Point of View

IoT security:
An IBM position paper

Sponsoring executives:
Harriet Green and
Alessandro Curioni
Contact authors:
Tim Hahn and JR Rao
Contributing authors:
Jan Camenisch, Supriyo
Chakraborty, Tim Hahn, Michael
Osborne, JR Rao, Michael Rowe,
Fumiko Satoh, Kapil Singh and
Andreas Wespi

Watson IoT™

IBM

Table of contents

Introduction: IoT and Cognitive IoT

Coined by Kevin Ashton in 1999[1], the term Internet of Things (IoT) has come to denote the widespread deployment of sensors and actuators with ubiquitous interconnectivity, potentially to the Internet, to monitor and control physical systems and critical infrastructure such as electrical utilities, transportation systems, Supervisory Control and Data Acquisition (SCADA) systems, factories, and buildings. The goals of the effort have been to gain better visibility and understanding into the operation of these systems and to effect change that would lead to vastly improved efficiencies of operation. As the IoT has been adopted by businesses, we see it expanding to both structured and unstructured data. This includes sensor data, social data, and even audio and video streams. *Ever since its advent, it has been widely recognized that security and privacy are key enablers for the IoT.*

More recently, the emergence of cognitive computing has heralded the arrival of systems that learn at scale, reason with purpose, and interact with humans naturally. Rather than being explicitly programmed, such systems learn and reason from their interactions with humans and from their experiences with their environment. In a computer system, *understanding* means being able to take in large volumes of both structured and unstructured data and derive meaning from it—that is, establish a model of concepts, entities, and relationships. *Reasoning* means using that model to be able to derive answers or solve related problems without having the answers and solutions specifically programmed. And *Learning* means being able to automatically infer new knowledge from data, which is a key component in understanding at scale.

The application of the notion of Cognitive Computing to the IoT has led to the second coming of IoT, aptly labeled as the *Cognitive IoT (CIoT)*. A CIoT introduces cognition into the fabric of sensors and actuators of the IoT enabling the system to understand, reason, and learn. In this vision, sensors and actuators share information with each other, build models of expected behavior of systems, and unlock the complex relationships that exist between different parts of the system. Automated mining of massive amounts of sensor data leads to the extraction of patterns and formulation of behavioral models, which would normally have defied manual human realization.

A CIoT leverages the massive amount of data obtained from not just IoT device data, but also interconnected physical, social, enterprise, and other cyber entities to understand and reason about the current state of the system. In short, CIoT provides visibility of the whole solution through the consolidation of data from all IoT devices; the whole is greater than the parts. Such systems can generate responses automatically in terms of guidance, assistance, and recommended action. These recommendations are created in a manner that teaches itself and adapts, augmenting human intelligence through human-machine collaborations.

If the first-generation of IoT technologies enabled us to achieve operational efficiencies, the CIoT enables businesses to not only do things more efficiently, but vastly increases the capabilities of their systems to improve customer satisfaction, to discover new business opportunities, and to anticipate risks and threats so they can better deal with them.

In 2015, IBM® published our PoV on IoT Security best practices.[2] The entire domain of IoT security is broad and deep; we will not address each unique aspect of every possible security and privacy issue. In this paper, we focus on how Cognitive technologies will impact Security in IoT systems. We discuss the security and privacy implications that CIoT will surface, and then review leading-edge research activities to address the challenges and opportunities that the IoT will provide.

Security and privacy implications of Cognitive IoT

We now look at how the CIoT offers capabilities to help businesses and the risks that business needs to address.

Cognitive IoT exposes new attacks

Water systems are being attacked[3], nuclear power plants can be breached[4], baby monitors[5] can be used to snoop on your house, wearable data can be used for planning robberies[6], and even heart monitors are under threat with potentially dire consequences.[7]

Today, interconnected sensors and actuators have pervaded almost every sphere of our lives ushering the dawn of the IoT era. Our homes and appliances are increasingly being made smarter through embedded sensors and actuators[8]; connected medical appliances allow for continuous remote monitoring of patients and timely administration of medicines[9]; the construction industry is using smart cement with sensors (e.g., accelerometers) to monitor the load on bridges and perform preventive maintenance[10]; power grids are being instrumented with sensors to detect possible disruptions and accordingly manage the generation and distribution of power[11]; embedded sensors are being integrated into the heavy machinery used in manufacturing for increased worker safety, optimization of processes via automation, and anomaly detection[12]; finally, with connected cars, automated traffic control and fleet management are no longer distant realities.[13] According to an estimate from Cisco, 25 billion devices (things or physical objects) are already connected to the Internet, and this number is expected to grow to about 50 billion by 2020.[14] The potential economic impact of this revolution is also estimated to be between $2.7 trillion and $6.2 trillion per year by 2025.[15]

In spite of our increasing reliance on these embedded sensors and actuators, their security has unfortunately not attracted as much attention as it deserves. The spate of recent attacks that have been realized on these embedded sensors bears testimony to their ubiquity but also raises serious concerns about their security. These devices, by virtue of their deployment, can be used to cripple critical infrastructure that was once considered invulnerable.[16]

The attacks on these systems can be broadly categorized into two types: *active* and *passive*.

- **In the case of active attacks,** an adversary gains access to the device and uses it to control the device and run malicious code on it. One of the most widely known attacks of this kind on IoT systems is the Stuxnet worm, which is also the first worm known to attack SCADA (supervisory control and data acquisition) systems.[17] Designed to infect industrial systems, in particular control systems that operate equipment, such as centrifuges, the worm, in addition to allowing its authors access to the industrial systems, takes control of the programmable logic controller; ultimately destroying physical equipment. Recently, hackers have demonstrated that code running on gadgets plugged into our car's dashboard for monitoring speed, location, and driving efficiency (e.g., for insurance, fleet management) can be used to also send commands to the car's Controller Area Network (CAN) bus, enabling or disabling brakes.[18] [19] A similar attack on the vehicle's control systems, including brakes, was demonstrated by hacking into the connected vehicle's entertainment system.[20] Unauthorized commands could be sent to a device to negatively impact the health of a patient. More recently, it has been shown that connected pumps used to deliver insulin or other medicines to patients can be remotely hacked into and controlled to change the dosage the pump delivers, threatening the life of the patient.[21]
- **In the case of passive attacks,** signals emitted by these devices are used to infer sensitive information about the system or the usage and activity of the system. For example, the acoustic emanations from the CPU of a computer has been used to infer the RSA encryption key using a mobile phone kept in the proximity of the CPU.[22] The electromagnetic interference signatures that the power supplies of modern TVs produce are used to determine the video content that is displayed. The signatures are discernible and are resilient to the presence of other noisy electronic devices connected to the same power line.[23] Similarly, smart meter data has been used to identify the multimedia content playing on a TV set.[24] Optical channels have also been exploited to identify the media content playing on the TV.[25] [26] Recently, the power profile on a smartphone has been used to identify the location of the user.[27] And thermal profiles of a multi-core processor have been shown to leak information regarding the code that is currently executing on it.[28] Not all security exposures and attacks need to be a complex and sophisticated as the ones listed. Information leaked in the hands of attackers can be just as dangerous for individuals and enterprises. The sheer number of IoT devices and the data they collect and represent could be used by attackers for opportune targeting, for example knowing where and when people will be in a building.

Security threats in Cognitive IoT

As more and more systems transition from "traditional" IoT to CIoT, a new range of security attacks becomes feasible. *Attackers can interfere with the process of cognition and force the system to learn incorrect behavioral models. By subverting vulnerable sensors and actuators, or feeding learning systems with false data, attackers can corrupt the learning process.* Even slight changes in the learned models of individual components can have an amplified impact when these components are integrated. Systems, which are based on machine learning and intended to decide questions such as: should this user get access, should we extend credit to this customer, and what will this insurance policy cost, will typically base decisions on factors beyond human cognition and may not appear to follow rules or policies that are self-evident to human beings. Given the scale and scope of the ambition for such systems, this could have significant consequences to human life and businesses.

