PcVue Secure

PcVue Secure. Protection of PcVue SCADA system using KasperskyOS-based technologies

kaspersky

KasperskyOS®

Challenge

Ensuring the information security of industrial control systems (ICSs) is a critical task that's becoming increasingly important with time. On the one hand, new regulatory requirements are emerging, such as Russian Federal law 'On the safety of critical information infrastructure of the Russian Federation' of July 26, 2017 No. 187-FZ. On the other hand, ICSs are becoming more and more complex and deeply integrated into various spheres of everyday life. Despite all the undeniable advantages, the use of the Industry 4.0 paradigm means the attack surface of ICSs is becoming very large.

This situation is compounded by the fact that many existing ICSs bear the legacy of a time when very little thought was given to information security. As a consequence, these systems are poorly protected, and enhancing their security levels requires substantial investment, to the point of a complete overhaul. However, even such drastic measures would fail to provide 100% security guarantees, because the environment in which ICS components operate is also insufficiently protected. Critical vulnerabilities are constantly being detected in the most common operating systems.

Solution

Kaspersky has been working in the field of information security for more than 20 years and offers effective technologies and solutions for ICS protection.

The use of the KasperskyOS operating system and related technologies makes it possible to solve important issues concerning the protection of SCADA systems – a key element of an ICS.

Kaspersky has collaborated with ARC Informatique in developing the PcVue Secure solution, a protected SCADA based on the PcVue and KasperskyOS products.

PcVue Solutions is a scalable software platform that provides complete control of a company's processes and supports a broad range of hardware from a variety of manufacturers. The platform's main component is the PcVue SCADA package.

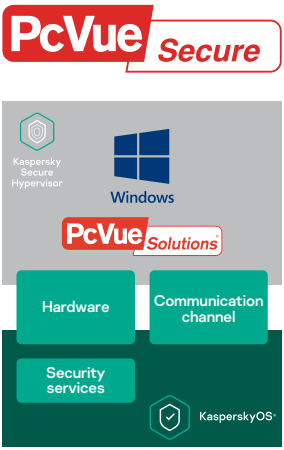
PcVue is a full-featured Windows-based SCADA designed to create data collection, management and monitoring systems for solutions of varying scales: from standalone operator stations to distributed management systems with client-server architecture that involves large numbers of workstations and servers. It comes with support for remote access, including access via mobile clients.

Thousands of industrial facilities around the world are currently powered by PcVue Solutions. The list of industries using the platform includes building management systems (BMS), energy, water supply, transportation, infrastructure, oil and gas, manufacturing, etc.

KasperskyOS and Kaspersky Secure Hypervisor make it possible to significantly enhance the security of SCADA solutions, and this approach can be applied without modifications or with minimum modifications to the SCADA solution.

Result

Description of the approach



Kaspersky has developed a secure operating system – KasperskyOS – that guarantees a high level of safety for the software components operating under its control. A distinctive feature of this OS is the Kaspersky Security System (KSS) subsystem that allows you to set extremely flexible security policies to control interactions between software components within KasperskyOS. These policies are based on various security models, with the ability to use several of them simultaneously.

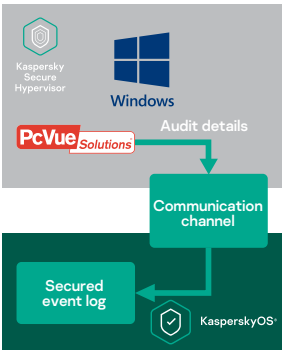
The Kaspersky Secure Hypervisor (KSH) virtualization subsystem has also been developed for KasperskyOS. This is a Type 2 hypervisor (other software components can run without limitations along with the hypervisor within the KasperskyOS context) that is implemented using Intel VT-x, VT-d hardware. Kaspersky Secure Hypervisor supports various guest operating systems, including Windows (XP, 7, 8, and 10) and the most popular distributions based on the Linux kernel.

In the PcVue Secure solution SCADA is launched from the Windows 10 guest operating system running on a KSH-based virtual machine, which provides a controlled channel for interaction between the software components of the guest OS and KasperskyOS.

