



Secure solutions for the IoT by Kaspersky Lab and Advantech



KasperskyOS®

www.kaspersky.com
os.kaspersky.com

ADVANTECH

Enabling an Intelligent Planet

www.advantech.com

“In today’s interconnected world where the competitiveness of practically every business depends on the effectiveness of the IT solutions used, device security and reliability play a pivotal role. This is particularly important for the class of devices known as gateways, because they are, by their very nature, interfaces between different information spaces. Security features define the degree of trust for these devices, and are therefore one of the key factors when choosing one. And I understand those clients who include information security requirements in the technical specifications for their information systems.”

Andrey Doukhvalov,
Head of Future Technologies,
Kaspersky Lab

The market now offers a multitude of computer appliances that can be used as gateways for data aggregation, processing and transfer. These devices can act as media and protocol converters, come in a variety of shapes and sizes and, most importantly, come with a variety of characteristics. When it comes to choosing a device like this, it’s not only the goals and environment that should directly influence the decision but also the level of security it can provide.

Challenge

The specialists at Kaspersky Lab were faced with the task of finding a versatile hardware platform capable of adapting to a wide range of tasks and conditions, and then using that platform to build a security solution for IoT gateways.

The following selection criteria were used:

- the hardware platform had to be widely available;
- the hardware platform had to support Linux operating systems and have a good BSP;
- the device characteristics had to implement all the intended security functions without impacting performance – to protect both the device itself and to monitor other devices connected to it.

The Kaspersky Lab solution

After analyzing the options, the Compact Box Computer UBC-200 by Advantech, based on an ARM processor, was chosen as the first step. Of all the options on the market, this hardware platform came closest to meeting all the requirements. In addition to the features required to implement the Kaspersky Lab solution, the UBC-200 is highly versatile, meaning it can be used in the most diverse IoT verticals, from industry and automation of smart cities to the agricultural sector.

Subsequent steps saw Kaspersky Lab develop Kaspersky IoT Secure Gateway based on the RSB-4411 SBC and UTX-3117 x86 architecture.

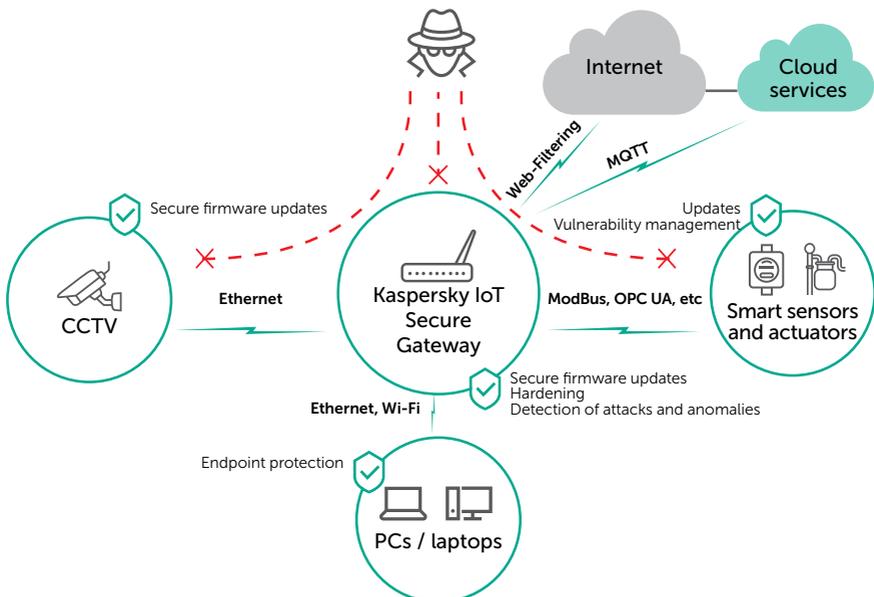
The following are the main advantages of using the Advantech Compact Box Computer UBC-200 as a hardware platform:

- **High performance**
i.MX6 quad-core processor based on ARM Cortex-A9 up to 2 GB DDR3 RAM
- **High network bandwidth**
Gigabit Ethernet and the ability to use wireless modules.
- **Software support**
Functional Linux BSP.
- **Compact and climate resilient**
Dimensions: 111 x 77 x 30 mm; weight: 312g. Operational temperature: 0~60° C; relative operating humidity up to 95%.
- **Power supply and consumption**
UBC-200 uses a DC input of 9~24V. At maximum load, the power consumption of the device is just 3.16W.
- **Security**
UBC-200 allows you to apply advanced security technologies developed at Kaspersky Lab specifically for protecting IoT devices, increasing the level of security for both the device and the entire network.