Protecting against such attacks will require the invention and use of new ways of detecting aberrant behavior by such systems. Often seemingly normal behavior within accepted tolerances and recommended actions may hide a subtle shift towards achieving the attacker's goals. For instance, systems will need to protect against attacks which introduce contaminated data, in order to influence the learning process and modify the decision algorithms and parameters without being detectable (because the algorithms are self-modifiable). This may necessitate the invention of redundant components and systems that provide checks and balances on each other, under the assumption that the attacker cannot compromise a plurality of these systems. IBM, along with our customers, is investigating Blockchain technology to address consensus based security. The growth of the number of devices that companies and individuals are using may ultimately drive us to the point where no individual can hope to understand them all and the interdependencies. Eventually, much like the human bodies own defensive systems, this may lead to security and privacy architectures that are more decentralized and adaptive.

Privacy threats in Cognitive IoT

As people use more mobile and connected devices in daily life, and security solutions rely heavily on pattern matching and monitoring technologies, the privacy of individuals has become a big concern. Many services collect unnecessary personal information, requiring "all-or-nothing" policies that force the users to give up personal sensitive data, e.g., geo-location. Security solutions must offer a high-level of security while preserving individuals' privacy through flexible and consumer-oriented policies. We already see governments working to address privacy concerns with regulation like the Global Data Protection Regulation (GDPR).[29]

In order to be prepared for future analysis of behaviors or use, companies may over-collect and retain information or even default to collecting everything and hold on to it "just in case". Consumers have been lulled into just "hit accept" on long and complex EULAs (end user licensing agreements), as the legal language and pointers to embedded third-party agreements has become a labyrinth. This approach has allowed for more and more data to be collected and stored within company data stores.

Using cognitive analysis of personal data (in particular behavior data) promises to provide better customer service. However, collection, processing, and storing behavioral data may put the security of a person at risk by exposing location and other insights. Thus the question is to what extent this is a tradeoff and how one could get the benefits of the stronger authentication without incurring the downsides to the individual privacy.

As more and more devices share more and more data, the value of breaching these systems increases. The network effect caused by meta-data and social graphs can expose non-obvious relationships, which can be exploited for additional value.[30] Simple devices with network connectivity may become the preferred attack surface as they become the onramp to a digital treasure trove of information. Information is at the same time an asset and a liability. When the value of the information is less than the liability risk of having it, businesses should be looking to proactively delete and destroy this information. Currently, business who do remove data tend to use simple time-based models, deleting all data older than x-time; however, using more granular/ consent-based models allows for a more appropriate response to an individual's/ organization's/ or business's needs.

Assessing risks

We look at three areas to understand the risks to which CIoT systems are exposed.

Authentication

Humans are important actors within an enterprise. Protecting the CIoT system requires that human users are securely authenticated. Currently, the burden of making such authentication secure is on the user. We have to select and manage passwords for many sites, each requiring them to satisfy conditions (mixture of characters, length, etc.). Employees need access to company information everywhere, with any device, at any time, making protecting the accessed information very hard. There have been efforts to address secure access to company information from mobile devices (laptops, tablets, and mobile phones). IBM provides such solutions through MaaS360.

While biometrics is another means of authentication, an instrumented world begins to remove this form—as recordings of voice, activity, habits, and so on are logged and not just "what you are". Advances in passive and ambient sensor technology, are even encroaching on "what you know"—not to the point of determining a password, but at least in recognizing emotion and intent.

Devices are the other critical actor within and across enterprises. Far more data is generated by devices and sensors than by humans.[31] As such, many of the same authentication challenges presented by human actors are present in devices. Hardware going in and out of service, having part replacements or updates that change or add new capabilities require constant assessment of risks. The number of devices and sensors far outpace the number of humans, and as such will create additional challenges for authentication.

Virtual enterprise

The boundaries between intranet and extranet are disappearing as companies offer access to data and services to other companies and external individuals. Maintaining security and privacy becomes increasingly difficult.

Cognitive data analysis

Companies increasingly want to make use of cognitive technology to better understand and use their data. Enabling such analysis by generating, collecting, and storing additional data makes a company also more vulnerable to the loss and misuse of such data. Also, providing data to third parties for their analysis opens up new exposures. As companies deploy IoT solutions the networks are potentially bridged and so the attack surface widens.

Attacks and threats to companies could be in the form of leakage of sensitive data or manipulation of the corporate network by rogue devices. These same attack surfaces could allow attacks, which take over devices and allow for manipulation of a company's network infrastructure.

Data privacy regulations are moving towards greater control and specification of use by data subjects. It is not clear what effect these regulations will have on learning systems which have used a subject's information in the past, and at some point in the future the subject demands redaction or removal.

Ultimately, as devices and sensor are connected in IoT applications, a comprehensive assessment of security, privacy, and safety should be performed. For CIoT System IBM Research is working to drive innovative solutions to address security, privacy, and safety.

Cognitive IoT security framework and research projects

IBM Research is leading many efforts related to CIoT security. These efforts are looking to address many of the privacy and security challenges identified in this paper. While NIST has identified a Cybersecurity Framework, (Prevent, Detect, Respond, and Recover)[32], and has extended it for Cyber-Physical system, (Safety, Reliability, Resilience, Security and Privacy)[33], we will focus on a Cognitive framework called: Security 360.

Security 360°: A security framework for Cognitive IoT

IBM Research has been working on a new and operational model for security, called Security 360°, depicted in Figure 1. The model described below can be applied to protect a security target such as a high value asset or service in the enterprise, a critical enterprise workload in the cloud, or a process control subsystem in cyber physical systems. The paradigm is distinguished by characteristics: it is contextual, cognitive, and adaptive security. We envision three phases: Monitor and Distill, Correlate and Predict, and Adapt and Preempt.

Monitor and distill

In the first phase, all available aspects of the environment of the security target are instrumented to construct a 360-degree view to assess the security posture.

As opposed to a siloed and fragmented approach that only monitors pieces of the infrastructure, such as the network traffic or user activity, we focus on collecting information from all possible monitoring points including the network, the devices, the workloads, the users (external as well as privileged), the data, the application, and the business processes to gain an end-to-end view of what is under attack. Such instrumentation can be achieved by passive monitoring (simply looking at the network traffic), near-field monitoring (looking at artifacts of the security target, such as disk image and the memory image of the virtual machines in cloud environments, emanations of side-channel information as analog signals from devices etc.), in-device monitoring (monitoring of the hypervisor or using agents to monitor in the virtual machine level), or even using active monitoring (probe the workload, explore what kind of vulnerabilities and weaknesses it might have). Understanding the data in context allows for a much better understanding of the security risk. With today's security controls, a firewall can see a packet cross an enterprise perimeter and sometime later, a sensor might register activity at an application level. To connect these dots and realize that these activities are causally related, it is important to connect the monitoring data from the firewall with the data at the identity and application level, using context to get a more comprehensive and end-to-end view.