KSH controls all aspects of the virtual machine's operation, including granting/restricting access to peripheral hardware, while the actual virtual machine hardware can be provided via KasperskyOS as is or emulated. In the latter case, it is possible to assign new properties to the hardware using KSH and KasperskyOS in such a way that it's transparent to the guest OS. For example, a traffic encryption feature can be added for the network adapter, while a function can be added for intercepting/modifying keyboard input.

A scheme like this makes it possible to implement various protection scenarios for a SCADA solution, some of which are described below.

Secure event log



Secure storage of event log data is an important cybersecurity objective because event log spoofing is an important element of many computer attacks.

However, it is very difficult to ensure secure storage of the event log when running a general-purpose operating system. One reason for this is that an event log requires a specific security policy with the following properties:

- Option to add new records to the event log.
- No option to modify records after they are added.
- No option to delete records, with the exception of user(s) with special privileges.
- Ability to view records defined by the user's privileges.

This is easy to do with KasperskyOS.

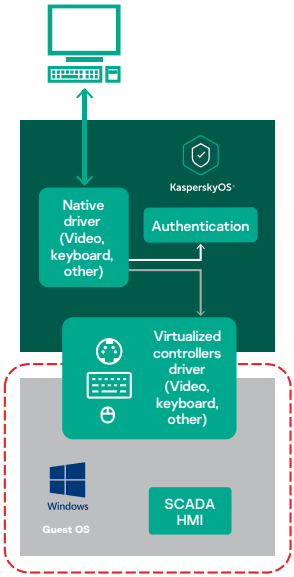
SCADA implements a mechanism that allows you to intercept logs and transfer them to the application handling events on the KasperskyOS side.

KSS tools set the required security policy when working with data.

Since event information is stored in the context of a trusted environment, the guest OS does not have access to them, and once the data has been received it cannot be modified. All subsequent operations involving the event log data are performed using KasperskyOS in accordance with the security policies assigned to the solution.

Kaspersky also offers Secure Audit technology that uses blockchain technology to guarantee data integrity even if unauthorized access has been obtained. With Secure Audit, it is possible to reliably determine whether or not data spoofing has taken place.

Enhanced authentication



The standard authentication mechanisms offered in Windows are rather weak. For example, there are some typical problems associated with password protection: a complex password is difficult to remember, while a simple password can be easily compromised. At the same time, there are many authentication mechanisms not supported by Windows.

Using a hypervisor makes it possible to implement a reliable mechanism for user authentication that is independent of Windows.

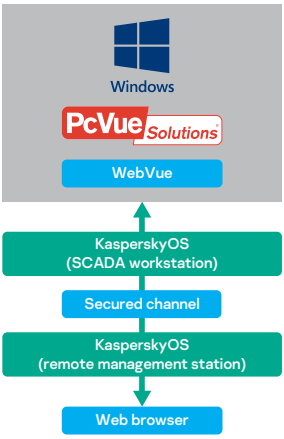
Kaspersky Secure Hypervisor allows you to control the virtual machine's access to peripherals, particularly to implement a scenario for blocking a virtual machine when user I/O devices are disconnected from it.

Access to the virtual machine can only be granted if the user has been successfully authenticated by KasperskyOS.

There are a number of advantages to this approach:

- The use of KasperskyOS guarantees that the authentication procedure cannot be compromised.
- It is possible to implement various authentication mechanisms, regardless of the guest OS.
- Information about the user appears in KasperskyOS, which allows this data to be used in the corresponding security policies, for example, to implement a role-based access control model.

Secure remote access



The possibility of remote access to information systems presents a number of advantages, but it also poses a complex problem from an information security standpoint – and this is especially true for SCADA systems. The use of KasperskyOS makes it possible to effectively solve this problem and implement secure remote access to SCADA.

The main problem of remote access from an information security standpoint is the organization of a secure communication channel that guarantees the confidentiality, integrity and authenticity of data.

The use of cryptography stacks of popular operating systems provides limited guarantees only. Even if the SCADA workstation is well protected, it is much more difficult to ensure the security of remote clients because they work in conditions with a greater risk of compromise.

KasperskyOS software components run in a secure environment and under constant control, which provides much higher security guarantees than other operating systems. In the remote access scenario, KasperskyOS tools implement a secure communication channel independently from the guest OS with the ability to use various cryptography algorithms, for example, symmetric encryption algorithms.

