AXIOM
AN AVNET PUBLICATION

Clear and Present Danger: Intel Delivers End-to-End Security for the Internet of Things

Willie Chow – *Internet of Things Channel Architecture Manager, Intel*

Think your devices are secure? Think again. In June 2016, IOActive* released a sobering set of findings from its Internet of Things (IoT) Security Survey of senior security professionals.[1] A full 85 percent of those surveyed believe that less than half of all IoT products are secure. In fact, that may be an optimistic assessment, given that an earlier study by HP's* security unit, Fortify, found that 70 percent of popular consumer IoT devices are easily hackable.[2]

We're all aware the IoT is fostering innumerable advances that are making people's lives better and expanding business opportunities across nearly every sector. But the security concerns associated with the IoT also pose very real challenges to consumer safety and business revenue, as the very connectivity that forms the basis of the IoT also creates openings for attacks that span data, devices and systems.

Consider, for example, a factory floor where programmable logic controllers are used to operate robotic systems. Assuming the PLCs are integrated with the enterprise IT infrastructure, how can they receive security patches in a timely manner? And how can they be shielded from human interference?

> *"…70 percent of popular consumer IoT devices are easily hackable."*

Now imagine a smart meter that sends energy usage data to a utility operator for dynamic billing and real-time power grid optimization. How can both the meter and its data be protected from unauthorized access without hindering performance?

In response to these and other IoT security challenges, businesses need to adopt a multilayered approach that integrates device and data security into IoT solutions from the outset of their design and development. That is precisely the approach Intel® is taking. As the world's leading chipmaker, Intel is also a leading provider of fully integrated hardware- and software-based security solutions that span entire IoT platforms.

The Opportunities and Challenges of Networked Devices

An example from the healthcare industry demonstrates the opportunities and challenges of IoT solutions—and the need for built-in security measures. One of the most exciting opportunities in IoT is the development of networked medical devices, including wearable, temporarily ingested and embedded devices that can be used for medical treatments, medication and general health and wellness.

Deploying so-called "cyber-physical systems" could save $63 billion in healthcare costs over 15 years, including reductions in hospital equipment expenditures and improvements in patient throughput.[3]

However, the many benefits of networked healthcare can only be achieved if product developers and engineers can find a way to overcome a variety of significant security challenges. Specifically, a report by Intel Security and the Atlantic Council titled *The Healthcare Internet of Things: Rewards and Risks* details four primary areas of concern: accidental failures, theft of personal information, intentional tampering with devices to cause harm and widespread disruption (spreading malware across connected devices).[4]

The report also provides detailed recommendations to encourage innovation in networked medical devices while at the same time addressing the many security risks. One key recommendation is that security should be built into devices as well as the networks they use from the outset, with device manufacturers adopting a "secure-by-design" approach to research and development of IoT solutions.

"Adding security features to products after their initial rollout is a losing battle," the report states. "It is simply too costly and ineffective to try to secure systems already in the possession of the end user."

Intel believes security must instead be integral to a device's basic functions, with software security controls introduced at the operating system level. In addition, devices need to take advantage of the latest hardware security capabilities. In other words, a holistic, multilayered approach to security is necessary.

Built-in Protection, from Things to Cloud

The best way to protect sensitive data while also preventing and limiting device thefts and malware attacks is with end-to-end security solutions. That's why Intel offers hardware- and software-fortified security that creates a chain of trust extending from the "thing" (device, sensor, etc.) to the network to the cloud. Intel solutions safeguard valuable data against theft and tampering, ensure only trusted data is analyzed, and protect against attacks.

Critical to the security provided by the Intel® IoT Platform are Intel® IoT Gateways (https://www-ssl.intel.com/content/www/us/en/embedded/solutions/iot-gateway/overview.html), which support comprehensive device protection that extends from a hardware root of trust through boot and software loading. Intel Gateways also provide a number of advanced security features—including hardware identification, whitelisting and secure boot—that enable data to flow safely between edge devices and the cloud.

> *"The best way to protect sensitive data while also preventing and limiting device thefts and malware attacks is with end-to-end security solutions."*

Through hardware identification, Intel Gateways provide a unique hardware ID for every edge device so that it is clear which device is being communicated with and whether it is approved. Whitelisting allows the user to determine which agents are allowed to run on each device while blocking all others that may not be approved or secure. And the secure boot feature helps ensure that devices can be trusted every time they boot up, with the devices effectively checking themselves against a known good image.

With the help of McAfee® Embedded Control security technologies (http://www.mcafee.com/us/products/embedded-control.aspx), Intel Gateways also integrate the hardware-based security of Intel processors with operating system and application software security. That enables data to flow seamlessly and securely from the edge to the cloud, with data protected at rest and in motion.

