SYNOPSYS®

CASE STUDY

Redesigning an Implantable Medical Device Communication Protocol

Customer overview

The first step of the project involved the identification of risks. An understanding of those risks would then drive appropriate system requirements. However, the firm was struggling to find consensus on how to go about doing this.

About the customer

A global leader in medical technology recently approached Synopsys for help. They were redesigning a communication protocol for an implantable medical device. The firm was struggling to identify whether the increased introduction of flaws was due to the redesign. At the time, the firm had no risk prioritization or management strategy in place to mitigate risks.

The firm engaged Synopsys to conduct a threat model assessment of their neuro-implantable system and Diffie-Hellman key exchange design proposals.

Alignment and risk challenges

The firm's development team had been leveraging widely recognized threat modeling tools, which reported an overwhelming number of flaws. This led to recurring discussions within their development organization about risk prioritization and mitigation.

Struggling with team misalignment

While upgrading the wireless capability within the neuro-implantable device, the firm became concerned about authentication. The solution that was previously in place relied on proximity to authenticate the device. This proximity-based authentication method required a cost-prohibitive electronic component. A primary goal of the redesign was to reduce the cost of the device by eliminating this specific component.

The firm was also trying to determine the risks of moving away from their current proximity-based approach. This change in design would remove their current means of authentication and replace it with a wireless key negotiation protocol.

The first step of the project involved the identification of risks. An understanding of those risks would then drive appropriate system requirements. However, the firm was struggling to find consensus on how to go about doing this. The business stakeholders liked the idea of a new wireless implementation because of reduced costs. The engineering stakeholders didn't agree. This approach would require the removal of the current authentication control—introducing security risks.

Throughout the development organization, recurring discussions ended in disagreement. Without clear visibility into present risks, the development of requirements wasn't progressing.

Struggling to identify real risks

Part of the risk identification problem was the previous approach. The threat modeling approach they had been using identified over 300 distinct risk items. Struggling with the sheer volume made the team unable to see the forest for the trees. Identifying the root causes of the items was a difficult and time-consuming task. But without identifying these root causes, the firm lacked clarity around the true risks.

Without clear visibility into present risks, the development of requirements wasn't progressing.

Struggling with risk prioritization and management

Without a clear understanding of potential vulnerabilities and impacts, the development team was unable to prioritize the risks. Additionally, they were identifying more risks than they were able to effectively mitigate. The key here is that they weren't able to identify which risks were most critical to resolve.

To resolve concerns relating to the use of wireless components, the firm was considering the implementation of a Diffie-Hellman key exchange security control. However, they didn't understand that Diffie-Hellman lacks authentication controls. Their new design didn't have the same authentication as their current implementation. This resulted in a lack of clarity around their planned security control implementing the key exchange.

Solution: Threat modeling

During the threat modeling process, Synopsys interviewed members of the neuro-implantable system team. The Synopsys team also reviewed design documentation to identify assets, threats, trust zones, potential attack vectors, and security implications of the proposed design.

Aligning the team

The threat model provided risk identification and a foundational understanding of these risks. This understanding resolved the team's confusion. They moved on to create concrete requirements with rationale in a matter of weeks. The team achieved this with a systematic, disciplined, and repeatable approach to risk identification. They produced artifacts communicating the impact of potential cost-saving decisions to engineering and management.

Identifying real risks

The threat model produced a traceability matrix of assets, threats, and potential attacks to controls and system requirements.

The Synopsys team identified risks and the underlying root causes. Those risks were then traced back to the security principles. With the risks, root causes, and security principles outlined in the matrix, it was now possible to define high-level draft requirements and test plans. These would help to reduce the risks to an acceptable level.

Benefits of threat modeling

- Get a blueprint of your system's attack surface: major software components, assets, threat agents, security controls, trust zones, and corresponding relationships between objects.
- Identify attacks that are unique to how your system is built.
- Easily update your threat model to accommodate new frameworks and highlight new threats.

The Synopsys threat modeling approach proved highly effective when compared to the firm's previous approach. Synopsys reported a smaller number of tangible risks for the firm's development team to focus on. Additionally, system-specific context highlighted the business impact, which allowed for greater understanding.

Prioritizing and managing the risks

In response to the identified risks, Synopsys provided recommendations to the firm's development team based on root cause analysis. After business impacts were identified, the risks could be prioritized to align with the firm's goals.

The highest risks related to

- the device's battery life,
- key disclosure,
- confidentiality, and
- integrity of communications.

This information would drive prioritized effort toward the highest risks, thereby ensuring high-level requirements were created to reduce each risk to an acceptable level. This would also be followed by appropriate verification and validation efforts.

Results and impact

The Synopsys threat modeling methodology provided traceability and visibility into the necessity of requirements. The process provided the firm with an effective and systematic method of making informed decisions—in particular, those relating to cost savings achieved by leveraging the wireless communications. Additionally, the development team saved time and effort by focusing on a small number of root cause issues, rather than several hundred risks.

The repeatable risk identification approach resonated with the development team. The prioritization of the threat model's results allowed the firm to kick off the design and implementation phases. The goal of these phases focused on risks and enabling the team to make informed decisions. Increased productivity ultimately led to the delivery of high-quality, actionable results. In the end, the team was able to implement these results immediately.

The Synopsys difference

Synopsys helps development teams build secure, high-quality software, minimizing risks while maximizing speed and productivity. Synopsys, a recognized leader in application security, provides static analysis, software composition analysis, and dynamic analysis solutions that enable teams to quickly find and fix vulnerabilities and defects in proprietary code, open source components, and application behavior. With a combination of industry-leading tools, services, and expertise, only Synopsys helps organizations optimize security and quality in DevSecOps and throughout the software development life cycle.

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: sig-info@synopsys.com