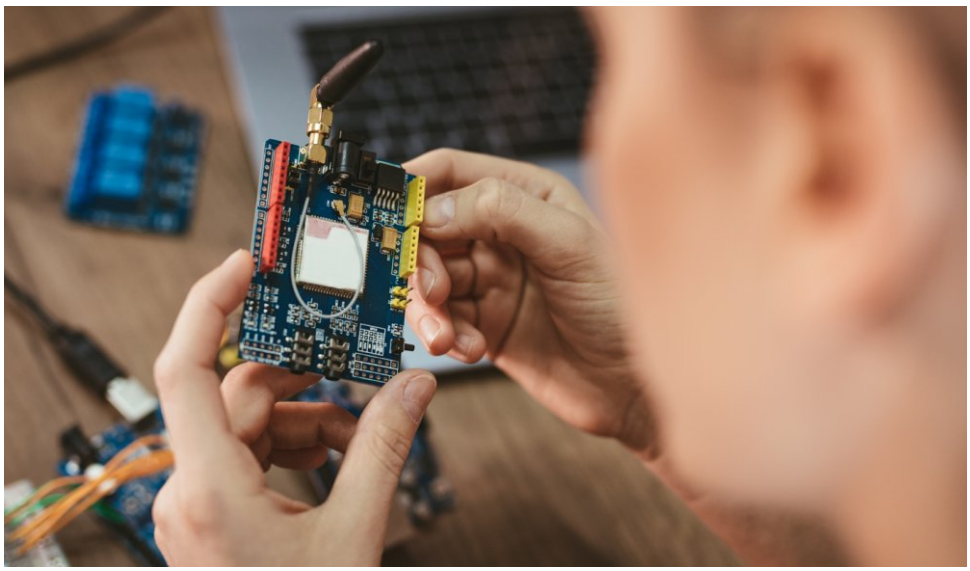
VANDERBILT

News

Vanderbilt discussions: We need to talk about IoT security

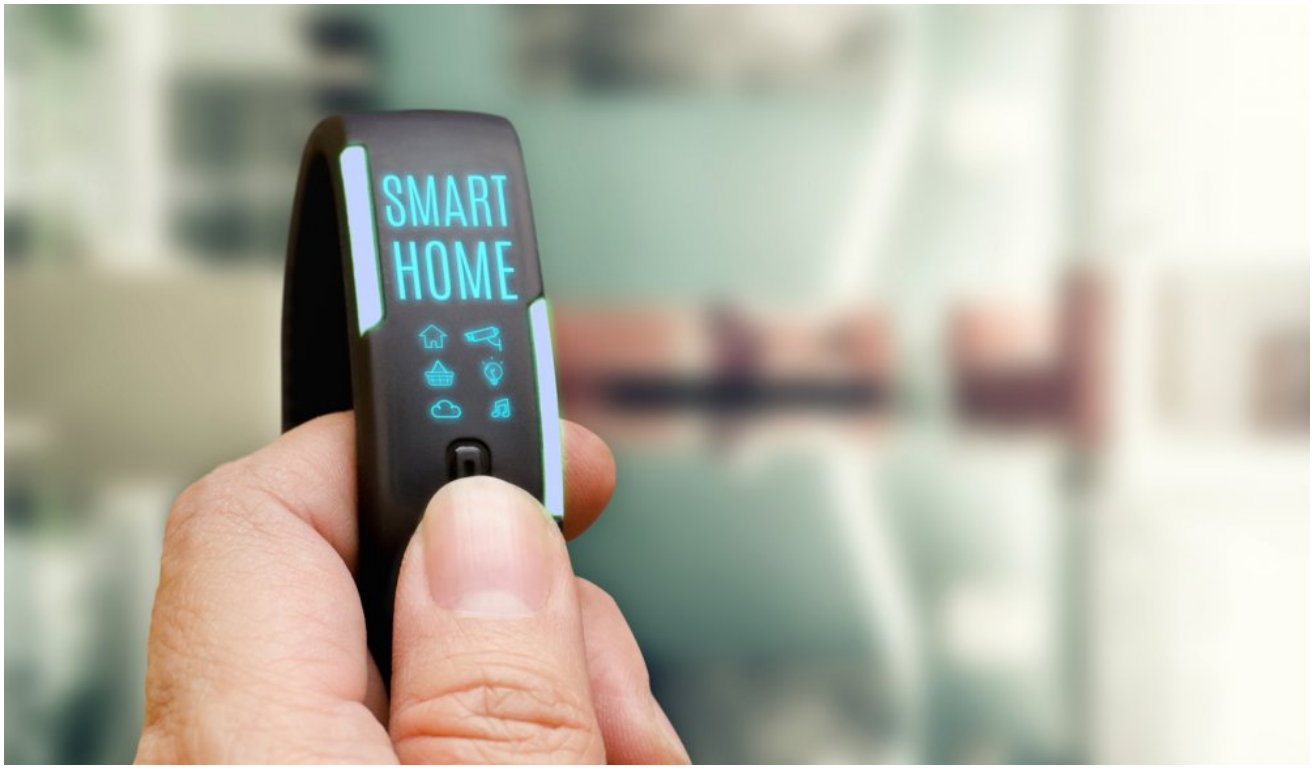


IoT technology is accelerating at such a pace that it can potentially create detrimental problems for which many organizations may be ill-prepared - or may not even be able to comprehend. Several flags have been raised already when it comes to the connectivity of IoT technology, and the debate still centers around who is responsible for the security of these kinds of devices.

When the internet first originated in the mid-90s, it was a utility only accessible through computers and dial tones. Now its reach is far and wide, and IoT technology includes everything from wearable devices that are equipped with sensors that collect biometric data, to smart home systems enabling users to control their lights and thermostats.

These devices typically come with built-in electronics, software, and sensors, **and are also assigned unique IP addresses**

. This allows them to communicate and exchange data with other machines. This design is built around convenience. But how much attention should be centered on security when designing these devices?



Unfortunately, all cyberhackers require is one weak link to infiltrate a system before spreading throughout a more comprehensive network. For instance, smart vending machines on a college campus were recently used as a starting point to launch a cyberattack against an unnamed university in the United States.

How IoT Devices are Compromised

Attackers employ a variety of methods to infiltrate devices and use them to gather, process, and transmit data. The more information the device can transfer, the more valuable it becomes, **making this hijacking more tempting and rewarding**.

