Is Your Internet Of Things (IoT) Trustworthy?

Abstract

The Internet of Things (IoT) is undergoing major transformations, shifting to autonomous (intelligent) operations across a connected mesh of devices with data aggregations and control at a global level (e.g., cloud computing platform with big data analytics). The merging of the networked physical and cyber components also requires the merging of various disciplines to properly evaluate risk and achieve required levels of security, privacy, and situational awareness. This is a far greater challenge than many organizations may anticipate.

To meet this challenge, organizations should strive to achieve an acceptable level of IoT trustworthiness through risk model analysis for cybersecurity, privacy, reliability, resilience, and safety. Additionally, a new thought leader (e.g., Trust Officer) is required to ensure adequate levels of trustworthiness for the IoT. The CEO and Board of Directors will ask "Is our IoT trustworthy?" As the IoT becomes pervasive and central to enterprise operations, organizations will seek a level of trustworthiness for the business as a whole. The CEO and Board of Directors will ask "Is our business trustworthy?"

Definitions

Internet of Things (IoT) – "Network of physical objects or 'things' embedded with electronics, software, sensors, and network connectivity, which enables these objects to collect and exchange data." IoT is also described as connected smart systems, the Industrial Internet, Cyber-Physical Systems (CPS), machine-to-machine (M2M), smart cities, etc.

Cyber-Physical Systems (CPS) – "Integration of computation, communication, sensing, and actuation with physical systems to fulfill time-sensitive functions with varying degrees of interaction with the environment, including human interaction."

Trustworthy – "The system does what is required despite environmental disruption, human user and operator errors, and attacks by hostile parties and that it does not do other things."

Concerns

IoT is an emerging technology which so far lacks proven frameworks. Standards are still evolving.

IoT projects are significantly broader in scope and require collaboration among many thought leaders (risk, IT, cybersecurity, legal, compliance, physical security, and engineering).

The supply chain for IoT will be vast and global with risks, threats, and vulnerabilities at the component, device, and system levels.

While the opportunities offer significant business productivity gains and cost savings, IoT introduces new challenges for both risk and security professionals.

Actions

Discover opportunities where you can leverage the IoT for significant gain or competitive edge.

Don't block potentially successful IoT projects based on security concerns or other unexplored assumptions.

Tear down traditional silos and work collectively across all NIST risk properties.

Enable the business by starting IoT projects as a Proof of Concept (POC) with trustworthiness being one of the stated goals.

Even while in draft form, the NIST Framework for Cyber-Physical Systems can provide useful guidance in designing, building, and verifying IoT and as a tool for analyzing complex IoT.

Use standards and open source algorithms when possible.

Align your organizational (or project) structure with the Trust(worthy) Framework which will establish proper roles and responsibilities.

When embarking on an IoT project, do not attempt to 'boil the ocean'. Divide the project into subsets and use an iterative approach while implementing lessons learned after each iteration.

Analysis

The promise of the Internet of Things (IoT) is already being realized by organizations with a significant return on investment. With the growth of IoT devices installed projected to reach 26 billion by 2020, it's not a matter of if firms will get on board, but when. The impetus is toward early adoption to gain competitive advantage, however, securing the IoT ecosystem is one of the greatest challenges firms will face. Those who venture into this space without ensuring their systems are secure may face financial, legal, compliance, reputational, and operational consequences.

The IoT bridges the digital and physical worlds represented by one device or multiple interconnected devices called a System-of-Systems (SoS). The sheer breadth and depth of the potential IoT market is visually represented by Beecham Research's Sector Map which is categorized by Service Sectors (e.g., Energy), Application Groups (e.g., Alternative), Locations (e.g., Wind), and Devices (e.g., Windmills). The Department of Homeland Security (DHS) states that "any IOT system's security is limited to the security level of its least secure component...in addition to the typical vulnerabilities of IT systems, IoT enabled systems create additional security concerns because IoT domains are: autonomous and control other autonomous systems; highly mobile and/or widely distributed; are vulnerable to physical and virtual threats."

IoT devices are composed of physical, analog, and cyber components which interact and must be well understood to assess risks. In addition, there are numerous timing aspects related to the physical and cyber architectures which affect the goal of ensuring access to secure and resilient times.

Trustworthiness

Managing risk and securing an IoT project is broad in scope and requires a larger model than the traditional cybersecurity triad of confidentiality, integrity, and availability. Gartner, Inc. recognized this deficiency and in June 2015 they shook the cybersecurity world's foundation by expanding the sacred CIA triad tenets to include safety (CIAS). Enterprises who manufacture or deploy devices which can potentially harm human life, either directly or indirectly, should develop a risk model which favors safety.

