SPOTLIGHT / DIGITAL SUPPLY CHAIN

IoT Proliferation Teeters on the Edge

By Alex Iuorio, Senior Vice President, Supplier Management and Business Development, Avnet Electronics Marketing

In his January 12, 2015 speech (https://www.whitehouse.gov/the-press-office/2015/01/12/remarks-president-federal-trade-commission) to the Federal Trade Commission on the growing cyber security threat, U.S. President Barack Obama declared: "If we're going to be connected, we've got to be protected." At the same time the President was speaking, hackers seized control of the U.S. Central Command Twitter account (http://www.washingtontimes.com/news/2015/jan/12/obama-lays-out-new-data-protection-bills/#ixzz3RdfKHUDf). The irony of this situation would be comical if the national security implications of the breach weren't so dire. But they were. And the clear takeaway from this scenario, and the many other high-profile hacks which have occurred since then, is that as connected as our society has become, we are still far from protected.

In fact, a report from digital security company Gemalto revealed that in 2014, more than a billion data records were compromised as a result of 1500+ data breaches worldwide—a 78 percent increase in the number of breached records in 2013. The Gemalto report notes that the size and frequency of these breaches continues to grow, despite enterprises spending $32 billion on security technology in 2013.

What these statistics reveal to me is that the current methods of enterprise security are simply no match for the cunning and malicious intent of today's cyber hackers. One shortcoming in many enterprise IT strategies, I believe, is the failure to recognize that cloud technologies and the Internet of Things make it very difficult for organizations to define, and therefore defend, the "edge" of their enterprise through traditional network perimeter security technologies.

Cloud technologies and the Internet of Things make it very difficult for organizations to define, and therefore defend, the "edge" of their enterprise

Companies will have firewalls to protect their server and storage networks, but they may not consider other potential points of entry, such as their connected lighting or HVAC systems. In addition, corporate bring-your-own-device (BYOD) adoption has opened a significant back door to many enterprise networks. According to a study released in 2014 by Hewlett-Packard (http://www.ibtimes.com/internet-things-very-susceptible-hacking-study-shows-1647924), 70 percent of devices connected to the Internet are vulnerable to some form of hacking. This security picture is likely to get exponentially messier with predictions of as many as 26 billion connected appliances and devices in the next five years.

Clearly, making the IoT more secure will require a multi-layered approach that can enable networks to be open to connectivity, while creating absolute data protection. While I am far from an information security specialist, my experience with state-of-the-art electronic component technologies leads me to believe that device-level authentication technology such as NFC and use of digital certificates (PKI) holds a

tremendous amount of potential for mitigating data security risks, including the pervasive man-in-the-middle (MITM) attack method.

Protecting enterprise IP in this evolving IoT era is undoubtedly the greatest IT challenge facing members of the electronics supply chain. There are no easy answers or silver bullets; but recognizing that traditional perimeter security strategies are insufficient to secure a network edge in the nebulous, virtually boundless Cloud is a crucial first step.

Related Resources:

- Article: IoT is connecting the edge to the enterprise (http://www.techcentral.ie/iot-is-connecting-the-edge-to-the-enterprise-to-boldly-go-where-no-tech-has-gone-before-says-avnets-murphy/?utm_source=twitterfeed&utm_medium=twitter)

- Article: IoT: More than just cool technology (http://www.ept.ca/electronics/iot-more-than-just-cool-technology/1003077590/?er=NA)

Alex Iuorio

Alex Iuorio is Senior Vice President of Supplier Management and Business Development for Avnet Electronics Marketing, Americas. Alex is a 35-year high-tech industry veteran who manages supplier programs and relationships to better meet the changing demands of the marketplace.