Maintain a Safer Connection

By UL

For more information about UL's Cybersecurity Assurance Program visit UL.com/Cyber. To speak with a knowledgeable expert contact us today at ULCyber@ul.com.

Over the last several years, it has become clear that connected technologies – those that comprise the internet of things (IoT) – are only going to grow in significance, capability, and overall number. Today, these products span across commercial, residential, and industrial products and allow users to enjoy devices that seamlessly communicate with one another and broader systems. Naturally, as these devices have increased in popularity and function, they have also become more appealing targets for bad actors. According to recent sector reports, the number of attacks on these devices and the network they rely on has suffered from a substantial growth.

This surge in malicious activity highlights the mounting importance of software cybersecurity and the role it will play in helping to maintain the security, privacy and performance of the systems in these growing networks. As connected devices and the software they rely on are also growing in complexity and sophistication, cybersecurity evaluations are fundamentally important to help demonstrate performance and reliability, reduce downtimes due to system breaches, mitigate damage and risk, and assure overall security and soundness of systems and individual connected products.

Managing Cybersecurity in a Connected Era

Assessment of both known and potential vulnerabilities in software can help prevent the possibility of cyberattacks. For users, the IoT looks like a heterogenous network of sensors and devices that communicate both with one another and with cloud services, and, when everything is working well, all of this communication appears seamless and simple. However, the systems that support and enable this connectivity are incredibly complex. Each node contains a software stack, composed of low-level drivers to connect to Ethernet or WiFi, and by communication layers such as TCP/IP, application protocols such as HTTP and encryption/authentication in TLS.

Any individual piece of software can have vulnerabilities that, in a worst-case scenario, can lead to the device itself becoming completely compromised. Therefore, managing these systems means managing an ever-growing set of software and firmware for a multitude of different devices and architectures, as well as the continuously monitoring of the respective software bill of materials (SBOM) for each device. To keep such devices secure, they must be designed to allow for regular software update – over the air updates (OTAU) make this easier than ever – and patches help address vulnerabilities as they arise.

Staying Up-to-Date and Updated

IoT devices share the same risks as many traditional IT systems, but the overall landscape has shifted. First, the number of devices surrounding users in daily life and operating round-the-clock has risen dramatically. Secondly, because these systems appear to work so effortlessly, the current ecosystem is sometimes neglected in terms of patch management and system/software updates. Traditionally, it was an established practice to regularly keep computers, smartphones, and network softwares up-to-date to avoid open vulnerabilities, but IoT devices are occasionally overlooked because the manufacturer is not aware of a specific problem. When a hacker is able to access a device, this poses a risk for the privacy of the user itself (e.g. by eavesdropping using IoT sensors or stealing data) and the integrity of the system itself as this access point allows a hacker to move freely through the network, compromising additional devices.

Though there is a lot to consider in the security of today's networks and IoT devices and it is easy to become overwhelmed, the process does not need to become cumbersome. There are practices to help you design security into your products as well as standards specifying how to test cyber security in IoT devices to better understand and manage risks. By remaining aware of relevant challenges and working with a third party to help you evaluate and mitigate risks, better cybersecurity is easier to achieve than it may initially seem.

Reduce the Risks, Test Your Security

The first step for consumers and manufacturers alike is to maintain a critical view of devices. For example, is the device preloaded with a default password? That can be a significant problem as unique passwords are one of the first lines of defense. As a manufacturer, it is also necessary to adopt a secure product development process that includes clear definitions of how the device is enrolled (and what types of key material it handles in that process), how the integrated security is further developed and patched during its lifetime and how it is decommissioned. With this process developed, field testing and monitoring are critical. In addition to these internal efforts, engaging a third party, such as UL, to help test your processes and evaluate your supply chain can prove beneficial.

At UL, we recognized the shifting technology that was beginning to shape the IoT ecosystem and we developed the UL Cybersecurity Assurance Program (UL CAP) to help reduce security risks associated with a wide range of connected products, assessment and certification. UL CAP uses the new UL 2900-1 Standard to provide cybersecurity criteria that can be tested to help you evaluate vulnerabilities in your software and weaknesses in your supply chain. By working with UL to verify security of both products and systems, you can minimize damages, correct known malwares, and examine the security protocols you have in place.

Connectivity among devices will only continue to accelerate, making it difficult to predict where the market is headed or how bad actors will seek malicious involvement. The only thing we can say for certain is as sensors and circuits occupy more and more of day-to-day lives through new, exciting technologies, a focus on safety will only become more important.