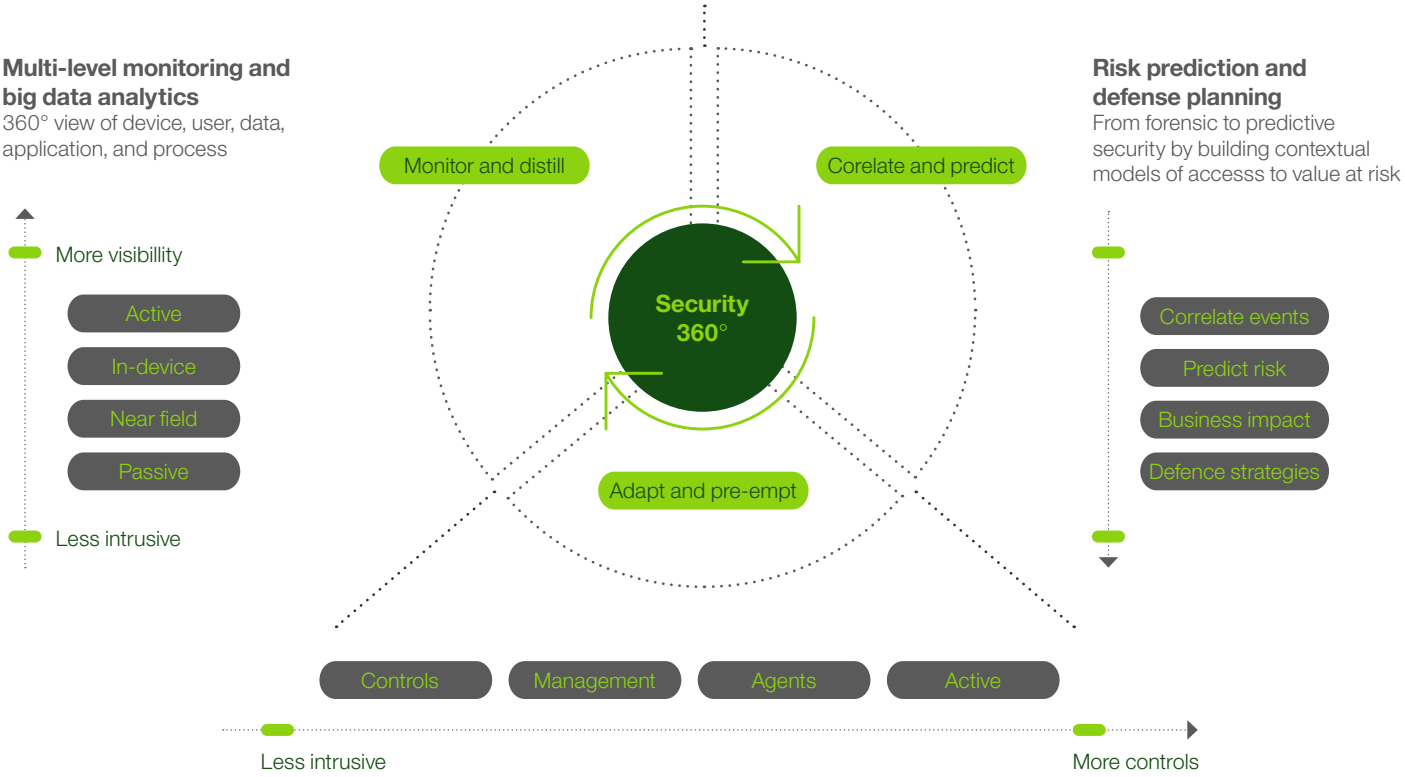

Figure 1:
Security 360°: A contextual, cognitive and adaptive approach to security

Correlate and predict

The second phase focuses on examining the contextual observations to construct behavioral models. The models have to be carefully crafted though, if the behavior observed is over a period which security has already been compromised then the "normal" behavior being modelled is in fact modified behavior. If the models are built or accepted without consideration to these weaknesses, then the reliability of this approach in a security context is fundamentally flawed and in itself could mask additional attack surfaces. The goal of this phase is to assess the changes in the security posture of the security target and plan a defense. The amount of data that comprises the contextual observations is large and it is here that we have to bring automation to bear on the problem.

Cognitive computing has an important role to play in two different ways: first, we use data-driven techniques to aid analytical modeling and insight extraction. Data mining and machine learning techniques can aid security administrators with automated methods to build models, track normal behavior, and flag anomalous activity; second, we can use the same techniques to consolidate and create an authoritative feed of threat intelligence from both external and internal sources. This is the phase in which one can use passive and often static threat intelligence information to understand and drive responses to the threat kinetics that one sees in the environment.

Adapt and preempt

While enterprises are beginning to adopt more dynamic methods to provision logical systems, many of today's security targets suffer from being mostly static, presenting stationary targets for adversaries that have the patience to perform reconnaissance.

Attackers enjoy the advantage of determinacy and can observe target systems over a sufficiently long period of time to map their topology, available services, and applications supported. As a result, attackers know exactly where to point their tools to discover vulnerabilities, exploit them, and affect enterprises. The static posture essentially presents a limitation for today's defenses. We, therefore, focus on a much more agile methodology to counter evolving threats. In this sense, environments like the cloud offer us a unique opportunity. With software defined environments, we can use techniques like software-defined compute to migrate workloads across different servers or perform server "rejuvenation" that restarts physical or virtual servers from a well-known, untampered state. We can also use software-defined networks to interpose security controls in a manner that is commensurate with the threat environment and software defined storage to use secure information dispersal techniques to protect data. As is to be expected, there is a tradeoff here between the additional security of the various agile security mechanisms and their usability and a judicious choice has to be made to select the appropriate mechanism. We expect that such an approach will, once again, raise the ability of enterprises and cloud operators to defend against attackers in the security arms race.

Security Intelligence for Cognitive IoT

There are a wide variety of IoT devices, ranging from wearables to heart monitoring implants to parking meters to automobiles with a myriad of built-in sensors.

Some of the devices, in particular the larger ones, have built-in diagnostics to detect malfunctioning caused by failing components or tampering attempts from external attackers. In IT environments, security monitoring and analytics as a complementary means to securing systems is widely accepted because systems may have known deficiencies that cannot be fixed. There is always the possibility of misconfigurations, and there is also the risk of previously unknown, inherent vulnerabilities that may become known and exploited at some time in the future.

Security Information and Event Management (SIEM)

In IT environments, SIEM solutions are the standard way of collecting security-relevant events and analyzing them. SIEM solutions come with a default set of rules of how the collected IT events can be analyzed. The set of rules can be modified and enhanced with environment specific rules.

A benefit of using standard SIEM solutions for IoT is that security intelligence can be built based on standard IT solutions with IoT specific adaptations. Furthermore, there is no strict separation of the IT and IoT domains. For example, business processes may be triggered by IoT events or IT environments may be reconfigured based on IoT demands. Being able to use one security solution for both domains and covering the intersection of the two domains is of high value.

Many IoT devices do not support device-internal security monitoring necessitating additional solutions for extracting security relevant events in IoT environments. Such security solutions are evolving, for example, Industrial Control System security solutions are being developed that monitor Programmable Logic Controller (PLC) devices or embedded security solutions for automobiles. Their output can be processed by IoT SIEM solutions.

IT SIEM solutions are configured based on known threat scenarios. However, in the case of IoT, there is little public information available about IoT specific attacks, and therefore configuring IoT SIEM solutions is difficult. To address this difficulty IBM Research is approaching SIEM with Cognitive IoT Security Intelligence.

Security Intelligence

Novel approaches are needed to detect malicious and accidental faults in IoT environments. The goal of advanced CIoT Security Intelligence solutions is to use any kind of information available for assessing the security of an IoT environment. The information to be collected may not be specific to security. In the simplest case it is the information reported by the device anyway, e.g., measurement data such as temperature or pressure measured by a device. It could also be information retrieved by instrumenting the IoT device or by analyzing the communication protocol that is used by an IoT device.

The main goal of CIoT Security Intelligence is to detect attacks against an IoT environment. Given that currently there is little information available about IoT attacks, signature-based detection systems are only of limited value. Therefore, detection systems also have to deploy behavior-based detection techniques to identify deviations from a learned normal behavior. Machine learning of normal behavior can begin as early as the design phase of an IoT system. Requirements, test data, and other data sources could be included in understanding the system behavioral characteristics. Behavior-based systems also have the advantage that they provide operational insight. Beyond security, they can show the devices being used, and how these devices operate and interact.

An additional usage scenario of CIoT Security Intelligence is that any IoT data stream can be analyzed for detecting abnormal behavior. CIoT Security Intelligence can be used to identify suspicious IoT data that may result, e.g., from failing IoT devices, malicious activity, or misconfigurations by an operator. This suggests that CIoT Security Intelligence should be applied to IoT data streams before any IoT analytics takes place in order to improve the quality of the overall IoT solution.

