SYNOPSYS®

www.synopsys.com |

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.

The Synopsys Difference

Synopsys offers the most comprehensive solution for integrating security and quality into your SDLC and supply chain. Whether you're well-versed in software security or just starting out, we provide the tools you need to ensure the integrity of the applications that power your business. Our holistic approach to software security combines best-in-breed products, industry-leading experts, and a broad portfolio of managed and professional services that work together to improve the accuracy of findings, speed up the delivery of results, and provide solutions for addressing unique application security challenges. We don't stop when the test is over. Our experts also provide remediation guidance, program design services, and training that empower you to build and maintain secure software.

For more information go to www.synopsys.com/software.

Synopsys Inc.
185 Berry Street, Suite 6500
San Francisco, CA 94107 USA

U.S. Sales: (800) 873-8193
International Sales: +1 (415) 321-5237
Email: software-integrity-sales@synopsys.com