Result

Thanks to the use of Advantech Compact Box Computer UBC-200, Kaspersky Lab's specialists were able to implement a number of security modules and technologies:

- **Kaspersky OS**
KasperskyOS can be used as a software framework (optional). KasperskyOS is a secure operating system for embedded connected devices with specific cybersecurity requirements. KasperskyOS creates an environment where a vulnerability or bad code is no longer a big deal.
- **Kaspersky Security System**
Depending on business requirements, part of KasperskyOS – Kaspersky Security System (KSS) – can be used on Linux-based operating systems. KSS ensures the implementation of security policies for software component interactions.
- **Secure Boot**
With the use of cryptographic methods, Secure Boot makes it possible to confirm the integrity and authenticity of a firmware image before it's loaded by a device.
- **Secure Update**
Secure Update allows the system to verify the integrity and authenticity of firmware updates using cryptographic methods, and ensures firmware is only updated from correctly signed and encrypted images from trusted sources.
- **Secure Audit**
Secure Audit is a Kaspersky OS feature that recognizes, records and stores audit logs and provides guarantees that log entries cannot be altered.
- **Linux Application Control**
Linux Application Control makes it possible to create white- and blacklists of executable objects in the system and block the execution of unresolved files, as well as contact Kaspersky Security Network to obtain a reputational trust level and security recommendations for an application. This technology can prevent infections of IoT devices with malware like Mirai or Bashlite.



About Kaspersky Lab

Kaspersky Lab is a global cybersecurity company, which has been operating in the market for over 20 years. Kaspersky Lab's deep threat intelligence and security expertise is constantly transforming into next generation security solutions and services to protect businesses, critical infrastructure, governments and consumers around the globe. The company's comprehensive security portfolio includes leading endpoint protection and a number of specialized security solutions and services to fight sophisticated and evolving digital threats. Over 400 million users are protected by Kaspersky Lab technologies and we help 270,000 corporate clients protect what matters most to them.

Learn more at www.kaspersky.com.

About Advantech

Advantech's corporate vision is to enable an intelligent planet. The company is a global leader in the fields of IoT intelligent systems and embedded platforms. To embrace the trends of IoT, big data, and artificial intelligence, Advantech promotes IoT hardware and software solutions with the Edge Intelligence WISE-PaaS core to assist business partners and clients in connecting their industrial chains. Advantech is also working with business partners to co-create business ecosystems that accelerate the goal of industrial intelligence.

Learn more at www.advantech.com.

- **Web-filter/Parental control**

Depending on the purpose of a device, web filtering (for enterprise and industrial devices) or parental control (for consumer devices used, for example, in smart homes) technology can be applied to the firmware.

- **Machine learning-based protection**

To ensure reliable protection of devices and networks connected to the gateway, machine learning (ML) technologies are used in Kaspersky IoT Secure Gateway to identify and categorize all devices on the network by actively and passively analyzing their behavior, composing a profile of each device and detecting unforeseen activity.

- **ML asset discovery**

ML-based asset discovery technology can discover, categorize and organize all the assets in the protected network automatically. Using special fingerprint technology, our solution detects the type of device, maker's name and model (and even firmware version) by simply analyzing specific parts (metadata) of the network traffic.

- **ML device behavior analysis**

Once assets in the network are discovered and categorized, a specific profile is created describing the overall (healthy) network behavior of the asset. Such profiles describe how a specific device with the current firmware is behaving in the customer's network.

- **ML anomaly detection**

Based on ML asset discovery and device profiling, any anomaly in IoT (or IIoT) device behavior can be detected. ML anomaly detection can detect malware and botnet activity, use of your device in DDoS attacks, firmware exploitation, miners, device control interception by hackers, etc.



KasperskyOS®

Find out more at
os.kaspersky.com

www.kaspersky.com

© 2019 AO Kaspersky Lab. All rights reserved. Registered trademarks and service marks are the property of their respective owners.