There are known attacks such as Stuxnet that are difficult to detect if IoT data streams are analyzed individually. For example, a hacked Programmable Logic Controller can maliciously take over control of a device but still report back valid data to the overall Control system. What is needed is a CIoT Security intelligence solution that can detect and analyze the interdependency of IoT devices and the data they generate. For example, in an automobile there are many sensors installed that report data. There is interdependency between speedometers and sensors attached to the engine. If an attacker modifies the data of only a subset of the sensors, inconsistencies can be detected and reported by a multi-sensor CIoT Security Intelligence system. We expect that the sensors can be used to help cross-verify IoT data in order to identify misbehaving devices.

As it is widely known, IoT can generate massive amounts of data. Edge analytics and edge processing of high frequency samples of information is important. We envision an CIoT Security Intelligence gateway that performs local (edge) security analytics whenever possible but can also send raw data and correlated data to a central backend for further processing. Edge security is powerful not only because of the data volumes of IoT environments but also from a responsiveness and isolation point of view. Edge security can provide increased responsiveness to exposures, threats and attacks by providing faster detection and remediation at the source, this is particularly useful if communications are intermittent or temperamental. Edge security also helps to isolate incidents at the source, potentially limiting the spread of attacks and protecting other pockets of the enterprise from revenue loss.

Such a setup is also relevant from a privacy perspective. Privacy-sensitive data can be processed locally. A seamless, edge and backend-based CIoT Security Intelligence solution is key to ensure timely performance, convenience, and a good user experience. If the data subject wishes can be easily enabled into edge devices and gateways, then appropriate information flow (and restriction) can be placed in the most appropriate location in the IoT Solution.

Secure end-to-end lifecycle management for Cognitive IoT

IoT endpoints are distinguished by three key characteristics. First, they are typically severely resource constrained. Second, they must operate in a hostile (not physically secure) environment without human intervention and for very long periods of time (10s of years). And third, they frequently support critical infrastructures, like energy production and distribution, transportation, healthcare, factory, and home automation. This means that while security and privacy of these endpoints is paramount, the opportunity to add security features at the hardware and software and in particular, the ability to support strong cryptographic protocols, is limited.

The growth of IoT systems has been inorganic, involving several players that has resulted in great heterogeneity in the capability of the endpoints and their market ownership. As result, there is a greater need to secure the lifecycle of these diverse IoT devices in order to have any confidence in the security of the IoT ecosystem. The following is a list of some key elements for securing the lifecycle of IoT devices:

- A **secure source of identity** that cannot be spoofed and that can be used to authenticate the endpoint. This is a common requirement across all network security protocols (IPSec, SSL/TLS, SSH) as endpoints need to be mutually authenticated in order to set up a secure channel. Closely related to this requirement is the need for some form of secure storage that can be used to store keys, passwords, certificates, etc. that prove identity.
- A set of **tamper detection and resistance mechanisms** for endpoints that may be subject to physical access by adversaries, for example in connected cars, smart homes, healthcare, etc. Tamper protection adds an additional layer of defense for sensitive keys, passwords, and certificates used to establish a secure channel or to encrypt data.
- A set of mechanisms to **control and verify the software that runs on the device,** applicable during boot-time, run-time, and during device updates. This is important to ensure that the right firmware/ software that implements cryptographic algorithms, network security protocols, secure storage, etc. is running on the IoT endpoint.
- A set of **cryptographic capabilities,** with possibly cryptographic acceleration, to support fast and efficient execution of capabilities such as encryption/decryption, signing/ verification, etc. and that is further optimized to execute efficiently on the platform. Since the IoT endpoint will typically exist in a hostile environment, it should be protected from attacks by users such as tamper attacks, side-channel attacks etc.
- A **secure and verifiable registry** that enables decentralized, at-the-edge registration and management of the endpoints. Such a registry would potentially entail input and validation from mutually-distrusting parties, and would contain information, such as the device identifiers, their capabilities, public cryptographic information, etc. To support automation and subsequent auditability, the registry should maintain history for updates, such as device identifier and capability changes, and such a history should be queryable. Technologies, such as Blockchain, satisfy many of these requirements and we are evaluating the use of Blockchain.

Leveraging IoT industry & standardization developments to secure the end-to-end (E2E) lifecycle of IoT endpoints

Hardware and device manufacturers like ARM, Intel, TI, and Freescale, are increasingly starting to build new capabilities for IoT endpoint security. For example, ARM mbed[34] will offer a form of secure boot, as well built-in cryptographic and protocol support for secure network connections. Freescale[35] has made available development boards for embedded processors equipped with e-fuses that allow the provisioning (write-once) of unique, tamper resistant identities. As reported in Linux community conferences, a number of embedded device manufacturers running Linux are planning to or already leveraging Linux integrity monitoring for their devices.[36] One example is Juniper networks which is exploring the use of IMA/ EVM in the OS of their networking devices.[37]

In the standards space, there are numerous organizations vying to define relevant IoT security standards. Among them, the Trusted Computing Group (TCG) has started a subgroup of the Embedded Systems Working Group, which is focused on IoT security and has generated a first draft of guidelines for securing IoT.[38] TCG is aiming to define a “minimal” set of core root of trust for IoT devices, providing similar capabilities to a Trusted Platform Module (TPM) but with a smaller footprint. This standard will establish the requirements for providing trusted identity and software integrity. It is worth mentioning that Microsoft and Google have made a joint proposal for minimal core root of trust for IoT devices that is currently being debated in the working group. IBM Research did some early work in this space under the TrustDust project.[39] Part of the work demonstrated end-to-end security by signing measurements and controlling access to keys through TPM integrity measurements.

The emerging endpoint security capabilities should be leveraged by IoT cloud endpoints and applications to provide comprehensive E2E security and encryption. There is a need to provide an ecosystem that supports the secure E2E lifecycle management for IoT devices. Some applications that support E2E lifecycle management are:

IoT code signing server

Code integrity is a critical aspect of IoT security. While emerging secure boot capabilities will ensure that IoT endpoints run only code signed by authorized software providers, managing the signing process, protecting the respective private keys, and handling the lifecycle of code updates is a sensitive process.

IoT vendors like Analog Devices[40] have identified this as one area of concern. The goal of signing code for IoT addresses both the initial provisioning of signed firmware from multiple providers, e.g., ARM, ADI, IoT device integrator (smart meter, automotive, healthcare, etc.), as well as subsequent updates.

IoT device integrity monitoring service

As IoT devices introduce secure and trusted boot capabilities, it will gradually become feasible to continuously monitor the integrity of their software during boot and run time.

Therefore, mechanisms for integrity monitoring for hosts, VMs, and containers can also be applied to IoT. In fact, in the IoT domain, endpoints are expected to run a much smaller set of applications and code, and hence, scalability issues in terms of number of measurements are expected to be muted. As an example, a service build for Linux monitoring could also be applied to IoT devices running embedded Linux.

Blockchain as a building block for IoT lifecycle management

Two key capabilities that will drive IoT in the new era are automation and transactions among mutually-unknown and mutually-distrusting endpoints. Automation will require an IoT endpoint to be able to discover the identity, capabilities and services available at other IoT endpoints.

Transactions will involve negotiation/ agreement for services and possibly some form of payment for the services. Many of these transactions, especially in critical sectors such as finance or healthcare, will be validated and recorded for future auditing.

Blockchain—the technology platform underlying the decentralized crypto-currency Bitcoin—is a ledger of transactions shared by participants of the network. Blockchain holds a record of every transaction ever completed in the network. Every block on the ledger contains a "hash" of the previous block and hence maintains an auditable record of all transactions. Since multiple copies of the ledger are stored and distributed across participants, and the construction of the ledger includes crypto-protected information, tampering with the ledger is extremely difficult and would require collusion between mutually distrusting parties. New implementations of Blockchain technology that target enterprise use cases, such as IBM Blockchain, support the concept that transactions can be audited by an authorized party and that transactions can be restricted to authorized parties.

