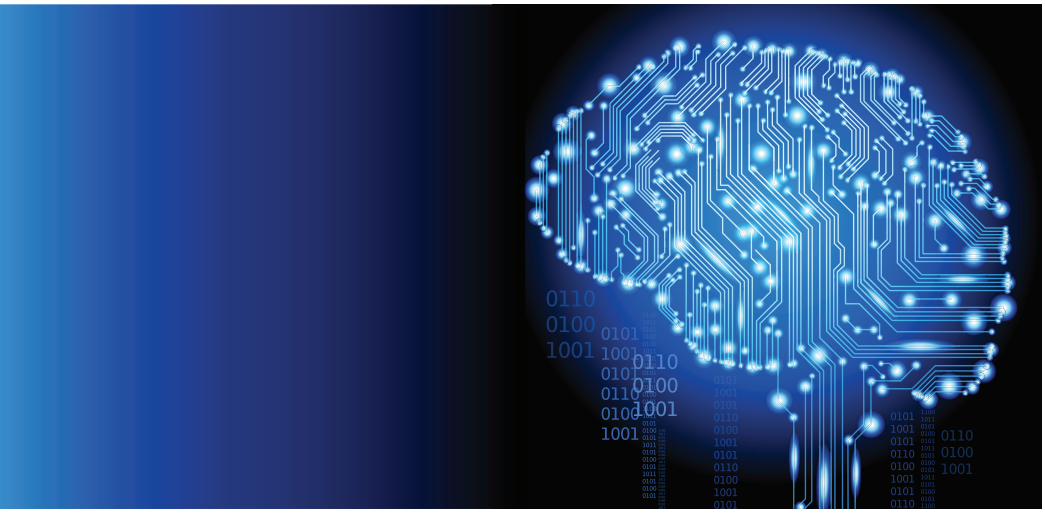
Intelligent Systems

Securing Intelligent Systems from the Ground Up



As the Internet of Things becomes a reality, conventional perspectives on security must be revisited and revised

—Jack Shandle, Principal e-ContentWorks

Ever since 1982, when a Pennsylvania high school student unleashed Elk Cloner —the first known microcomputer virus to spread in the wild—cybersecurity technology has been playing catch-up—and very successfully. It has grown into a multibillion dollar business that has saved corporations and individuals billions of dollars more than they've invested.

Viruses, Trojan horses, worms, back doors, spoofing, DoS attacks, and other cyber-security threats are now part of everyone's computer vocabulary. What's next? For all of its promise, the Internet of Things is likely to become the greatest challenge for security technology to date, defying conventional security solutions, paradigms, and tools.

The Internet of Things is a global revolution in which billions of "devices" seamlessly connect, are managed, and interact over a network in order to acquire data that enables people, devices, and systems to turn this raw data into actionable information that delivers valued services.

The Internet of Things includes devices big and small: things as mundane as a kitchen appliance that can be controlled remotely from a smart phone; or, something as life-saving as a heart monitor that reports cardiac anomalies to a hospital's computer; or, something as mission-critical as a circuit breaker in the Smart Grid whose operation can enhance efficiency enormously or, if compromised, cascade the grid into service interruptions stretching across several states.

Another relatively new phrase in our technology lexicon is Big Data, which is not just large in volume (think petabyes instead of terabytes) but also diverse (email, social media, video etc) and has high velocity (instead of batch processing, real-time analysis). Big Data gets bigger when we consider the idea of billions of intelligent devices in the Internet of Things sending trillions of data bits hourly. It has the potential of making business far more efficient and empowering individuals in new and creative ways.

This can happen only if the data can be trusted.

