WHITE PAPER

Industry
Solution Focus Area

Enhancing National Cybersecurity for a Safer World through the Internet of Things

Intel Corporation Contributors:

Bridget Karlin
Eve Schooler
Sven Schrecker
Lorie Wigle
Marjorie Dickman

Intel believes the Internet of Things (IoT) presents a transformational opportunity for the U.S. and the world. It will enable innovation, increased productivity, and new efficiencies across the public and private sector. With an estimated 50 billion devices and 212 billion sensors expected to connect to the Internet by 2020, the IoT offers unprecedented global economic and social opportunity. The IoT presents the opportunity to connect these devices, efficiently analyze the data, and use that knowledge to improve real-time decision making and address societal problems. And in doing so, IoT is expected to have a multi-trillion dollar global economic impact.

There are several potential barriers to delivering on the promise of IoT, if not properly addressed. Intel prioritizes security and recommends the following actions to address this challenge.

Establish Security as the Foundation

It is important that the IoT is secure from the sensor to the cloud, including all hardware and software. Intel believes that the strongest foundation for a secure IoT is integrating security capability at the outset. Starting with the development and design phase of all cyber physical systems and their components, security must be designed in from the beginning. We must also develop infrastructure compute capability and include security algorithms alongside Internet infrastructure, to enable the attestation of the integrity and authenticity of IoT elements as they move through the hardware manufacturing lifecycle, the software integration phase, user deployment, and data creation process. As Intel prioritizes security as the foundational element in our IoT solutions, we are building cryptography into our chips to enable strong identity and data protection. On top of security in the compute device itself, our IoT solutions employ advanced hardware and software security to prevent harmful applications from being activated on the device or from taking down the network. (Figure 1. Intel® IoT Platform Reference Security Model on page 2.) Why is this important? Because integrating multiple layers of security at the outset enables trusted data necessary for successful IoT deployments.

Table of Contents

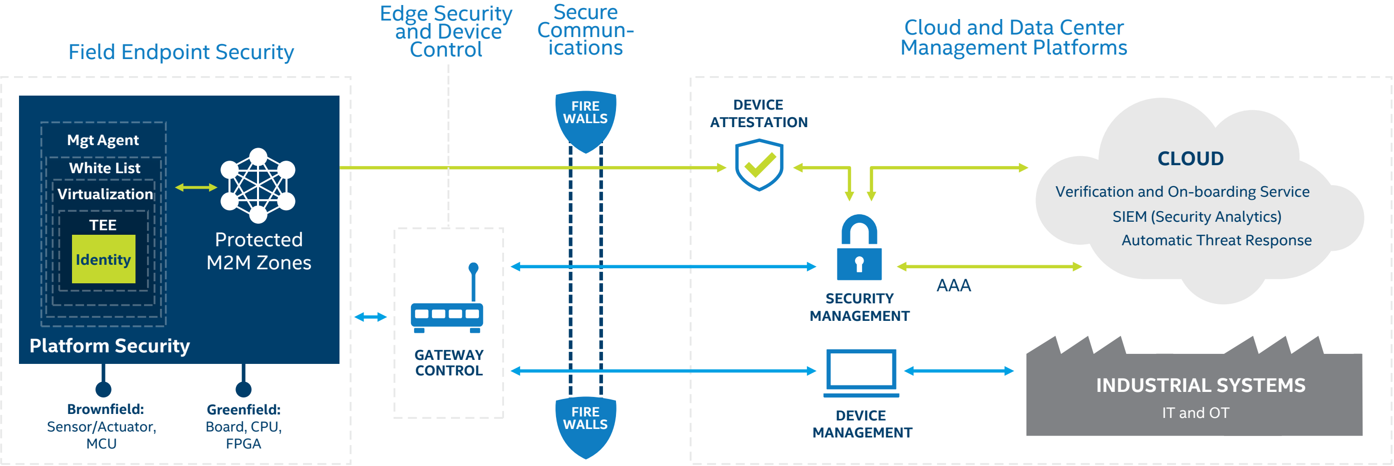

Figure 1. Intel® IoT Platform Reference Security Model.

An example of an important Intel IoT security technology that is both hardware-based and software-enabled is Intel® Enhanced Privacy ID (Intel® EPID). Intel EPID may be used for very robust device identity, which is critical for IoT. It is imperative that an IoT system be able to trust that the data it's using is coming from a known and secure device. Intel EPID goes a step further by offering anonymity-preserving properties that allow a device to be securely identified as part of a group, without revealing its specific individual identity within that group (see Figure 2. Intel® Enhanced Privacy ID vs. Public Key Infrastructure). To enable the industry to incorporate this level of hardware security, Intel has released this technology for broad licensing and it has been adopted as an industry standard. Why are these strategies important? Because integrating multiple layers of security at the outset enables more robust IoT deployments and because offering open standards makes security more widespread in the massively-connected IoT ecosystem. The U.S. government should encourage open security standards to maintain the long term viability of IoT and to foster solutions that are interoperable and reusable across a variety of use case deployments, vendors, sectors, and geographies.