Applying the Blockchain concept to the world of IoT offers fascinating possibilities of managing the lifecycle of IoT devices. As soon as an IoT endpoint is assembled (possibly as part of a product such as an automobile), it can be registered by the manufacturer into a universal Blockchain representing its beginning of life.

Once sold, a dealer or end customer can register it to a local Blockchain (e.g., permissioned by an enterprise). When registered, the IoT endpoint remains a unique entity within the Blockchain throughout its life. The possibility of maintaining device information, history, and software revisions in the Blockchain means the Blockchain itself can become the trusted IoT registry.

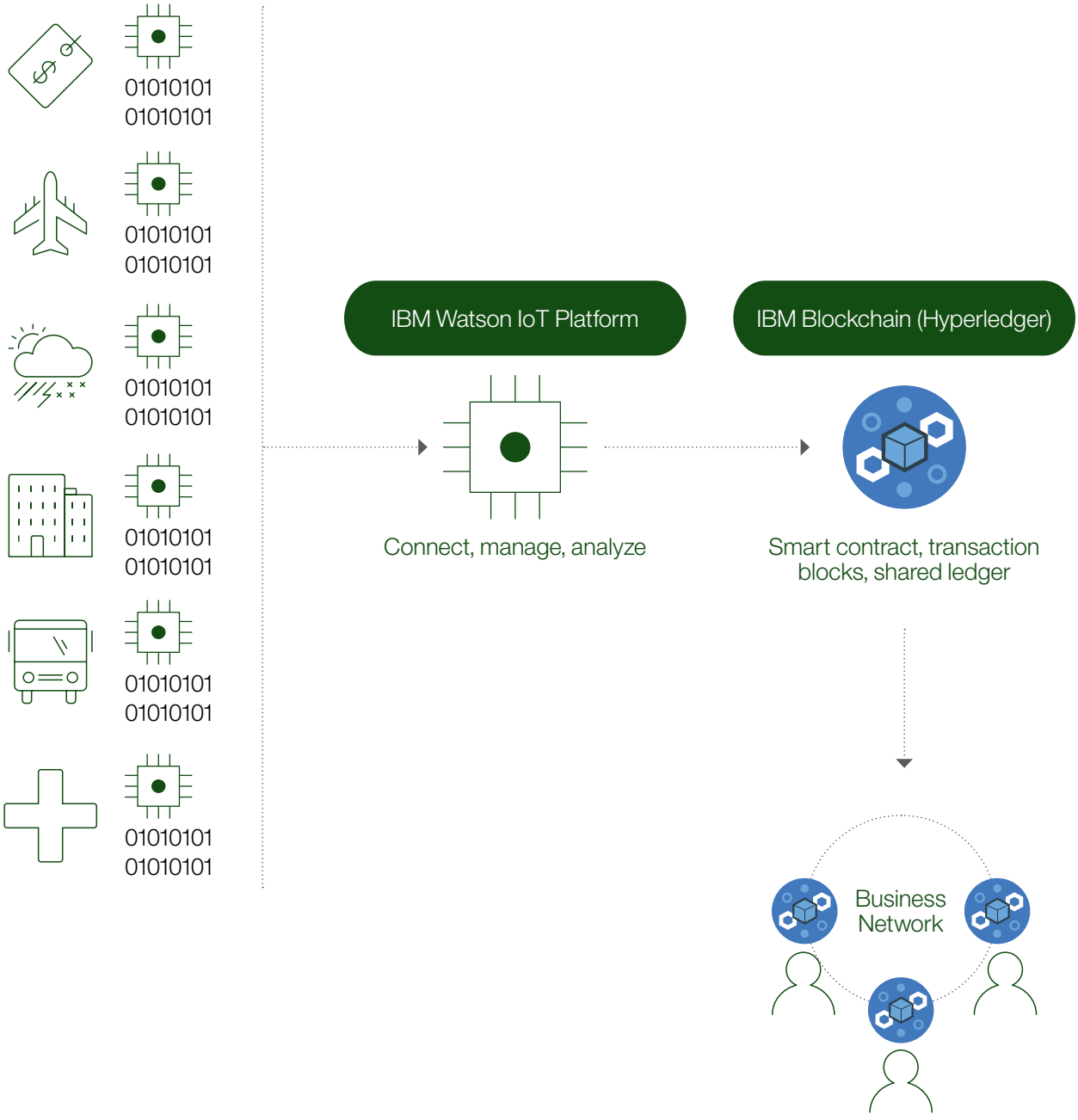

Figure 2:
The IBM Watson IoT Platform takes information from sensors and devices and communicates it to the blockchain ledger where it can be accessed by members of the business network.

Now imagine the scenario where two IoT endpoints are involved in a service transaction. The consuming device can query the Blockchain to know the capabilities and history of the endpoint providing the service, and make a judgment about the device reputation (for example, based on its security capabilities) to decide whether to follow through with the service. All this process can happen autonomously.

The transaction could be validated based on a smart contract and logged to satisfy future auditing requirements. *A Blockchain-assisted IoT can be a promising approach to autonomous transaction processing among devices.* However, how the solution is built, deployed, and maintained is critical to ensure that the solution itself does not become an additional candidate for attack and exploit, thereby widening the attack surface. If information about which devices are less secure, for example, those out of date firmware with known security vulnerabilities gets into the hands of the wrong people then that could circumvent all the other security measures in place.

Privacy

Privacy is a key concern for CIoT systems that are used to instrument personal, social, and work environments. On the one hand, the large corpus of data generated directly or indirectly can be used to learn and extract valuable contextual and behavioral information about the instrumented systems.

This corpus will enable and feed cognitive insights, actions, and continued learning. On the other hand, the same data may be used to infer sensitive information. When that information gathered pertains to human activity or human state a person may want to keep private or is security relevant. Advances cryptographic mechanisms and privacy by design principles can, in many cases, achieve the seemingly impossible to provide privacy while maintaining the ability to use the information to build the desired functionality.

Privacy preserving data sharing

A key objective of IoT applications is to achieve end-to-end security while allowing relevant data from IoT endpoints to be processed by approved parties, such as the cloud applications. Data should be under the control of device owners/ operators and only disclosed with cloud applications as appropriate and specified by data controllers and the agreements they have with their users. To that end, new lightweight cryptographic algorithms and protocols, as well as key management, are being be developed to allow E2E security between IoT endpoints and application endpoints and to allow selected data to remain private from other infrastructure components.

In some cases, existing IoT endpoints cannot be upgraded and do not have the hardware, OS, or application components to support E2E encryption. *IoT gateways* have been proposed as a way to insert a device to implement security and encryption features that is as close as possible to the actual IoT endpoints. Devices from, for example, Intel[41], ARM[42], and CISCO will implement the OS, containerization, hardware crypto and crypto algorithm support necessary for E2E security, as well as talk to the legacy endpoints and appropriately translate their protocols.

Data privacy

Understanding the tradeoff between utility gain and corresponding risk of sharing data is a major challenge for both individuals and enterprises. The simplest and often well understood binary choice is between Opt-In and Opt-Out, where selecting one over the other often implies sacrificing either utility or privacy completely.

Over the years, several other privacy approaches have been proposed for micro data release. This includes data anonymization techniques that sanitize the data by removing all personally identifiable identifiers (e.g., name, social security, etc.) and encodes the remaining quasi-identifiers (e.g., age, gender, zip code) through generalization and suppression of outliers such that it is difficult to distinguish (via de-anonymization attacks) a particular individual from a group of individuals. The metrics that are typically used for privacy include k-anonymity, l-diversity, and t-closeness.

