KASPERSKY lab

Kaspersky Security System

Introduction

Nowadays all computer systems, including cyber-physical systems used in critical infrastructure, are prone to many cyberthreats. These computer systems are often protected by add-on tools that are incapable of addressing their specific security requirements. Such security tools don't have adequate means of defining the appropriate security policy for every system or for enforcing these policies exactly as defined.

For this reason Kaspersky Lab has created an embeddable solution that meets current security requirements. Kaspersky Security System is an innovative framework that is intended to secure a wide range of computer systems such as:

- Enterprise systems
- Special-purpose computer systems
- The Internet of Things
- Smart grids
- Industrial systems
- Transportation systems
- Critical Infrastructure

Advantages

- The Kaspersky Security System paradigm is based on the strict separation of security features from the functional components of the computer system. Security is provided regardless of how the system is implemented. Because of this, trusted systems can be built using untrusted components and KSS. Security rules and policies can be varied without changing any functional components.
- Kaspersky Security System allows for the combination of different security models, such as connecting basic and specific security policies.
- Under some special conditions Kaspersky Security System can be used in real-time operating systems.
- The architecture of Kaspersky Security System enables the definition of specific security rules for every given system and excludes unnecessary controls and complicated configurations from the overall solution.

History

Kaspersky Lab is creating a portfolio of security solutions for critical infrastructure as part of a global initiative. One of these solutions is KasperskyOS, the secure operating system. KasperskyOS was developed using the best design practices and de-facto security standards. Adherence to these practices and standards will better assure the confidentiality and integrity of the data in the computer system.

Kaspersky Security System was initially implemented as a part of KasperskyOS with a view to supporting diverse security models. But during development it became clear that Kaspersky Security System fits the needs of many other operating systems

and hypervisor-based solutions. As a result, it has evolved into a stand-alone project and can now be embedded into other systems that demand high security levels.

Implementation

Kaspersky Security System is implemented as an OEM component for operating system or hypervisor-based solutions.

Target audience

- Vendors of operating systems and hypervisor-based solutions
- Vendors of IT systems demanding enhanced security levels
- System integrators

Main features

- Applying access control rules based on the separation of security domains
- Adjusting the interaction of components related to different security domains
- Classifying informational resources according to a given security policy
- Computing the security verdict to authorize every action in the system
- Security logging and audit
- Providing additional security services

Integration

The integration of Kaspersky Security System into the initial operating system or solution can be undertaken in two phases:

Stage 1. Pre-project phase

1. Analyzing the existing solution (operating system or hypervisor-based solution, special hardware aspects).
2. Defining a plan to adapt Kaspersky Security System to the existing solution.
3. Creating the appropriate security policies.

Stage 2. Integration phase

4. Integrating Kaspersky Security System into the existing system.
5. Deploying the security policies.

Components

- **Security Runtime** is the module that enables the interaction between the existing system's internal components and Kaspersky Security System. It delivers every request to the security verdict engine and returns the computed verdict to the system.
- **Security Server** is the security engine that computes the **security verdict** (whether an interaction should be permitted or not). It provides its verdict using the following factors:
  - ✓ The set of security rules implemented in the **security policy** for the system

- ✓ **The security context** that describes the current state of the system
- **Configuration tools** are used to adjust security policies and rules and deploy them in the system.

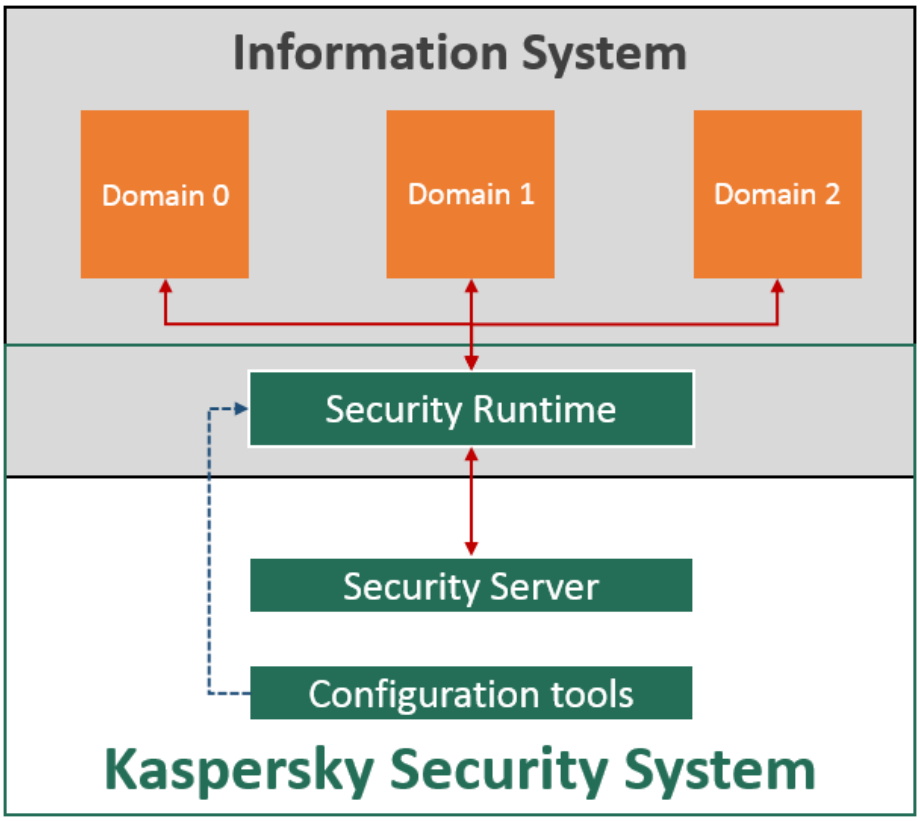

*Figure 1. An example of Kaspersky Security System managing three **security domains** of an Information System under a single security policy. The part of Kaspersky Security System, **Security Runtime**, mediates communications between security domains and enforces predefined security rules which are set by **Configuration tools**. **Security Server** includes a customizable database of security policies and provides decisions to Security Runtime based on the current state of the system.*

Operating modes

There are two operating modes for Kaspersky Security System:

- The **basic mode** includes a wide range of security policies, sufficient for most usage scenarios.
- The **customized mode** builds on the basic mode with special security policies necessary to comply with the specific objectives of the target solution.

Compatibility*

Kaspersky Security System is now available for the following operating systems:

- KasperskyOS**
- PikeOS
- Linux

Supporting documentation

The supporting documentation includes a set of design patterns, best practices for software development, and configuration rules to help achieve the highest levels of security.

Patents

The technologies that form the basis of Kaspersky Security System and Kaspersky OS are covered by a set of patents: US 7386885 B1, US 7730535 B1, US 8370918 B1, EP 2575318 A1, US 8522008 B2, US 20130333018 A1, US 8381282 B1, EP 2575317 A1, US 8370922 B1, EP 2575319 A1.

** Work on providing support for other operating systems, including some real-time OS, is in progress*

***The deep integration of KasperskyOS and Kaspersky Security System creates a sustainable, versatile and high performance platform to support security in different systems, including industrial networks.*