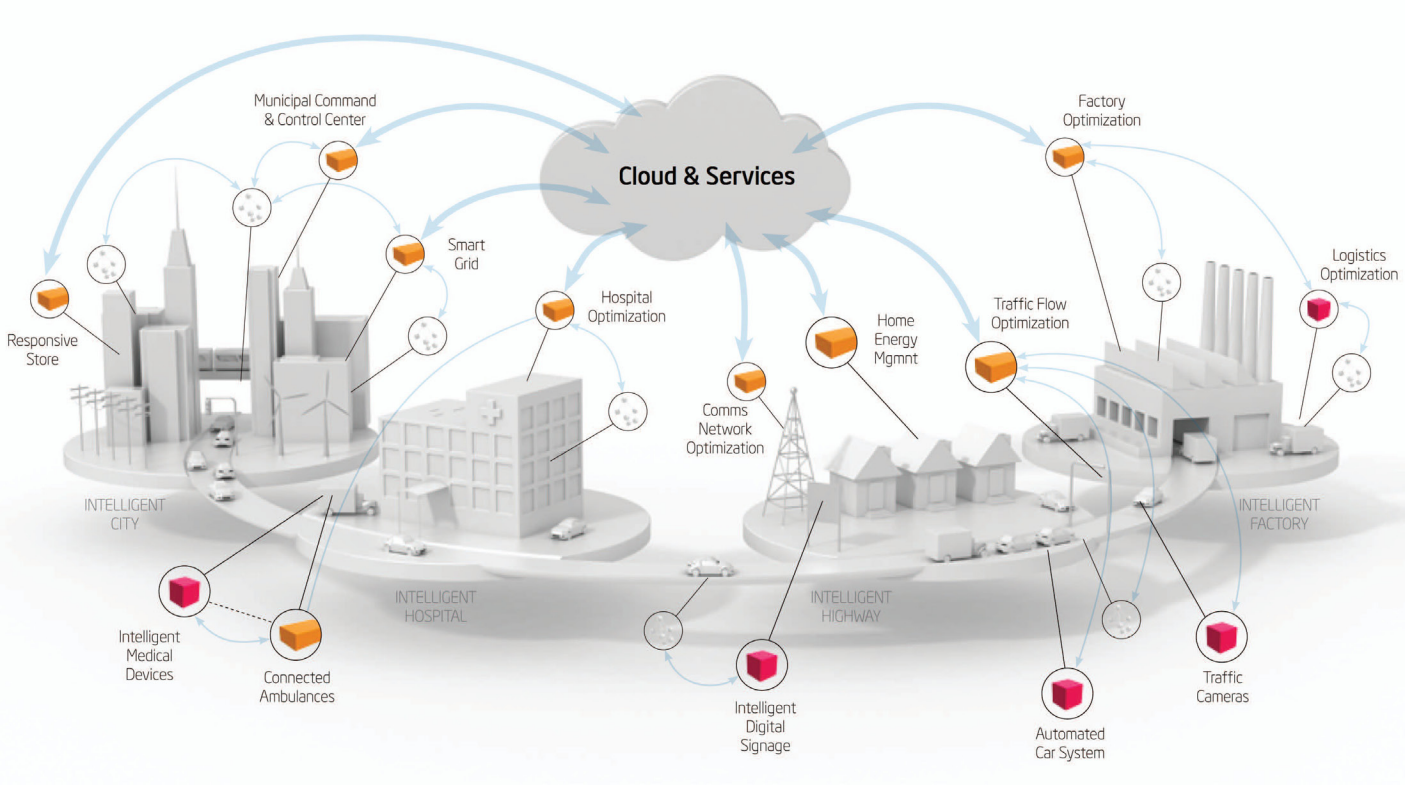


Figure1

Transforming the Internet of Things into Intelligent Systems

Before there were computers, there were embedded devices. They tended to be single-use devices that typically did not communicate with the outside world. If they did, communication was limited. There was little need to consider security.

Evolving from single-use, unconnected devices to system-level, hyperconnected solutions implies higher levels of connectivity, manageability and security. Among the requirements for implementing intelligent systems is revising the design paradigm for individual embedded devices so they can participate in end-to-end (embedded chip to enterprise server) security. Instead of designing superb point-of-sale kiosks or robots or kitchen appliances, the design paradigm for intelligent systems requires the inclusion of features that make them part of the higher level system—and that includes security as a top priority.

The burden of designing an embedded device that is fully capable of participating in a hyperconnected, intelligent system need not fall solely on the device designer. In fact, it cannot. Security in the Big Data era is a task sized for a vertically integrated solution from the entire design ecosystem—from chipmaker to OS vendor to the security software company.

Offloading the designer of a good part of the security responsibility also pays other dividends. The most important is that the design team will have more time to spend making its system the best that it can be and adding value for customers.

Batch processing of the data produced by embedded devices will become far less pervasive. Consider a vending machine sitting in front of a service station. It reports inventory statistics several times during the day instead of once a week. If a product is out of stock and a delivery truck is in the vicinity, the truck might be diverted to restock the vending machine.

The warehouse receives an update as well. It may revise its delivery schedules accordingly. At the enterprise level, data from many vending machines can be aggregated to track trends of interest to marketing, finance, and manufacturing. Companies that make the products stocked in the vending machines, for example, might be advised to make more—or fewer—of a particular product.

While a great deal of value can be extracted from intelligent systems, the unprecedented degree of connectivity carries with it many potential points of attack for hackers.

