Embedded Software Testing

Test for vulnerabilities in a resource-constrained environment

Software defects in embedded devices can have a large impact on the reliability of systems upon which people's lives and livelihoods depend. That is why testing is a crucial component of the embedded system development process. We understand all the tradeoffs that must be made when creating a system and knows that balancing all the resources to meet aggressive timelines is no small task. This balancing act requires taking a risk-based approach to efficiently identify those defects which matter most to your business.

We stay ahead of the curve

From ATMs to automobiles to medical devices, we understand the unique resource constraints and security concerns of embedded devices due to the environment they are designed for. We also have the deep expertise required to effectively test the following constraints:

- Long lifecycles
- Limited or no user interaction
- Insecure physical environment
- Regulatory considerations
- Power constraints
- Connectivity with other devices
- Limitations on maintenance

We'll help you cross the finish line

At the end of each assessment, we will conduct a read-out call with your development team to walk you through:

- Descriptions of each vulnerability
- Reproduction steps (including exploit code if applicable)
- Screenshots (if applicable)
- The likelihood a problem will be exploited based upon attacker skill and access
- The impact if a vulnerability is successfully exploited
- A standards-based risk rating that combines likelihood and impact
- One or more recommended mitigation solutions tailored to address the unique limitations of embedded devices

Our risk-based approach combines three tracks of analysis

Our embedded software testing process takes a risk-based, systems approach that covers the following three areas:

COMMUNICATION ANALYSIS

Our experts intercept and analyze communication with other local or remote components (if applicable). Depending on the device software, this may or may not be possible without gaining privileged access on the client first (e.g. installing a trusted CA certificate on the device may be necessary). This step may involve communication over interfaces such as USB, serial, Ethernet, POTS, Wi-Fi, cellular, etc. We have experience working with many communication protocols commonly used by embedded devices such as Bluetooth low energy and ZigBee, as well as proprietary protocols.

CLIENT ANALYSIS

We test high priority areas and attempt to gain access to sensitive data or functionality on the device and escalate privileges until we can perform an attack that impacts one or more business risks. The activities during this phase are highly dependent on the specific device and attacks of concern, and may include chip removal, reverse engineering/tampering with device firmware, fuzzing inputs to processes running on the device, and finding kernel-level exploits.

SERVER ANALYSIS

We analyze the server-side software using various manual and automated tools once the communication channel between the client and the server is intercepted.

About Black Duck

Black Duck® offers the most comprehensive, powerful, and trusted portfolio of application security solutions in the industry. We have an unmatched track record of helping organizations around the world secure their software quickly, integrate security efficiently in their development environments, and safely innovate with new technologies. As the recognized leaders, experts, and innovators in software security, Black Duck has everything you need to build trust in your software. Learn more at www.blackduck.com.