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.

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