Establish a Chain of Trust

We must be able to rate the trustworthiness of IoT elements, so that users (and the devices or wearables that serve as their proxies) can decide which trusted devices are safe to connect to or allow connections from, which cloud infrastructure offers the safest haven for data storage, which is the best dataset to use for reliable decision making, and how to gage what constitutes normal versus anomalous behavior in IoT systems. A chain of trust must be established so that we are able to attest to the trustworthiness of devices during their life cycle, beginning with manufacturing and later during provisioning, then deployment. With an established chain of trust, there is a foundation established for trusted analytics and in turn, trustworthiness of the decisions being made from the analytics. Intel believes that all participating IoT elements should be architected to enable some degree of direct measurability, not only for security, but also for reliability, safety, and optimization. Analytics on these measurements can boost our ability to identify anomalies and violations in a timely manner. Technologies such as blockchain also offer promise to validate reported measurements and transactions. To help align the industry toward achieving trust, it would be beneficial if there were standards-based common criteria that could serve as guidelines to help specify the security goals for IoT systems and how to measure against those goals. One outcome would be for all IoT elements to be able to report the degree to which they meet these criteria, assisting with the evaluation of trustworthiness and the strength of security offered.

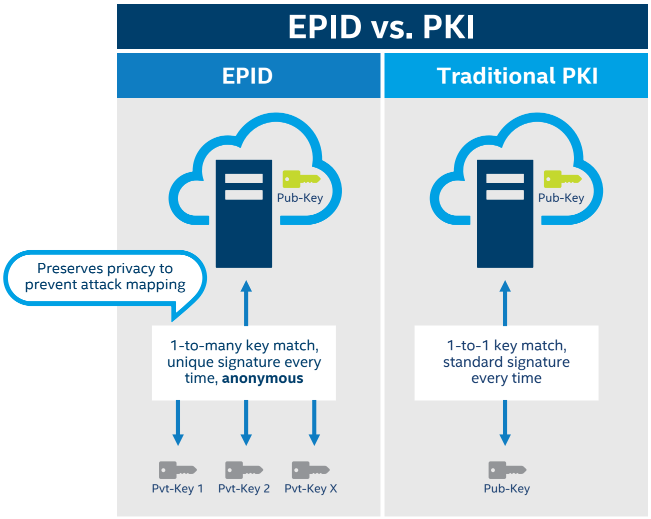
EPID vs. PKI
EPID
Traditional PKI
Pub-Key
Pub-Key
Preserves privacy to prevent attack mapping
1-to-many key match, unique signature every time, anonymous
1-to-1 key match, standard signature every time
Pvt-Key 1
Pvt-Key 2
Pvt-Key X
Pub-Key

Figure 2. Intel® Enhanced Privacy ID vs. Public Key Infrastructure.

Foster Interoperability

Interoperability has several dimensions. One aspect is to support interoperability of new devices with legacy devices and legacy infrastructure, neither of which may have been built with required levels of security nor designed for compatibility. Techniques are needed to sandbox legacy systems to reduce security risks, while at the same time enabling interaction between old and new technologies. Another aspect to interoperability is data sharing. There is a strong need for data to be self-describing, to support data aggregation and data analytics. In fact, there is a strong need for all IoT elements to be self-describing, what some in the standards community would call Semantic Interoperability; to capture not only what an element is but its function or role in the larger ecosystem. A third facet of interoperability is to support the inherent compositionality of IoT solutions, which are often composed from systems of systems. It is no longer the case that a single vendor will manufacture the full end-to-end integrated IoT technologies, as might have been the case a decade ago. As a result, trustworthiness is more crucial and calls for open interfaces and APIs that mediate the relationship among specified components. The NIST Cyber Physical Systems (CPS) framework, which was developed in partnership with industry, academic, and government experts, serves as a methodology for understanding, designing, and building CPS to enable seamless interoperability. Towards that end, Intel has contributed the Intel® IoT Platform, which includes IoT reference architectures and a set of IoT ready technologies that provide secure, open, standards-based, scalable, and interoperable technology building blocks. In addition, Intel leads, participates, and monitors many of the IoT-related standards bodies such as OCF, IIC, OpenFog, ECC, IETF, 3GPP, NIST, IEEE, and others.

Accelerate Leadership in IoT Security

In this whitepaper, the term Security is intended as a broad category term to cover Security, Privacy, and Trust. To accelerate leadership in IoT Security, Intel believes that the U.S. must invest in IoT research focused on Security, Privacy, and Trust. For example, Intel has partnered with the National Science Foundation to fund academic research in the areas of Cyber Physical System Security & Privacy, as well as Information-Centric Networking in Wireless Edge Networks, both of which are tackling fundamental security challenges. With the sheer volume of data coming off of IoT devices, it is vital we foster research that allows us to balance security and privacy.

There is a human element to accelerating cybersecurity leadership. The U.S. must work to create more security professionals if we expect to be able to embed robust security in our products and infrastructure.

In conclusion, we are becoming a smart and connected world. The Internet of Things has the promise of improving our work, our communities, our homes and our lives, but we must design our systems with security and privacy built into them from the outset. Intel is confident that the U.S. can enhance our national cybersecurity with a continued open and joint dialogue across government, industry and academia, and with a commitment to work together on developing, implementing, and deploying technology solutions that have integrated security at the onset.

Software and workloads used in performance tests may have been optimized for performance only on Intel microprocessors. Performance tests, such as SYSmark and MobileMark, are measured using specific computer systems, components, software, operations and functions. Any change to any of those factors may cause the results to vary. You should consult other information and performance tests to assist you in fully evaluating your contemplated purchases, including the performance of that product when combined with other products. For more complete information visit http://www.intel.com/performance.

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No computer system can be absolutely secure. Check with your system manufacturer or retailer or learn more at http://www.intel.com/content/www/us/en/benchmarks/intel-product-performance.html.

Printed in USA 1116/BEK/HBD/PDF ♲ Please Recycle 335180-001US