Other examples of how intelligent systems add value can be envisioned by following the connections in Figure 1. Applications and devices as disparate as signage, ambulances, traffic cameras, and robots all have the potential of adding more value when connected to the enterprise.

Securing the Internet of Things

The security of intelligent systems operating on Big Data will be radically different from the security paradigm we have become accustomed to with computers. The new requirements spring from just a few fundamental differences in the security profile.

1. Contrary to our previous experience with computers and smartphones, the billions of devices that compose the Internet of Things will have no users. But users are, in fact, the linchpin of today's security trust model. Password protection and many authentication technologies depend on users acting intelligently at the security perimeter. Users are tasked with installing patches and upgrading operating systems. They are often the first to report problems to cybersecurity companies.

   On the other hand, after an embedded device is put in service, who is responsible for monitoring and maintaining it? How do you patch it? How do you update it? How do you terminate the device in case it's infected? Without users to report problems and initiate actions, the linchpin of the new security paradigm must be the hardware platform.

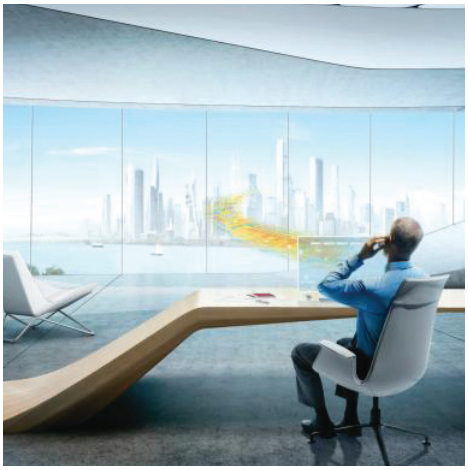
2. Lifecycles of embedded devices are measured in years—and often in decades. Having a system with an OS that has not been updated for several years poses a significant security threat because the ingenuity of hackers—and the tools at their disposal—is constantly growing. The first line of defense in this scenario is at the chip level. But OSs, middleware, and security systems management also have indispensible roles to play.

Contrary to our previous experience with computers and smartphones, the billions of devices that compose the Internet of Things will have no users. But users are, in fact, the linchpin of today's security trust model.

3. Unlike conventional computer and communications systems that use a small number of dominant operating systems and hardware platforms, embedded devices are built on a multitude of platforms. This has a lot to do with the extraordinary diversity in product purpose and functionality; but the differences go beyond functionality. Point-of-sale kiosks, consumer appliances, medical devices, industrial robots, and literally thousands of other product types each have strikingly different functions, design restraints, and performance requirements. In the past, most embedded devices were typically designed with cost as a major constraint (no bells and whistles), a narrow perspective on interoperability, and an even narrower perspective on security.

Threat Analysis and Response

The purpose of the device will drive its security profile requirements. A toaster performs a simple task, and the data it generates is of limited interest to a hacker. But in the Internet of Things, it could be a point of attack because it is only a few short hops from the toaster to the smart meter, to the smart grid to the utility's command center. A medical device



requires a sophisticated security profile. Its design can be complex (megabits of code) and the data it handles is sensitive. Federal and state regulations come into play for medical devices that can communicate over the Internet or a LAN or PAN.

Containment is another issue that must be redefined in the age of a userless security paradigm and the unprecedented number of devices in the Internet of Things. Over the years, security companies have thought through the problem and developed identification, isolation, and containment technologies that work for computers and smartphones. Today, security incursions can be isolated and contained fairly quickly. The defenses and responses for computer are, however, not quite as useful for embedded devices. A computer-oriented security profile typically requires rebooting after a new version or patch is installed. If it is to be retained, it will have to accommodate devices that are primarily autonomous and for which rebooting is not an everyday process. The "patch early and patch often" approach will have to be modified to accommodate embedded devices that may be in the field for 10 to 15 years.

Since there will be an end-to-end connection between the chips that power embedded devices and the core of the enterprise, an intelligent systems security paradigm should also be end-to-end. It can be conceptualized as having three primary components.

1. Platform protection begins in the chip. It addresses security threats at the BIOS/firmware level as well as enhances system reliability. Platform protection includes capabilities such as: building in the ability to manage security across systems; protecting virtual environments from malware and rootkits; remotely diagnosing, isolating, and repairing an infected system regardless of operational state; encrypting faster for enhanced protection; and, protecting the OS from privileged escalation attacks.