While determining the optimal encoding for achieving k-anonymity is an NP-Hard problem, effective heuristic algorithms exist that ensure that the data encoding performed while satisfying the anonymity requirements maximizes a chosen utility measure. Instead of micro data, if one chooses to release aggregate statistics (e.g., mean, count, variance, histogram) computed over the data, then formal measures such as differential privacy can be used to perturb the function output (through addition of controlled noise) such that the ability of an adversary, with access to the perturbed function output and arbitrary side channel information, to determine if a particular individual is present or absent in the dataset is strictly bounded. This allows for the data to be sued for gaining insights and for machine learning, while not disclosing information about the data sets from which the data was collected.

Time series data from IoT systems, due to their large volume, high dimensionality and spatio-temporal correlation present unique privacy challenges. Unlike relational databases or other structured data types, the semantic interpretation of a sequence of time annotated vector values (e.g., a location trajectory of latitude, longitude pairs) is often unclear. Preprocessing is thus essential even to determine the information that needs to be protected (e.g., trajectory plotted on a map reveals home, work, and other places visited).

CIoT systems can learn this contextual information embedded in the data can help reduce the dimensionality of the data as well as provide insight into the behavioral patterns of the system under operation. These behavioral patterns once encoded by computational models can be used to design better anonymization and perturbation techniques that can handle the privacy needs in a much more effective manner while maintaining data utility. This remains an area of active research.

Privacy protecting authentication

Many legacy IoT networks are not protected by firewalls. It is thus important that data collected by devices and the devices themselves both be authenticated and that communication be encrypted.

While the technology for the latter is readily available, the standard solution for the former two requirements result in the data and the devices being uniquely identifiable. This is problematic from both a privacy and a security point of view. Consider for instance usage data collected by a device. On the one hand, if all usage data can be linked to a particular device, this allow one to deduce information about the owner of the device (e.g., at home only on Wednesdays) or about production and process secrets of a company (possible in connection with data from other related devices).

On the other hand, it might be that the usage data needs to be attributable to a certain device under exceptional circumstances, e.g., in case of warranty claims. Modern cryptography provides tools that allow one to address both these seemingly contradicting requirements. Example protocols addressing just the basic use cases are TCG's (Trusted Computing Group) direct anonymous attestation and Intel's EPID work.[43]

Translatable identifiers for distributed databases

Collecting and processing all data in a single location introduces a single point of failure and attack. Instead, collecting and processing the data in a distributed fashion is preferable from a data security and privacy point of view and often also because of operational aspects.

Indeed, it has been shown that distributed systems often outperform centralized ones (examples include traffic control systems and government processes). To protect decentralized data, different and unlinkable identifier should be used for the same data subject in the different databases. Nevertheless, this should not prevent the exchange of data about the subject between these databases. Also here, modern cryptography offers many solutions addressing such requirements.

Best Practices: IBM POV: Internet of things security

The following is a digest summary from the 2015 IBM Point of View on IoT security.

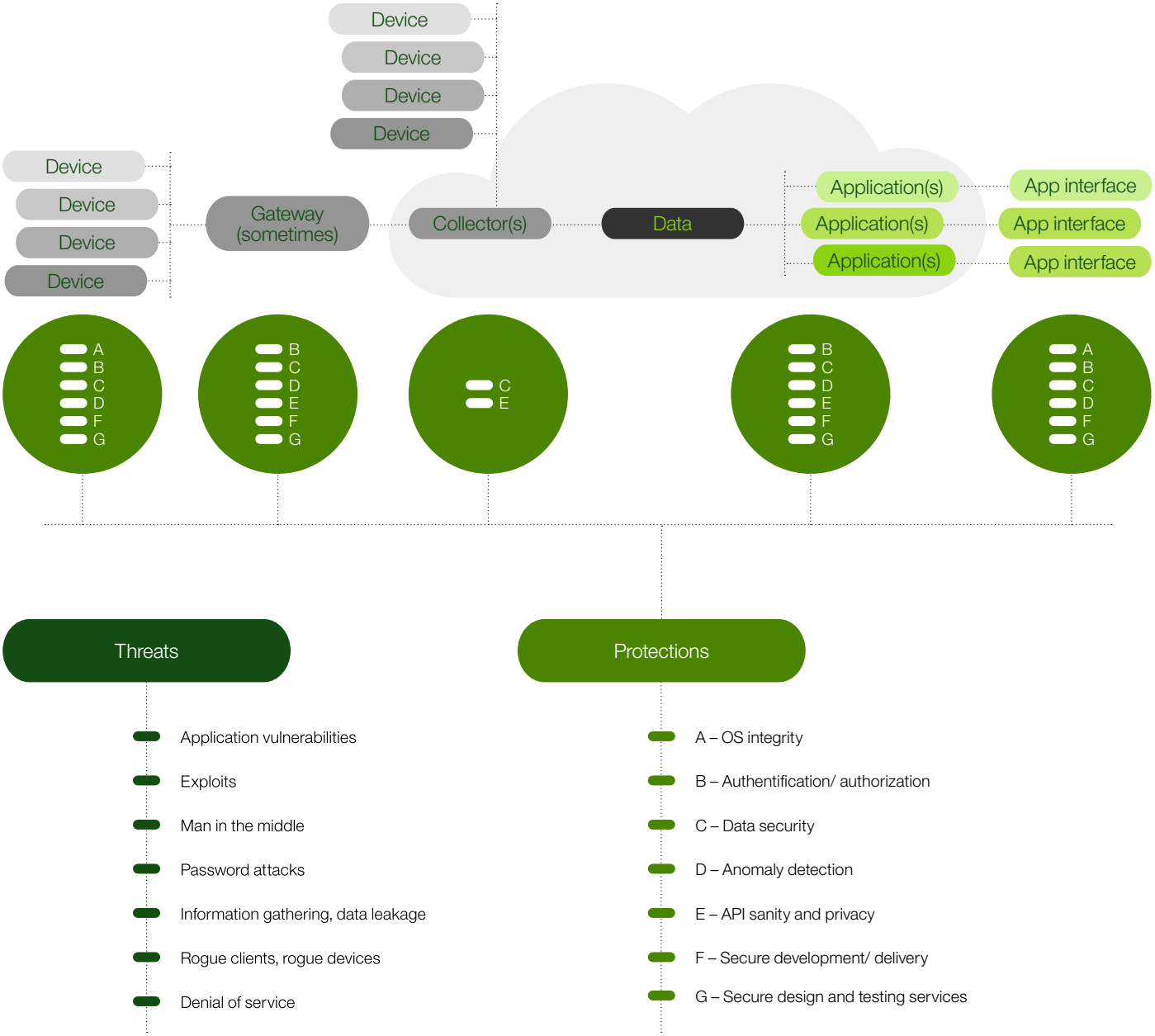

Figure 3:
IoT system with threats and protections annotated

Makers of things—Design and manufacture securely

IBM has published its internal best practices for software assurance and cyber supply chain security in the IBM Secure Engineering Framework (SEF)[45]. Makers of things should understand these frame works and the following best practices in order to understand and address how they manufacture and deploy IoT devices.

Design for security

Key to this approach are the following five practices.

- Apply Secure Engineering principles to the design of connected devices and the environments in which they operate.
- Defense in depth—have multiple layers of defense in the solution.
- Devices are "in the wild" and now part of the attack surface.
- Devices that were isolated before are now connected, which considerably broadens the potential significance of any security breach.
- Fail-safe modes of operation must be assured for devices, even if they become isolated from communication with other parts of the environment. Indeed, disconnecting devices or voluntary removal of a device from the network may be part of the device's response to detective suspected attacks.

Design for privacy

We need to focus on four key privacy issues, when we design for privacy.

- Employ data separation, segregation, redaction, and data transformation techniques to remove or obscure personally identifiable information.
- Unique device identifiers can be considered personally identifiable in some situations. (This point becomes even more important as we look at cognitive systems).
- Use ephemeral and separate identifiers in communications and data storage.
- Isolate associations with unique device identifiers and with unique personal information.

