Internet of Things
Security Backgrounder

Confidence, Safety and Security in the Digital World

The Internet of Things (IoT) has the potential to transform our world and reshape the way we interact with our environment. Millions of previously unconnected devices will soon begin to transmit valuable data to the cloud and to each other, making us even more reliant on the Internet and the technology that enhances our daily lives. Data is crucial in the Internet of Things, as it enables new insights and innovations in automation. Sensors and devices are constantly sending and receiving information, presenting a challenge of extraordinary scope and complexity for companies transforming their operations. Intel has the technology, expertise and reach to bring simple and secure IoT solutions to new industries, helping to accelerate the development and deployment of new products while ensuring security.

Intel sees security as one of the five fundamental pillars for IoT solutions. With decades of experience in computing, Intel Security takes a holistic view of defending against the threat lifecycle, with solutions that protect against attack, detect compromises, and correct or remediate to restore normal operations. The very nature of the Internet of Things means that any disruptions can be very damaging. Technology companies have to make sure security is woven into the fabric of the connected world. The Intel® IoT Platform can help system integrators create new applications that feature security as a core component for specific industries.

The Challenges in Securing the Internet of Things

IoT systems interact with the physical world and increasingly operate within critical infrastructure such as utilities and transportation. This means that security solutions have to flip the usual considerations when securing solutions, focusing on delivering availability first, followed by integrity and confidentiality. The very nature of IoT presents a new set of challenges that developers and system integrators historically haven’t had to deal with, including:

- A long, complex lifecycle in which devices are not rebooted often, if ever, makes continuous threat prevention imperative. Critical security updates must be delivered while ensuring uptime.
- Devices are often part of a system of systems – complex networks that need to be secured along multiple endpoints and communication channels.
- IoT solutions often rely on devices that are mass-produced in the same configurations, leaving a broad swath of systems that can be left vulnerable without proper installation and updates.
- Gateways represent a great opportunity to include legacy equipment in IoT, but because these devices were never intended to be connected, they do not have

even the most basic security protections. The gateway needs to act as a "helper" to protect the edge.

- IoT is a very big space. When thinking about a solution, we need to consider security at the device level, the connectivity level and the cloud level in order to understand the potential threats to deployments.
- IoT devices could be used in different environments with vastly different risk profiles. For example, a temperature sensor might be used in a home or in a nuclear reactor, each with very different device security, data protection and encryption needs.
- Machine-to-machine communication presents a bigger challenge in terms of device identity. Security solutions have to verify the veracity of device data and identity while also ensuring data is protected as it travels to the cloud.

These challenges mean that companies pioneering the Internet of Things have to think differently about security. While there is no "silver bullet" to secure IoT, building solutions that treat security as a foundational element will allow us to offer peace of mind to consumers and enterprises, capitalizing on the promise of connectivity.

Addressing Security at All Levels

Intel Security takes a holistic approach to preserving the integrity of IoT solutions with a strategy of delivering IoT-appropriate software products, providing a robust hardware foundation built into Intel processors and SoCs, and offering platforms for integration with third-party security solutions. Our goal is deliver across IoT from end-to-end by hardening devices, securing communications and analyzing and monitoring networks while managing the complexity inherent to IoT. This means our customers can focus on creating new products that have security woven into their fabric.

While security fundamentals are consistent across the different market sectors involved in IoT, there is also a need to understand the specific risk profiles and implementation constraints for individual use cases. That allows us to tailor solutions for optimal cost benefit.

An example of a tailored and comprehensive offering is Intel Security Critical Infrastructure Protection (CIP). Intel Security CIP is a pre-integration of Wind River and McAfee branded products designed to provide end-to-end security for systems with the highest protection requirements. We've made use of Wind River's virtualization and secure operating systems plus McAfee integrity, network security and management technologies and have configured them to take full advantage of Intel silicon-level features. This delivers a complete solution for critical infrastructure providers.

Another example of a market-specific effort is the work Intel is doing in automotive security. In addition to delivering hardware security features plus Wind River and McAfee products to protect cars, we have undertaken an industry effort to learn from the best security researchers to improve best practices broadly. We have established the Automotive Security Review Board and have published a white paper, Automotive Security Best Practices to engage with other well-informed stakeholders to revise and drive these efforts to the broader benefit.

Companies developing IoT products have access to McAfee Embedded Control, which allows for whitelisting of products on networks to prevent rogue applications from running on devices. Additionally, McAfee ePolicy Orchestrator (ePO), which has been successfully helping enterprises manage hundreds of deployed devices with ease, may also be used to perform security management on IoT devices. McAfee ePO provides a platform for innovation, with more than 100 partners developing innovative applications to address the problems facing enterprises and system integrators today. Intel is bringing this product that has proliferated in the enterprise to address the needs of IoT solutions requiring the safekeeping of many devices in complex networks, offering easier updates and visibility into authorized and unauthorized security events. Lastly, Intel customers gain access to McAfee's Global Threat Intelligence technology, which leverages information from 1 million devices in 120 countries, collecting intelligence data to help companies fight against malicious agents.

Intel solutions also feature a hardened foundation, with security built into systems at the silicon level. Intel Data Protection Technology for Transactions, which is designed for use in retail point-of-sale systems, uses a trusted execution environment in Intel silicon to separate sensitive data from the solution's software, employing whitelisting and encryption capabilities built into the hardware to ensure security. The product ensures that information is securely handled throughout the entire chain of a connected solution, as it passes from peripheral devices to terminals, and eventually to the cloud for processing and analysis. Although this technology was initially developed with NCR for the retail industry, it can be used to secure all manner of IoT solutions. As connected solutions become more common in our daily lives, consumers will need reassurance that their personal information is being safeguarded regardless of the setting and platform.

Another example of hardware-based security technology that is very useful to IoT is Intel Enhanced Privacy ID (EPID). EPID may be used for very robust device identity, which is critical for IoT. It's imperative that the IoT system be able to trust that the data it's using is coming from a known and secure device. EPID goes a step further by offering anonymity-preserving properties that allow the device to be securely identified as part of a group. The oft-cited example of this is that of a smart driver's license. It could identify the bearer as being in the group of people of a legal age to drink without revealing address, driver's license number, actual birthdate, etc.

Intel Security also focuses on protecting industry innovation by building new products and platforms that make it easy for developers to secure their IoT solutions. The Intel IoT Platform gives system integrators a clear path that allows for specialization while taking care of complex security considerations. Additionally, Intel is constantly rethinking protection in order to innovate how we approach security in a rapidly changing technology environment. For example, in rethinking the concept of “trust,” Intel has evolved the process of attestation into a multifaceted approach in which devices and data centers must affirm their identity to each other. With this approach in mind, Intel has developed a number of technologies that force devices to prove multiple pieces of information about them, leading to more complex systems to safeguard data. Additionally, Intel has technology built into the silicon that allows only whitelisted software stacks to run on a device to prevent rogue agents from infiltrating the network by hijacking trusted devices.

Conclusion

The Internet of Things has the promise of improving our lives and our world, but we must design our systems with security and privacy built into them from the outset. Intel Security is committed to making that easy and effective for our customers.

# # #

CONTACT: Sal Viveros
+44-7921-891-506
salvador.viveros@intel.com