2. Software protection addresses threats at the OS and application level. Advanced software protection for intelligent systems includes: validated and supported middleware stacks; secure remote management including customized trusted boot; Web-based configuration management for device provision, setup and management; and compatibility with other layers of the Intelligent Systems Framework.

3. Data protection for application and data security and—just as important—security management protection, which includes rolling out and managing patches and updates. Desired features include: the ability to block unauthorized applications and change on fixed-function, point-of-service infrastructures; detecting, blocking, and remediating hidden attacks with protection outside the operating system; advanced encryption algorithms; and, multiple layers of data protection that address specific risk areas across intelligent system deployments.

It should be noted that a fourth layer exists, which is the existing computer, server and smartphone security measures and ecologies that have been developed over the four decades since Elk Cloner made its debut.

While each of the security layers is valuable standing alone, their aggregate value to OEMs increases dramatically when the layers communicate with each other and build on each other's capabilities. This can happen, however, only when an intelligent system framework is defined and specified.

In addition to linking the three basic security layers, a viable framework should have inherent characteristics of its own including the ability to provide flexible solutions using scalable, off-the-shelf elements. The goal is to enable vertical specialization by the OEM and allow the OEM to deploy resources from achieving interoperability to extracting value from Big Data.

Intel's Intelligent Systems Framework, for example, defines a set of fundamental capabilities delivered by components from Intel and its ecosystem partners that address connectivity, manageability, and security as shown in the table. Security features are called out in the third column.

Integration Solutions of the Intel® Intelligent Systems Framework

Connectivity	Manageability	Security
Multiple Protocol ▪ Wired ▪ Wireless ▪ Mobile ▪ Local	**Reliability** ▪ Improved system uptime ▪ Out-of-band detect, diagrose, and repair ▪ Device management	**Platform Protection** ▪ BIOS and firmware ▪ Platform hardware ▪ System reliability
Simple integration with Intel® solutions ▪ Combine X-Intel ▪ Components	**Efficiency** ▪ Remote power managemnt ▪ Off-peak maintenance ▪ Inventory and asset managemnt	**Software protection** ▪ Operating system ▪ Applications ▪ Pre-OS
Flexible combinations ▪ Easy integration	**Hardening** ▪ McAfee integration ▪ Compliance management	**Data protection** ▪ System/App Data

Intel processors supported in the framework include Intel® Xeon® processors, 2nd and 3rd generation Intel® Core™ processors with Intel® vPro™ technology, and Intel® Atom™ processors. OSs include Microsoft Windows*, Wind River* Linux, and Wind River VxWorks*. Security software includes McAfee Embedded Control* and Deep Defender*. Other ecosystem partners include: Advantech, Arrow Electronics, Avnet, Axeda, Dell, Digi International, Kontron, Portwell, Eurotech, ADlink, and WebHouse.

Forward Planning for Secure Devices

The paucity of information about Big Data security for embedded devices added to the inconvenient truth that today's security paradigm is inadequate for the Internet of Things add up to a disquieting prospect for companies that design and manufacture embedded devices.

There are, however, several actions that companies can take to prepare for their next generation of products. The first is to recognize that at some point someone will attempt to hack the device and has an excellent chance of succeeding. This is not a defeatist view but a pragmatic and helpful one. The point is to have a plan in place that will initiate identification and containment strategies without having to invent them on the fly. The design goal should be to create a reaction plan that can be executed by an autonomous device in real time.

Design teams should also acknowledge that they cannot solve the problem alone. Everyone in the supply chain should be expected to contribute. If the chipmaker, OS company, application developer, and connectivity partners are all working from the same playbook, then the embedded devices' design team will have a lot of built-in security to leverage.

The design team still has a critical role to play. In an environment as fragmented and diverse environment as the Internet of Things, it will be necessary for the intelligent systems framework to cast a very broad net—to consider every possibility. Therefore, appropriate controls must be selected and built in specifically by the device manufacturer based on the type of device. Devices must be manageable. Designers must think about what happens after the device is sold and deployed in the field: how to manage patches, for example, and how to issue configuration changes that cannot be spoofed.

The most important action a design team can take on security, however, is to get started. While the comprehensive solution is still evolving, the fact is, it will always be evolving and that a few security hooks built into an embedded product are better than none.

Conclusion

If the layered approach—platform security, software protection, data security—mentioned above is implemented intelligently and adopted widely, it will serve as a potent security framework that transforms today's insecure Internet of Things into a secured intelligent system that creates and processes data that can be trusted.

Just as important, however, is the necessity of a fundamental mind shift among design teams, who have to think about security from the beginning—something that is built in, not bolted on.

Intelligent Systems