Test for security

Testing of complex systems is difficult; testing of Cognitive Systems even more so. Having an appropriate system in place to test security of these systems requires that you have an approach that addresses the unique aspects of systems which learn. Understanding your architecture, system, and data flows is not enough, you must think about how the system will learn and what thresholds of data may change behavior. This is an area where more information will be coming forward as the industry matures.

However, at a minimum testing approaches must understand four key items.

- Security testing techniques apply to devices as they apply to any other software system.
- Code analysis, ethical hacking, and other techniques apply to devices and device-side code.
- Hostile environment testing extends beyond physical hostile conditions to include communications and network in hostile conditions.
- Code validation, using multiple checks at all stages of code: creation, build, delivery, signed Firmware Over the air (FOTA), and even with in memory validation checks during runtime.

Continuous delivery model

Systems under constant attack need the ability to be updated against threats continuously. This process is called continuous delivery.

You should understand and address four key points.

- Problems and vulnerabilities will be detected after the devices and systems are manufactured, delivered, and deployed.
- In-service updates to device-side code will be necessary.
- Plan for and utilize continuous delivery techniques for device-side and application-side code.
- Special considerations are necessary for determining when to apply/enact/enable updates. Systems in use should be able to be updated, and if an update fails, the device or system should be able to roll back to a known state.

Ensure integrity in manufacturing and delivery

Having a trusted supply chain is a key aspect ingredient to the manufacturing and delivery of secure devices.

Following the guidelines for supply chain integrity should ensure that your customers receive the device as you indented to build it.

- Commit to defined supplier conduct and security principles.
- Submit to periodic assessments.
- Commit to remediation actions if found to be out of compliance.
- Ensure the robustness, stability, performance, and security of components.
- Ensure that software and firmware development libraries and documentation have proper access controls.
- Provide certificate of originality by documenting the source of all delivered components.

Operator of things—Operate securely

As an enterprise begins deploying IoT systems, understanding how to operate these systems securely is critical. As we've discussed earlier in this paper, this systems and devices will expose new attack surfaces either through communications or through physical environment considerations.

IBM recommends that at a minimum you focus on five key approaches for operating your IoT systems securely. *Investing in continuous security education for security practitioners and solution operators is critical in the fight to maintain a healthy security posture. Educating end users and customers on best practice for security for IoT is important to reduce attack surface through the insider threat.* Knowing what to do and when in the event of security breaches through a defined and well drilled incident response program is incredibly valuable to enterprises and their customers.

Harden the device (check for device resiliency)

While a comprehensive development, test, and manufacturing process can increase the security of a device, it cannot prevent all potential security threats. Having multiple layers of defense for your solution is critical; techniques include (but are not limited to) firewalls and packet filtering and network segregation via gateways and routers to isolate vulnerable subsystems and devices.

Consider enabling a means of isolating compromised subsystems so that the overall solution remains available is also critical for business and process continuity. Furthermore, reduce the attack surface for devices and applications by elimination any extraneous or unnecessary functions in a device or application. As a simple example, if FTP is never to be used, remove the FTP client and server functions from devices gateways and applications. Taking this a step further, test that there are no unexpectedly open ports of communication.

Secure the communications channel

There are many different communication protocols for IoT solutions, including standards such as Bluetooth Low Energy, 6LoPAN, Zigbee, low power-long range methods, WiFi, 2G, 3G, and 4GLTE, along with high layer communication models, like DDS, CoAP, MQTT, UDP, TCP, and other IP based protocols. It is critical that you not only setup secure communication paths between devices and systems, but that you maintain that security.

Network type and connections might not be trusted, so periodic audit, validation and remediation will be required. Follow the established guidance for each protocol that is used in your system to ensure appropriate security practices. Ensure that you are using the appropriate security protocol, such as SSL/TLS, for the specific communications protocols you are using.

Audit and analyze usage patterns

While a securely developed and deployed system is a good start, it is not a guarantee of a securely running system. Attackers will continually probe and take new and novel approaches to attempt to breach the system. Prevention will not address all issues. You must have systems in place to detect when breaches have occurred.

Identification and timely response and remediation procedures need to be in place. Using existing log analysis techniques to identify and respond to anomalies is a good start; however, as we've discussed earlier, cognitive system which learn normal behavior and can automate the response to anomalies may reduce false positives and increase the security of your IoT System. Testing your response and remediation procedures is also recommended.

Maintain an up-to-date security environment

Enterprises have difficulty today to keep all their systems up to date across standard operating systems and applications. With IoT this challenge can be more daunting due to the increasing number and types of of embedded systems and variety of protocols.

Having a process and approach to keeping your IoT systems up to date should cover: authentication, authorization, auditing, administration, encryption/decryption, key management, software, hardware, and integrity checking. A combination of technologies and processes ensure that the environment remains secure.

Create a trusted maintenance ecosystem

It is highly unlikely that every aspect of your IoT system is built in-house. From the silicon to the applications, you will have an ecosystem of partners. Given that devices are operating in much less controlled conditions than systems running in a data center, cloud, or other controlled environment, you must create a trusted maintenance ecosystem.

You should follow existing guidance on setting up and maintaining all aspects of your secure IoT environment. Identification and communications of security related incidents and updates should be a key aspect of your comprehensive security incident response process. Building and investing in an ecosystem that develops and has security intelligence is also equally important.

Risk dashboard

IoT platforms provide a mechanism to consolidate and manage IoT devices and data from multiple sources. The selection and use of an IoT platform that maintains sound security operations is important in order to complement all of the other security measures enterprises put in place. Distinguishing and selecting those IoT platforms that have capabilities to address advanced security use cases could not only save time, money, and effort for enterprises IoT solutions, but also mean the difference between seeing a security threat and being able to address it before it is a major problem and being a victim of an attack. The IBM Watson IoT™ Platform provides a comprehensive solution to address the complexity of IoT security, based on both existing industry leading security solutions and IBM Researcher's cognitive Security solutions. It all begins with defining your risk management policy. This policy should address both internal and external criteria/ exposures. Policies are time sensitive based on the deployment of your IoT solutions, with a focus on risk reduction and compliance.

As your Cognitive security solution identifies suspect or compromised devices, cognitive systems should automatically quarantine these devices for further analysis. As Cognitive IoT Security solutions learn and discover exposures, the automation of policy improvement requires a granularity that does not scale well with traditional SOC practices.

IBM Watson IoT Platform will provide enhanced security features allowing visibility to possible exposures across the IoT landscape, alerts for immediate notification, and automatic operational responses tailored to individual customer environments.

The Risk Dashboard will allow your SOC to scale policy, discovery, and detection of IoT Security issues in line with the Security 360° approach described in this paper.

Standards and specifications

Many existing standards and guidance organizations, world-wide, are working on guidelines and recommendations for IoT and security in IoT systems. In particular, ISO/IEC, IEEE, ETSI, Industrial Internet Consortium (IIC)[46], Open Interconnect Consortium (OIC), NIST[47], CERT, and the EU Alliance for Internet of Things Innovation (AIOTI). There are also messaging and protocol, as well as industry-specific standards organizations, which are addressing security as part of their efforts, including: GSMA[48], AllSeen Alliance[49], ARM mbed[50], TCG[51], MQTT[52], and IBM's own Secure Engineering practices.[53]

Additionally, there are many standards and frameworks for development of safety critical systems (DO-178B for Aviation[54], IEC 61508 for Software safety[55], and others). These systems recommend specific requirements processes, test coverage and other disciplines in order to ensure that all aspects of a safety critical system behave as expected under defined conditions, and also have appropriate behavior in unknown situations. As multiple sub-systems are connected together, the larger combined system must also adhere to the requirements, as a safety critical system must be safe across all levels of that system. This same thought should also be applied to security in systems. The requirements for security of a system or application should not be undermined by one component that does not address those requirements.

What areas do we see evolving standards?

