www.pipelinepub.com
Volume 16, Issue 11

IoT Security Standards & Collaboration

By: Bruce Lehrman, Scott St. John

The demand for connected devices is seemingly insatiable. Based on most estimates, there are billions of connected devices online today, generating hundreds of billions of dollars in revenue, and this is estimated to grow to over $1 trillion across Internet of Things (IoT) market segments by 2026. Add to that another $13 trillion in estimated IoT platform revenue and the predicted momentum behind IoT is truly astounding.

When you drill down a little deeper, you see there is a wide range of IoT devices behind this boom, spanning everything from your video doorbell to appliances, industrial equipment, data centers, medical devices and extraterrestrial satellites. Whether we use them at home, manage them at work, wear them, or have them physically embedded inside of us, one thing is certain: we are really just beginning to scratch the surface of the IoT opportunity and the grave risks associated with it.

Just under four years ago, a brute-force DDoS attack against Internet service provider Dyn was launched using the Mirai botnet, leveraging millions of IoT connected devices—such as relatively inexpensive webcams and DVRs—to bring down nearly 1,700 commercial websites including Amazon, Paypal, and Netflix, and knock out the Internet across most of the Eastern United States. The damage estimates are staggering and encompass (nearly 10 percent of) Dyn customers who churned in the wake of the attack, and the loss of business from some of the world's largest online marketplaces. Today, a single cybersecurity breach can cost a company millions to tens of millions of dollars in damages and recovery costs.

While the Dyn attack may seem like somewhat old news, it marked a tipping point in IoT security at a time when IoT was just taking off. The Dyn attack demonstrated the use of an unprecedented

number of devices, speed, coordination, and regulatory response. While prior attacks leveraged hundreds of devices, the Dyn attack leveraged millions. Prior attacks had reached speeds of 620 gigabytes per second, but the Dyn attack set record speeds at 1.2 terabytes per second. The size, speed, and level of sophistication or this attack is a bad omen. The Mirai botnet is now widely dispersed, making this type of attack more likely—and raising legitimate security concerns that the frequency and severity of these types of attacks is expected to increase.

What's more, the increased frequency and severity of attacks like these have prompted a global IoT security response. With the ever-increasing concerns for data privacy, regulators have been frantically scrambling to catch up. This encompasses everything from new regulatory compliance criteria for cybersecurity certification, to significant penalties (up to $7,500 per incident), and regulatory liability (such as GDPR) for future breaches—which equates to tens of millions of dollars, at a minimum. In fact, the proposed California legislation attempts to protect consumers by enabling them to sue device manufacturers for statutory damages for data breaches, and the proposed UK regulation goes so far as to allow the government to seize and destroy non-compliant IoT devices.

But the potential threat of regulatory penalties and civil liability actually pales in comparison to the magnitude of damage that could be wrought as literally billions of IoT devices continue to come online. It's not so much what these devices are as much as it is what they do, how mission critical they have become, and how they could be misused for malfeasance. IoT connected devices control portions of the power grid. They are used in medicine for things such as insulin pumps and pacemakers. IoT connected devices are used in agriculture to help control and manage the global supply chain. They are used for air traffic control, banking, self-driving vehicles, dynamic highway traffic control, and much more—most of which has already been hacked or proven to be vulnerable to attack. All of this makes the potential and even damaging attacks practically imminent—and the dispersion of malware such as the Mirai botnet, and the possibility of new more destructive variants, frankly more alarming.

Experts have been calling for wide sweeping action from government regulators, connected device manufacturers, IoT vendors, standards development organizations, and everyday citizens for years now. Yet surprisingly, the regulation has been met with opposition. And, while there are IoT standards development organizations making headway, you probably don't know them well. At least not yet.

Pipeline recently had an opportunity to interview Joerg Borchert, president of Trusted Computing Group (TCG); Amy Nelson, TCG's technical committeeco-chair; andThorsten Stremlau, TCG's marketing chair. TCG has been answering the call for better device security since its genesis as the Trusted Computing Platform Association (TCPA) in the late 1990s. In 2003, the organization evolved into its current state and now TCG encompasses the world's leading device manufacturers, government regulators, research and academic institutions, other standards organizations, and IoT companies.

TCG is a diverse organization that works with a wide range of companies located around the world. Its members come in all sizes. Members include many smaller start-ups as well as the world's leading software and hardware companies. TCG's board of directors includes distinguished members from companies such as AMD, Dell, Fujitsu, Huawei, HP, IBM, Infineon, Intel, Lenovo, Juniper, and Microsoft. TCG works with global governments, standards bodies such as NIST, security experts, and key research and academic institutions to identify, define, develop, produce and promote security standards generated by nearly 20 different working groups. Its members leverage, adopt, refine, and use the IoT Security Standards TCG develops to implement the latest IoT security protocols.

TCG's many workgroups focus on specific security areas such as cloud, cyber resilience, cybersecurity, industrial, IoT, mobile, and PC to name a few. It also provides a resource center where security professionals can go to view and download FAQs, specifications, reference documents webcasts, white papers, and more.

Getting involved

TCG has several levels of **participation and membership**. At the Adopter level, members can consume the IoT security standards and related content, and have limited input into standards development. Contributors fully participate in the development formation of standards, including early review of standards and standards voting rights. Promoter is the highest level of membership, enabling the most access with participation into technical committees, which act as an arm of the board of directors. Individual Liaison members are also selected from key subject matter experts, government organizations, researchers, and academics.

"The level of influence members have is directly proportional to their level of desired participation," Nelson told *Pipeline*. "Members can join at the Adopter level in "read-only" mode to consume standards and specification and apply it to their business—and at the next level up—Contributor members can fully participate in the formation of standards."

"Hardware-based security is the foundation for much of what we do, which has never been more important," Borchert commented. "As security has evolved, we have continued to develop standards in all their forms, including many different use cases for securing data on the device, in transit, and located in the cloud."

"Everyone that is developing hardware or software products we feel should want to participate in the standards that TCG is working on now," added Stremlau. "We've seen a significant peak in demand from our members for use cases for securing everything from embedded webcams to secure satellite communication, and from the world's leading technical innovators, who are looking to contribute to the development of security standards."

Stremlau then went on to underscore the importance and ubiquitous aspect of data security and how it permeates virtually every workgroup.

"TCG has many workgroups that are developing standards that can be used across hundreds of different applications, and data security is a key current that runs through each of them."

Participation is paramount

TCG's framework works as building blocks that enable organizations to pick and choose which elements of their standard and what level of participation are right for them. The TCG standards can be applied across all vertical IoT markets. TCG and its members have been hard at work developing security standards at a time when they are so critically important. But prevention does require effort.

Whether you are developing the next connected device, car, or "thing," there are many ways to start getting involved, from consuming the TCG standards and specifications, to actively contributing in committees and workgroups, and even driving the topical areas on which those groups focus. We've seen that the cost of not acting has been high in the past, and failing to act now may cost you a lot more in the future.