a convenient abstract model to better represent the characteristics of the dual-EE approach;
- Our model was examined by revisiting the literature.

Outline

Perspectives

- Include primitives defined in the MILS architecture to our core properties;
- Use the dual-EE approach to design a better Trusted Execution Environment (TEE).

Thank you for your attention!