Standards take time to develop; the Cognitive Internet of Things is the evolution of the Internet of Things with added capabilities and complexity as we've defined above. IBM is working with customers to identify the benefits of security and address the threats of the Cognitive Internet of Things. We expect that the next generation of standards will begin to address these challenges. Open and active participation by researchers, businesses, and institutions can address the balance between privacy and utility, while at the same time considering safety of an instrumented, interconnected, intelligent and cognitive world.

Where should you go for more information or help?

The IBM Watson IoT Platform offers industry-leading solutions for the development of CIoT solutions.

For more information on how IBM can your enterprise leverage CIoT, visit **ibm.com**/internet-of-things/learn/what-is-watson-iot.

This framework can be applied broadly for use, not only for software application development, but also with connected devices and IoT Systems.

Footnotes

1. Kevin Ashton, "That 'Internet of Things' Thing: In the real world, things matter more than ideas. RFID Journal, June 2009, http://www.rfidjournal.com/articles/view?4986

2. IBM Point of View: Internet of Things Security, http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=RAW14382USEN

3. Water Utility Hacked: http://www.theregister.co.uk/2016/03/24/water_utility_hacked/

4. "Everything we know about Ukraine's Power Plant Hack", https://www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/

5. Hacking Baby Monitors, http://securityaffairs.co/wordpress/39811/hacking/hacking-baby-monitors.html

6. The surprising way your fitness data is really being used, https://www.outsideonline.com/2101566/surprising-ways-your-fitness-data-really-being-used

7. Hacking Pacemakers, http://abcnews.go.com/Health/HeartFailureNews/security-experts-hackers-pacemakers/story?id=10255194

8. The IBM vision of a smart home enabled by cloud technology, http://www.ibm.com/smarterplanet/global/files/uk__uk_en__cloud__a_smarter_home_enabled_by_cloud_computing.pdf

9. Devices and Diseases: How the IoT is Transforming MedTech, http://dupress.com/articles/internet-of-things-iot-in-medical-devices-industry/

10. Spence Wende, Chris Smyth, The new Minnesota Smart Bridge, http://www.mnme.com/pdf/smartbridge.pdf

11. Diane Cardwell, Grid Sensors Could Ease Disruption of Power, http://www.nytimes.com/2015/02/04/business/energy-environment/smart-sensors-for-power-grid-could-ease-disruptions.html

12. How the Internet of Things Is Transforming Manufacturing, http://www.forbes.com/sites/ptc/2014/07/01/how-the-internet-of-things-is-transforming-manufacturing/

13. The Smart and Connected Vehicle and The Internet of Things, http://tf.nist.gov/seminars/WSTS/PDFs/1-0_Cisco_FBonomi_ConnectedVehicles.pdf

14. IoT market analysis, http://postscapes.com/internet-of-things-market-size

15. McKinsey&Company, Disruptive technologies: Advances that will transform life, business, and the global economy, http://www.mckinsey.com/insights/business_technology/disruptive_technologies

16. "CYBERSECURITY: Threats Impacting the Nation", http://www.gao.gov/products/GAO-12-666T

17. David Kushner. The Real Story of Stuxnet, http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

18. Hackers Cut a Corvette's Brakes Via a Common Car Gadget, http://www.wired.com/2015/08/hackers-cut-corvettes-brakes-via-common-car-gadget/

19. D. Lundberg, B. Farinholt, E. Sullivan, R. Mast, S. Checkoway, S. Savage, A. C. Snoeren, and K. Levchenko, "On the security of mobile cockpit information systems," in Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, 2014.

20. Hackers Remotely Kill a Jeep on The Highway, http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

21. Connected Medical Devices: The Internet of things-that-could-kill-you, https://www.washingtonpost.com/news/the-switch/wp/2015/08/03/connected-medical-devices-the-internet-of-things-that-could-kill-you/

22. D. Genkin, A. Shamir, and E. Tromer, "RSA key extraction via low-bandwidth acoustic cryptanalysis," in Advances in Cryptology, 34th Annual Cryptology Conference, CRYPTO 2014.

23. M. Enev, S. Gupta, T. Kohno, and S. N. Patel, "Televisions, video privacy, and powerline electromagnetic interference," in Proceedings of ACM Conference on Computer and Communications Security, 2011.

24. U. Greveler, B. Justus, and D. Loehr, "Multimedia content identification through smart meter power usage profiles," in Computers, Privacy and Data Protection, 2012

25. M. Kuhn, "Optical time-domain eavesdropping risks of CRT displays," in IEEE Security and Privacy, 2002

26. M. Kuhn, "Compromising emanations of LCD TV sets," in IEEE International Symposium on Electromagnetic Compatibility, 2011

27. Y. Michalevsky, A. Schulman, G. A. Veerapandian, D. Boneh, and G. Nakibly, "PowerSpy: Location tracking using mobile device power analysis", in USENIX Security Symposium, USENIX Security, 2015

28. R. J. Masti, D. Rai, A. Ranganathan, C. Muller, L. Thiele, and S. Capkun, "Thermal covert channels on multi-core platforms", in USENIX Security Symposium, USENIX Security, 2015

29. http://www.ibm.com/analytics/us/en/technology/general-data-protection-regulation/

30. "Sixth annual Ponemon Benchmark Study on privacy and security of healthcare data incidents", https://www2.idexpertscorp.com/sixth-annual-ponemon-benchmark-study-on-privacy-security-of-healthcare-data-incidents

31. http://www.computerworld.com/article/2493701/data-center/by-2020--there-will-be-5-200-gb-of-data-for-every-person-on-earth.html

32. http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

33. https://s3.amazonaws.com/nist-sgcps/cpspwg/files/pwgglobal/CPS_PWG_Framework_for_Cyber_Physical_Systems_Release_1_0Final.pdf

34. ARM MBED IoT Device Platform. (n.d.). Retrieved from http://www.mbed.com/en/

35. http://www.freescale.com/tools/embedded-software-and-tools/hardware-development-tools/startertrak-development-boards:STARTERTRAK_HOME

36. Linux Security Summit: Linux Integrity Subsystem Status. Retrieved from http://kernsec.org/files/lss2015/LSS2015-LinuxIntegritySubsystemStatus.pdf

37. Linux Security Summit: IMA/EVM: Real Applications for Embedded Networking Systems.

38. http://www.trustedcomputinggroup.org/resources/tcg_guidance_for_securing_iot

39. Trust Dust. IBM Research.

40. http://www.analog.com/en/index.html

41. https://www-ssl.intel.com/content/www/us/en/embedded/solutions/iot-gateway/overview.html

42. http://www.mbed.com/en/

43. http://download.intel.com/newsroom/kits/idf/2015_fall/pdfs/Intel_EPID_Fact_Sheet.pdf

44. http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=RAW14382USEN

45. IBM Secure Engineering Framework, http://www.redbooks.ibm.com/abstracts/redp4641.html

46. Industrial Internet Consortium, http://www.iiconsortium.org

47. NIST Cybersecurity framework, http://www.nist.gov/cyberframework/

48. GSMA Security Guidelines, http://www.gsma.com/connectedliving/future-iot-networks/iot-security-guidelines/

49. AllSeen Alliance Security 2.0, https://allseenalliance.org/framework/documentation/learn/core/security2_0

50. ARM MBED IoT Device Platform. (n.d.). Retrieved from http://www.mbed.com/en/

51. http://www.trustedcomputinggroup.org/resources/tcg_guidance_for_securing_iot

52. MQTT and the Nist Cybersecurity framework, http://docs.oasis-open.org/mqtt/mqtt-nist-cybersecurity/v1.0/mqtt-nist-cybersecurity-v1.0.html

53. IBM Secure Engineering Portal, http://www-01.ibm.com/software/test/wenses/security/

54. https://en.wikipedia.org/wiki/DO-178B

55. http://www.61508.org/index.php

IBM Corporation
Route 100
Somers, NY 10589

Produced in the United States
of America, October 2016

Statement of Good Security Practices:
IT system security involves protecting systems and infor-mation through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

WWS12379USEN-00

Watson IoT™