KasperskyOS®

Secure OS for Telecoms Equipment

The only way is to develop a cyber-secure integrated software suite that includes an operating system, as well as system and application software

Technical requirements

- POSIX API (~98% API) compatible
- Intel x86, x64 и ARM (v6, v7, v8)

Patents

The technologies that form the basis of KasperskyOS and Kaspersky Security System 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,
US 9015797 B1, DE 202014104595 U1.

Introduction

As a system for exchanging diverse information, the Internet has become part and parcel of our everyday lives. Many traditional businesses are transforming themselves into IT and technology companies. We often don't realize to what extent our work, life and leisure are dependent on the Net.

At the same time, new opportunities give rise to new risks. In the case of the Internet, the risks are primarily associated with cyber threats that can affect the stability of the Internet's infrastructure, and how stably the Internet operates depends on telecommunications service providers and telecoms equipment.

Purpose

Among the cyber threats targeting telecommunications equipment, the following are particularly significant:

1. Threats associated with unintentional actions:
   a. Employee actions resulting in complete or partial equipment failure, switching off or changing the operation mode.
   b. Unauthorized installation and use of programs that are unaccounted for.
2. Threats associated with intentional actions:
   a. Remote attacks on hardware aiming to change its configuration or modify its built-in software (firmware).
   b. Exploiting built-in backdoors or known software and hardware vulnerabilities in order to intercept traffic or gain control of equipment or an automated system.
   c. Unauthorized installation and use of programs that are unaccounted for.

While some threats can be mitigated by developing dedicated security software, reliable protection from other threats can only be achieved by installing a trusted computer appliance providing guaranteed protection against unauthorized software installation or execution of undocumented functions.

This means that equipment manufacturers face a difficult dilemma. On the one hand, the equipment they produce must provide extensive functionality; on the other, its firmware should be sufficiently compact to make checking it for vulnerabilities and backdoors feasible. The equipment should also be reliable and provide faultless operation, but at the same time have excellent cyber-security characteristics.

It should also be kept in mind that protecting telecommunications equipment against cyber threats is further complicated by a number of factors, including:

(1) the need for the equipment to operate autonomously without maintenance or software updates for extended periods of time;
(2) specialized hardware;
(3) proprietary built-in software;
(4) permanent direct connection to the internet;
(5) not being able to install additional protection designed for general-purpose systems.

The only way is to develop a cyber-secure integrated software suite that includes an operating system, as well as system and application software.

Advantages

Inherent security. KasperskyOS is an operating system that is secure by design and we intend to keep it that way by using the best practices in software development.

Versatile modular architecture. Building the system based on loosely coupled modules helps minimize the amount of trusted code and tailor each solution to the customer's specific needs.

Well-designed applications. The component-based approach to creating secure applications makes developing them relatively easy and convenient, helping reduce the amount of time needed to take new products to market.

Flexible security configuration. Well-designed configuration tools make it easy to create declarative rule definitions and combinations of rules to control interactions in the system.

Separation of application features from security functions. The security architecture is designed to separate security functions from application business logic, making both configuring security policies and developing applications easier.

Full-fledged security for attached devices. KasperskyOS is a reliable platform for embedded systems that have special cyber-security requirements.

The equipment should also be reliable and provide faultless operation, but at the same time have excellent cyber-security characteristics

To address the issue of cyber security for telecoms equipment, while minimizing the time required to develop security features, we offer KasperskyOS, a secure operating system based on an architecture that is designed to ensure software is executed securely, including non-secure applications. In addition, KasperskyOS provides protection in the event of random software errors and improper user actions.

Features

There are additional security features that can be provided together with KasperskyOS for telecommunications equipment:

Trusted Channel

This is a set of components that can be used to organize a secure communication channel between a device and a remote party.

The technology is based on the TLS protocol, a mature standard protocol providing security for communications. Multiple implementations are available (including open source) from various vendors.

However, it is often the case that TLS-based solutions incorporate numerous functions (e.g. Linux process) into one domain:

- TLS implementation
- Connection management
- Application-specific protocol processing (e.g. HTTP)
- And even more high level logic

It means all these functions must be considered as trusted: compromising any of them results in a whole system being compromised.

Trusted Channel's main objective is to minimize the size of trusted code by separating secure connection, authorization and remote request processing. In KasperskyOS, a secure connection is made with TLS in a separate domain (entity), as well as authorization of the connection. Neither TLS nor authorization performs any application-specific message processing.

In this architecture, network modules, connection management and any application-specific data processing (e.g. HTTP parsing) are treated as untrusted. The only trusted components are TLS and authorization.

Secure Storage

Secure Storage is a key-value database with a simple interface, suitable for storing important configuration parameters.

Every parameter in the database is associated with its own security attributes.

A security policy can be applied to get/set a particular parameter based on its security attributes. It is also possible to specify a security policy for the whole configuration update that ensures individual parameter updates are aligned with each other.

KSS uses secure storage to store security policy parameters. Storage can also be used by any application in a system and a security policy has fine-grained control over which application can use which parameters.

Threat Intelligence Services

Kaspersky Lab offers a set of proactive threat intelligence services for telecoms equipment such as penetration testing and security assessment. Our experts will attempt to discover vulnerabilities and bypass authentication and authorization procedures on behalf of various types of intruders in order to gain control of the equipment.

www.kaspersky.com

© 2017 AO Kaspersky Lab. All rights reserved. Registered trademarks and service marks are the property of their respective owners.

Find out more at os.kaspersky.com
All about Internet security: www.securelist.com