Step Up IoT Protection with Intel's Multilayered Security Solutions

A closer examination of three additional Intel Security products is helpful to understand the depth and breadth of Intel's multilayered approach to IoT security.

The first product is Intel® Enhanced Privacy Identity ID (Intel® EPID) Digital Signature Technology, which provides an immutable hardware root of trust so IoT networks can identify devices and secure their communications. More than 1.1 billion Intel EPID certificates have already been deployed as security baselines across networks.

Intel EPID improves interoperability, making it easier for devices to connect securely to the Intel IoT Platform. The solution allows developers to establish a basis for trust, authentication, inclusion in relevant system relationships, and authorization for data access and actuation.

In addition, it helps protect personally identifiable information in connected devices. So, for instance, Intel EPID could be used to allow a car to connect to smart infrastructure without disclosing any information other than verification that it's part of an approved group.

A second powerful IoT security solution from Intel is McAfee® Enterprise Security Manager (McAfee® ESM) (http://www.mcafee.com/us/products/enterprise-security-manager.aspx), which works with McAfee® Threat Intelligence Exchange (http://www.mcafee.com/us/products/threat-intelligence-exchange.aspx) to fight advanced security threats. Together, the solutions provide situational awareness, actionable intelligence, and the instantaneous speed necessary to identify, respond to, and proactively neutralize threats.

McAfee ESM correlates insights from McAfee Threat Intelligence Exchange and provides advanced alerting and historic views to support security intelligence, risk prioritization, and real-time situational awareness. Unlike standard security approaches, this combined solution provides not only detailed file-level insights but also a complete and automated, closed-loop workflow from discovery through containment.

A third example of Intel's IoT security solutions is Intel® Security Critical Infrastructure Protection (Intel Security CIP) (http://www.mcafee.com/us/solutions/critical-infrastructure.aspx). Intel CIP separates the security management functions of a platform from the operational applications. That allows the operational layer to be secured, monitored and managed—all while working with both new and legacy infrastructures.

The goal of Intel Security CIP is to secure the electric power grid, and field tests have shown that it can do so while meeting National Institute of Standards and Technology (NIST) standards. The solution provides a secure managed platform with building blocks including device identity, malware protection, data protection, and resiliency, all tailored to modern machine-to-machine environments.

In the future, Intel Security CIP may be used in medical applications, the oil and gas industry, and other applications.

The Future of the IoT Depends on End-to-End Security

As every IoT engineer and developer (and now business leader) are well aware, security is paramount for the safe and reliable operation of IoT devices and the success of every IoT business venture.

The challenge is to implement effective and efficient end-to-end security measures at the device, network and system levels. Most experts also agree that security needs to be built in from the start, with device and data security fully integrated to protect all IoT applications and solutions.

Intel is a leading IoT innovator with a wide array of advanced solutions that together provide the multilayered security the IoT demands. As the world's leading chipmaker, Intel has been providing chip- and server-level security for decades, and has also emerged as a leader in data security solutions that protect data across transport, storage, and processing.

From encryption to access and identity management, Intel understands and has experience meeting and surpassing the unique security requirements of a broad range of end-market IoT applications and solutions.

For more information on end-to-end IoT security, contact http://www.mcafee.com/us/index.html (http://www.mcafee.com/us/index.html)

*Other names and brands may be claimed as the property of others.

[1] www.ioactive.com/news-events/iot-products-have-inadequate-security-according-to-practitioner-survey.html#_edn1 (http://www.ioactive.com/news-events/iot-products-have-inadequate-security-according-to-practitioner-survey.html#_edn1)

[2] http://www8.hp.com/us/en/hp-news/press-release.html?id=1744676 (http://www8.hp.com/us/en/hp-news/press-release.html?id=1744676)

[3] www.ge.com/sites/default/files/Industrial_Internet.pdf (http://www.ge.com/sites/default/files/Industrial_Internet.pdf)

[4] http://www.mcafee.com/us/resources/reports/rp-healthcare-iot-rewards-risks.pdf (http://www.mcafee.com/us/resources/reports/rp-healthcare-iot-rewards-risks.pdf)

Willie Chow

Willie is Intel's Internet of Things Channel Architecture manager orchestrating design programs to enable and to extend reach to the IoT Solution Integrators through value added distributors, IT Integrators and Operation Technologies communities. Prior to joining Intel, he worked for Cisco's IoT Go To Market team within the Worldwide Partner Organization for 10 years supporting Physical Security, DMS, MXE, Sport & Entertainment, and Connected Energy which expanded into the Internet of Things for transportation, energy with Oil and Gas, Smart City and Industrial factory automation. In addition, Mr. Chow also worked as a principal engineer managing the integrated solution needs of global and Federal customers at Tyco International, or currently known as Tyco Integration Services.