MANDIANT
NOW PART OF Google Cloud

DATASHEET

Embedded Device Assessment

Benefits

- Discover risks before your device goes to market
- Protect customer security and prevent reputational damage
- Improve the security awareness of your engineers

Why Mandiant

Mandiant has been at the forefront of cyber security and cyber threat intelligence since 2004. Our incident responders have been on the frontlines of the world's most complex breaches worldwide. We have a deep understanding of both existing and emerging threat actors, as well as their rapidly changing tactics, techniques and procedures.

Overview

Embedded Device Assessments highlight the strengths and weaknesses of a specific device as well as your team's development process. Understanding systemic flaws in the development process can improve the security of the device throughout its lifecycle.

This assessment addresses specific security aspects of the device based on the current state of its lifecycle, expected use and existing security hardening measures. Mandiant experts work with you to identify and accomplish mutually agreed upon security objectives.

TABLE 1. Security objectives over the lifecycle of a device.

	Device Lifecycle Stages			
	Design and Implementation	**Proof of Concept**	**Market Availability**	**End of Life**
Challenges	• Processor architecture • Kernel distribution method • Appropriate level of anti-tampering high security features • Available tools	• Design choice validation • Adequacy of security features • Use of up-to-date tools, libraries and software packages • Secure development practices	• Product safety for consumer safety and privacy • Validation of security claims	• Solid security throughout term of extended support contract
Example security objectives	• Validate decision choice prior to costly prototype production	• Evaluate development hygiene • Identify risks of hardware features • Reduce cost by identifying risks before production commitment	• Replicate malicious actor seeking to exploit product	• Conduct ongoing security testing

Service options

The assessment may be conducted in one of two ways:

- A black-box test, in which Mandiant consultants receive no prior information about the device
- A white-box test, in which your and Mandiant consultants discuss device design during the engagement

After the assessment concludes, consultants deliver documented recommendations to improve security for the assessed device.

How it works

Before they begin assessing an embedded device, Mandiant experts work to understand the threat model for the device's typical deployment scenario. This threat model helps demonstrate the real-world risk of any discovered vulnerabilities.

A threat model involves identifying all external inputs, determining accessibility from each input interface and determining internal connectivity. It also highlights a list of attack vectors and impact of compromise.

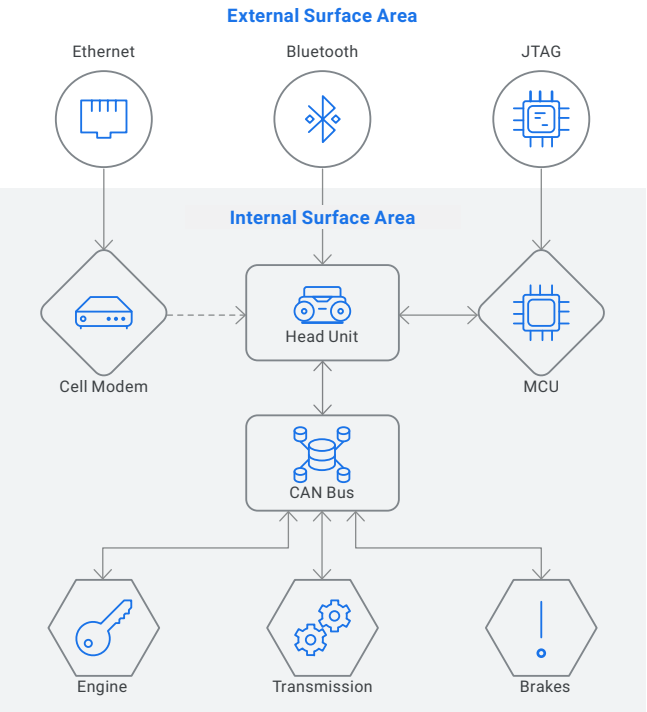

FIGURE 1. Sample threat model of a connected car.

Once a threat model has been developed, Mandiant experts probe all identified input and output interfaces to measure possible levels of interactivity and determine the external surface area for attack. These interfaces could facilitate access to a number of different protocols, such as:

- Common networking standards such as Ethernet or IEEE 802.11 wireless
- Personal area network standards such as Bluetooth/Bluetooth Low Energy or IEEE 802.15.4 and related application stacks such as ZigBee or Z-Wave
- Peripheral protocols such as USB, RS-232, RS-423, SPI or I2C
- Programming and debugging interfaces such as JTAG or ICSP

Mandiant experts attempt to gain information about device configuration and underlying programs by extracting and reverse engineering the device firmware, kernel or other information stored in non-volatile memory. Information obtained from these sources can help take control of the device and install backdoors, compromise the effectiveness of device encryption or take advantage of its trusted status within a larger system.

Internet of Things (IoT) or "smart" devices often have an associated mobile application or web services component. Mandiant experts can assess these for weaknesses, such as an insecure implementation of firmware updates. They use these findings to further compromise the device being assessed.

After a device has been compromised, Mandiant experts develop tools to demonstrate the impact of discovered vulnerabilities, such as compiling backdoor access tools for the device's specific architecture.

Deliverables

- Summary for executives and senior-level management.
- Technical details with step-by-step information that allow you to recreate our findings.
- Fact-based risk analysis so you know a critical finding is relevant to your device.
- Tactical recommendations for long-term improvement of your device's security throughout its lifecycle.