Defending smart homes against AI Cyberattacks

By Steve Hanna, Distinguished Engineer, Infineon Technologies



In recent months, the cybersecurity capabilities of Large Language Models (“models”) have become increasingly powerful. Recent research shows that today’s frontier models (Claude Mythos and GPT 5.5) with proper tooling have cybersecurity capabilities similar to trained cybersecurity practitioners and are doubling their ability every four months. Access to these frontier models has been restricted, but independent researchers have found that open weight models available to anyone can achieve comparable results.

What does this mean for smart homes?

For years, we have known that usually software and firmware have many bugs, and some of those bugs may induce security vulnerabilities. AI tools can now be used to quickly find and exploit those vulnerabilities. The good news is that this capability can also be used by defenders. Companies that make software and firmware are increasingly using AI to speed the process of finding and fixing vulnerabilities in their own code.

Within a few years, a much higher level of security with more secure software and firmware can be reached. However, a few years are expected to pass with elevated numbers of vulnerability alerts, software updates, and breaches.

What can be done?

Fortunately, there are many opportunities to mitigate this risk.

First, consumers and device makers should use the Matter standard. This Smart Home interoperability standard was designed with security as a top priority. Zero Trust Architecture (ZTA) principles are built into Matter to protect IoT Devices against infection and minimize damage if a device becomes compromised. As a simple example, each Matter Device gets only the minimal set of privileges that it needs. Because Matter implements this Least Privilege principle, an infected light bulb can’t cause much harm because it has low privileges.

Second, device makers should protect important secrets such as encryption keys using chips that have certified security. Many of Infineon’s OPTIGA™ and PSOC™ products have widely recognized security certifications like SESIP, PSA, and even Common Criteria. With such certifications, device makers can have confidence that these products have been thoroughly checked by independent security experts.

Third, the software update process must move faster. Device makers should streamline their processes for pushing out software updates, so they can stay ahead of attackers. Consumers should quickly install these updates so that their smart home can stay protected against the latest attacks.

Conclusion

Although media has focused on the risks posed by the growing cybersecurity capabilities of AI, they have not generally covered the advantages that AI can bring for defenders. Even more important, they have only sparsely provided specific recommendations for actions that one can take to address this problem. With this blog, you have the tools you need to manage this risk.

https://community.infineon.com/t5/Blogs/Defending-Smart-Homes-against-AI-cyber-attacks/ba-p/1226935