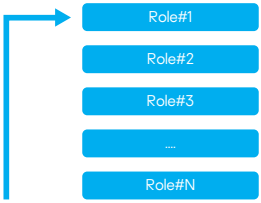
KSH emulates the network adapter for the virtual machine, intercepting traffic in KSH and encrypting it using the KasperskyOS cryptography stack .

SCADA PcVue version 12 offers a remote access web interface (WebVue).

The WebVue traffic from the SCADA workstation is protected by KasperskyOS and redirected to a remote workstation also running KasperskyOS with the Web Browser application installed. Since the remote workstation is managed by KasperskyOS, high security guarantees can be provided for it as well.

This means that integrity, confidentiality and authenticity requirements are fulfilled along the entire data transmission path between the SCADA workstation and the remote access workstation.

Role-based access control



When user authentication is performed by KasperskyOS, it is possible to implement scenarios based on the role-based access model.

In KasperskyOS, the role ID can be used as a parameter in security policies enforced by Kaspersky Security System. There is no way the ID can be altered.

Let's consider the possible roles and corresponding privileges that are applicable to the PcVue SCADA system. This list is not comprehensive and serves only to illustrate the approach. In real-life projects it can be modified or extended.

Role №1 – 'Observer'. This role gives access to the guest OS in order to view its screen, without the ability to perform any actions (display output is available, but device input is not).

Using the communication channel between the guest OS and KasperskyOS, the latter can notify the guest OS that the user has logged in, after which the guest OS can display information intended for that user.

Role №2 – 'Local SCADA operator'. This role allows the operator to access Web Browser, a local KasperskyOS application that operates in conjunction with the hypervisor. It is pre-configured to a dedicated controlled communication channel with the component WebVue SCADA PcVue. This dedicated controlled channel is implemented using the emulated network device for the virtual machine in the context of which SCADA PcVue operates. This means communication is totally transparent for SCADA, but the SCADA attack surface is small. The user is unable to escalate privileges using vulnerabilities in the guest OS because the user does not interact with it directly.

At the same time, the web interface provided by SCADA imposes practically no limitations on the solution's functionality, so the user can make full use of the PcVue features available to them.

Role №3 – 'Administrator'. This role grants maximum privileges to the user. Logging on with administrator privileges gives full access to the guest OS interface, including data entry using the keyboard and mouse. Additionally, depending on the settings of the solution used at the KasperskyOS level, the user can be granted or denied access to peripheral devices such as USB flash drives, CD drives, etc.

A user with administrator privileges can configure the guest OS and modify the SCADA project. In effect, the user privileges for this role are identical to those of a regular SCADA workstation operator if the solution is launched without a hypervisor.

It should be noted that these protection scenarios require minimal modifications to both the SCADA and the guest OS. However, if the components running in the context of a virtual machine created with KSH tools "know" about KasperskyOS and can use the services it provides, a wide range of additional features will appear for the SCADA system, both in terms of functionality and security.

About Kaspersky

Kaspersky is a global cybersecurity company founded in 1997. Kaspersky's deep threat intelligence and security expertise is constantly transforming into innovative 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 technologies and we help 270,000 corporate clients protect what matters most to them.

About ARC Informatique

ARC Informatique, France, the developer of PcVue Solutions software products, has been active in the market of industrial software for more than 35 years. The company is headquartered in Paris, France, and has 15 offices around the world: in the USA, Europe, Asia and Latin America, as well as its partnership network. Each subsidiary works in sales and technical support, and also participates in the development of software products. The company is ISO 9001 and ISO 14001 certified.

PcVue Solutions is a set of software and hardware solutions that offers a flexible solution and the required tools for data collection, supervisory control, network management, alarm control and database management.

ARC INFORMATIQUE is known in the industrial automation software market for such products as PcVue™, ContextVue™, PlantVue™ and remote access solutions WebVue™, SnapVue™ and TouchVue™.

More than 75,000 licenses are installed and operate around the world under the management of PcVue Solutions in various fields.

KasperskyOS®

Read more at
os.kaspersky.com

www.kaspersky.com