Kaspersky Smart Technologies and IoT Security Assessment

Embedded systems are becoming increasingly complex. Industry has made huge strides, from highly specialized microcontroller-based components to complex interconnected solutions built on third-party SoC platforms with real-time or Linux-based operating systems communicating with each other via dozens of different protocols. This kind of rapid evolution brings tremendous versatility, but it also comes at a price: the introduction of common computing platforms in embedded systems has brought its inherent threat landscape with it.

Kaspersky Lab offers a set of proactive security assessment services for vendors of embedded systems who want to enhance the security of their products and take a pre-emptive approach against advanced threats.

The following potential risk scenarios can be identified:

- Debugging interfaces available for end users (JTAG, SWD, UART, etc.)
- The likelihood of memory dumps and subsequent disclosure of sensitive information
- The likelihood of sensitive information transmitted between components of the device being intercepted
- Improper implementation of encryption schemes and algorithms
- The possibility of firmware modification that could circumvent normal business operation of the device
- The use of insecure network protocols for system management and information exchange
- Incorrect implementation of security mechanisms such as authentication and privilege separation
- Typical embedded software vulnerabilities, such as buffer overflow, integer overflow/underflow, etc.
- The presence of hardcoded credentials, undocumented authentication bypass and privilege escalation mechanisms.

Embedded Device Security Assessment

A comprehensive security-level evaluation of hardware and software components of embedded devices. The aim is to identify potential vulnerabilities, misconfigurations and design issues that could be used by criminals to compromise normal operation of the platform.

The following types of activities can be conducted with this service (depending on the type of system and access level granted):

- Threat modelling according to business logic and use cases
- Manual and automated identification of vulnerabilities, including research aimed at finding vulnerabilities
- Firmware and application source code analysis using static, dynamic and interactive approaches
- Security assessment of underlying communication protocols and existing security controls
- Radio channels security assessment, including mobile and wireless networks (2G/3G/4G, Wi-Fi, Bluetooth, ZigBee, Z-Wave, NFC, etc.)
- Configuration analysis for operating systems and application components
- Evaluation of implemented security measures
- Exploitation of the revealed vulnerabilities and attack demonstration
- Preparation of a technical report containing detailed information on findings, recommendations, and conclusions on the likelihood of different types of threats.

If our experts discover zero-day vulnerabilities, they will provide advisories to software vendors and at the same time follow a strict responsible disclosure policy. We also develop recommendations to mitigate any impact related to discovered vulnerabilities, until the vendor releases a security update.

The following types of vulnerabilities can be identified:

- Flaws in authentication and authorization, including multi-factor authentication
- Input validation (overflows, memory leaks, etc.)
- Code injection (SQL injection, OS commanding, etc.)
- Logical vulnerabilities leading to function abuse or fraud
- Client-side vulnerabilities (cross-site scripting, cross-site request forgery, etc.)
- Cryptography weaknesses (schemes, implementation, etc.)
- Vulnerabilities in client-server communications
- And more...

Application Security Assessment, Web Application Security Assessment, Mobile Application Security Assessment

These assessments involve a detailed security analysis of applications used to control and monitor the operation of embedded systems. It includes static and dynamic analysis of the application's source code and architecture. Kaspersky Lab's experts will discover any vulnerabilities that may allow an intruder to bypass authentication and authorization procedures, raise privileges, or bypass security controls or fraud detection.

The Application Security Assessment (using both automated and manual approaches) is aimed at detection of vulnerabilities leading to:

- Gaining control over the application
- Attacks against the application's clients
- Denial of service of the entire application, or partial denial of service (blocking access of individual users)
- Obtaining important information from the application
- Influencing data integrity.

During the analysis, our experts will not only discover configuration flaws and vulnerabilities in obsolete software versions, but will also deeply analyze the logic behind the processes performed by the application, evaluate the presence and quality of security mechanisms and perform security research aimed at identifying new vulnerabilities. Special tools for attack automation can be developed by request to demonstrate the impact of an attack and validate findings.

Our analysis identifies the following types of vulnerabilities:

- Vulnerable network architecture, insufficient network protection
- Vulnerabilities leading to network traffic interception and redirection
- Insufficient authentication and authorization
- Weak user credentials
- Configuration flaws, including excessive user privileges
- Vulnerabilities caused by errors in application codes
- Vulnerabilities caused by using outdated hardware and software versions without the latest security updates
- Information disclosure

Penetration Testing

Penetration Testing involves analyzing the IT infrastructure for the presence of security flaws that may allow external and internal intruders to operate embedded systems including testing attempts to bypass security controls to obtain the maximum possible privileges in critical systems.

Depending on your needs and the specifics of your systems, you can choose from various types of IT infrastructure security assessment services – or combine them:

- **External penetration testing** – security assessment from the Internet without any preliminary knowledge of your system.
- **Internal penetration testing** – security assessment on behalf of an internal attacker, for instance a visitor having only physical access to your office, or a contractor with limited access to certain systems.
- **Wireless networks security assessment** – our experts will visit your site and analyze Wi-Fi security controls.

Security Assessment Reporting

Once the security assessment has been completed, customers receive a report containing detailed technical information:

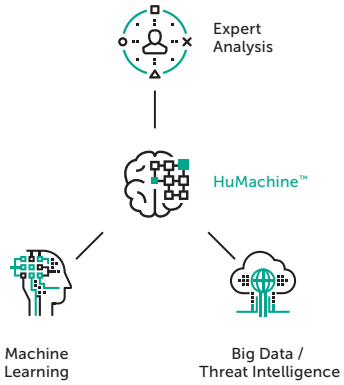
- High-level conclusions on the current security level of the systems in the scope.
- Description of the service methodology and process.
- Detailed description of detected vulnerabilities, including severity levels, exploitation complexity, possible impact on the vulnerable system, and evidence of the existence of the vulnerability (where possible).
- Recommendations on eliminating vulnerabilities, including changes in configuration, updates, changing source codes, or implementing compensative controls where vulnerability elimination is not possible.

About Kaspersky Lab

Kaspersky Lab, with its holding company registered in the United Kingdom, currently operates in almost 200 countries and territories across the globe, providing protection for over 400 million users worldwide. Kaspersky Lab is the world's largest privately held vendor of endpoint protection solutions. We are ranked among the world's top vendors of security solutions for endpoint users. For more than two decades, Kaspersky Lab has been an innovator in IT security, providing effective digital security solutions for large enterprises, SMBs and consumers.

Our most valuable asset is our wealth of expertise – including vulnerabilities and malware research, counteracting potentially dangerous applications, traffic filters, etc. – gained over 20 years of combating major IT threats. This helps us to remain a step ahead of the competition while providing our customers with the most reliable protection against new types of attack.

Learn more at www.kaspersky.com



Kaspersky Lab
Enterprise Cybersecurity: **www.kaspersky.com/enterprise**
Cyber Threats News: **www.securelist.com**
IT Security News: **business.kaspersky.com**

#truecybersecurity
#HuMachine

www.kaspersky.com