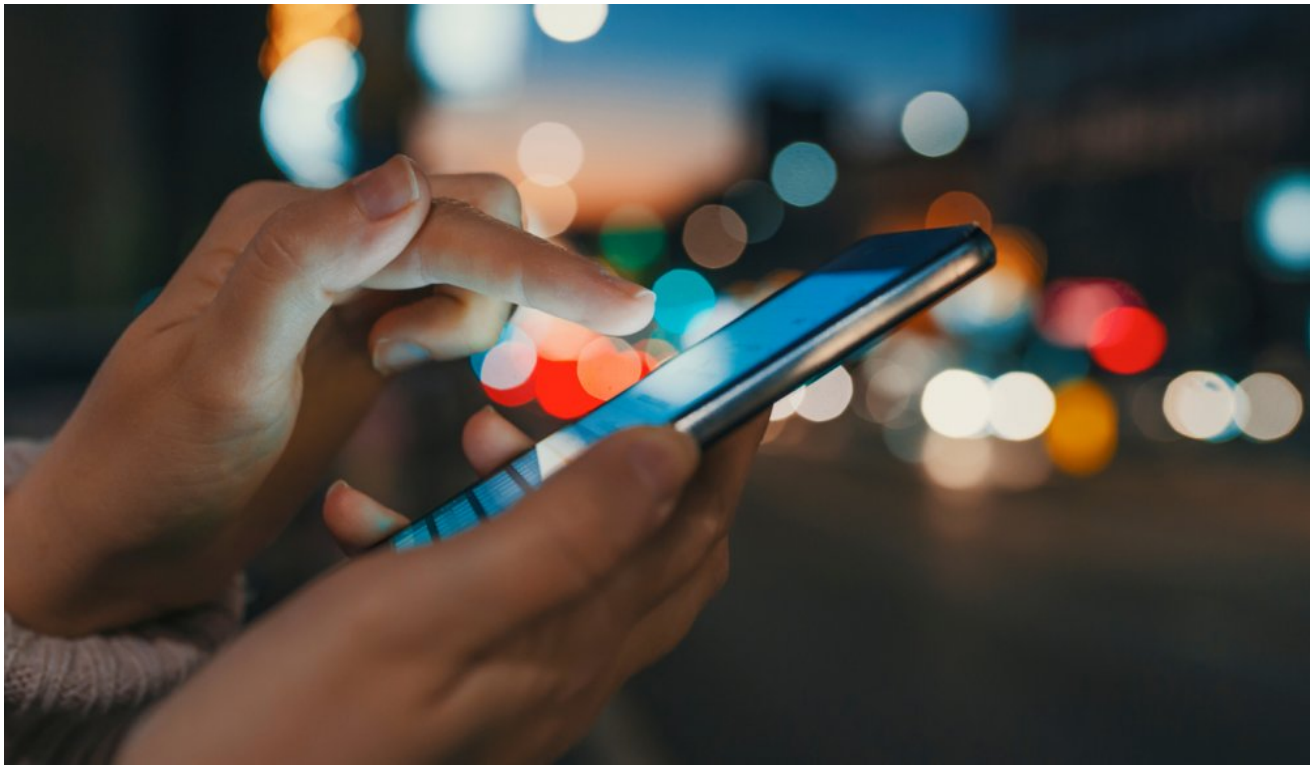
There are already millions of smart home devices in the world, including intelligent alarms, locks, lighting, baby monitors, thermostats and televisions. It is predicted that there will be more than 21 billion connected devices by 2020. For instance, Gartner recently predicted that IoT security spending would hit $1.5 billion by the end of the year, up 28 percent from 2017, and is **expected to more than double to $3.1 billion by 2021**.

Building a Secure IoT Device

In the IT industry, customer demand sparked the change to deliver robust security protocols, which manufacturers then implemented. Now companies like Microsoft and Apple openly fix software vulnerabilities on a regular basis, and no gloss is taken off the prestige of their brand for doing so, as this is what the consumer expects and wants of these software giants. This is the same mentality that needs to be adopted by IoT manufacturers.

IoT security falls on a number of entities to take responsibility for contributing to comprehensive IoT security: **the organization, the manufacturer, and the user**. The Vanderbilt SPC intrusion system takes the manufacturer's protection to a new level, as the goal of designing the solution was centered around its communications protocol with cybersecurity at its core. The entire protocol was designed to ensure everything is encrypted, all communications are monitored, and multiple types of attacks are considered for defensive purposes to provide the best security possible. Built-in protection mechanisms send the system into protection mode once its attacked by an outside source. While it will remain operational and still be able to communicate out, it will start to shut down elements of itself to protect the system from further attack.

Another way for manufacturers to deliver solutions that are protected from outside threats is through constant and consistent testing of the devices long after they are introduced to the market. Hackers wishing to do harm will stop at nothing to break into IoT-connected devices, taking every avenue to discover vulnerabilities. But a manufacturer that spends valuable resources to continue testing and retesting products will be able to identify any issues and correct them through regular software updates and fixes to deliver a secure device to consumers.



At Vanderbilt, we have always been an advocate of open platforms and integrations. That's why we have been integrating with some partners to provide better home automation and industrial solutions that have acquired a lot of interest from the market. We're seeing more and more drive for unified solutions, especially whereby there can be a separation of the security system and the home automation system. This allows people to use the home automation system they want in a secure way, while making use of the sensors and information available to them within their security system. By working with key partners, Vanderbilt can provide the best overall solution to our customers and we continue to explore these opportunities and interests to provide the most interesting innovations possible.

IoT security doesn't have to be an afterthought. It just takes a little more research – along with trustworthy manufacturers that take security to a whole new level and are ready for any

challenge.

#ReadyForAnyChallenge