In September 2015, the National Institute of Standards and Technology (NIST) released their draft *Framework for Cyber-Physical Systems*. Further expanding the risk and security scope, they declared IoT systems must be trustworthy - "the system does what is required despite environmental disruption, human user and operator errors, and attacks by hostile parties and that it does not do other things."

Trustworthiness systems contain the following NIST risk management properties:

Cybersecurity (or security) - Operational and Reputational Risk
"A condition that results from the establishment and maintenance of protective measures that enable a system to perform its mission or critical functions despite risks posed by threats to its use. Protection measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the enterprise's risk management approach."

Privacy - Unwanted Disclosure Rates
"A condition that results from the establishment and maintenance of a collection of methods to support the mitigation of risks to individuals arising from the processing of their personal information within or among systems or through the manipulation of physical environments. Risk mitigation controls may involve a combination of administrative, policy and technical measures directed at maintaining individual's autonomy and their physical, financial and psychological well-being."

Safety - Error Rates
"Absence of catastrophic consequences on the user(s) and the freedom from unacceptable risk of physical injury or of damage to the health of people, either directly, or indirectly as a result of damage to property or to the environment."

Reliability - Failure Rates
"The ability to provide a consistent level of service to end users or continuity of correct service."

Resilience - Recovery Rates
"The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents."

NIST warns the most significant cybersecurity challenge is the requirement for resilience. While reliability engineering attempts to ensure predictable system performance where interactions and environments are known, resilience addresses uncertainty, where interactions and environments are not known or well understood.

Ultimately, IoT environments may extend regionally, nationally, and globally with far greater exposure and potential risk of exploitation than traditional IT systems. A new ecosystem is needed to design, manufacture, test, deploy, manage, and destroy these devices. Trustworthiness must be part of the entire IoT life-cycle, not an after-thought.

It's important to understand that trustworthiness does not mean a device or SoS has absolute security and cannot be compromised. Trustworthiness provides some level of assurance the device will function as expected in given situations. For example, if a device is compromised it could limit its functions, fail-safe, or gracefully degrade. Dynamic adversary models should be created to understand the impacts of various attacks and the appropriate response. NIST highlights the need for proactive, real-time, autonomic algorithms and architectures which can defend dynamically against these adversary models.

The Trust(worthy) Framework

The trustworthy aspect of IoT will not exist in a vacuum – organizations will be a reflection of the trustworthiness of their operations. It will extend to all facets of the organization, affecting relationships with employees, business partners and customers. Are your employees, partners, and customers trustworthy? A trustworthy organization is the next evolution of the security culture.

IoT owners, developers, and operators should have an organizational structure and risk model that enables and supports the NIST risk management properties. As the IoT permeates an enterprise, an organizational structure which naturally enables and ensures trustworthiness will be advantageous. To lead this initiative, a new thought leader is needed, the Trustworthy Officer.

The Chief Trust(worthy) Officer (CTO or CTwO) reports to the CEO and is responsible for the trustworthiness of IoT devices, and SoS. Each NIST risk management property has a corresponding owner who reports to the CTO: Cybersecurity Director, Reliability Director, Safety Director, Resilience Director, and Privacy Director. It's likely the CISO will fill the Chief Trust Officer role. In smaller organizations the CTO can manage all roles.

The CTO should also collaborate with other C-Levels to ensure that IoT projects are aligned with the organization's risk appetite, adheres to enterprise policies, meets compliance requirements, are technically feasible, have adequate budget, and have skilled and available staff: Chief Risk Officer (CRO), Chief Executive Officer (CEO), Chief Legal Officer (CLO), Chief Information Officer (CIO), Chief Financial Officer (CFO), and Chief Human Resources Officer (CHRO).

The CTO must be well versed in and think holistically across all risk properties. Furthermore, all risk properties must be addressed for a device, or devices working together in a SoS, to be considered trustworthy. Care must be taken to ensure concerns for one property does not put the device at risk for another property. Other IoT stakeholders play a vital role in system success and should understand and potentially participate in the goal of trustworthiness. These include IoT customers/users, supply chain providers, insurers, regulators, competitors, and governments.

These concepts comprise The Trust(worthy) Framework (illustrated below), based on the NIST risk management properties, is an organizational model and holistic approach for achieving IoT trustworthiness.

The IoT Organization

While the Trust(worthy) Framework is not applicable to most organizations in the short-run, virtually every organization will become an IoT organization in the long run. Why? Today, most organizations manage their business using information technology - in fact, many identify themselves as an information technology business because a large part of their operations are rooted in technology. IoT will have an effect orders of magnitude greater than today's usage of information technology. Furthermore, organizations won't need to build and own the IoT infrastructure to be an IoT organization in the same way they don't need to build and own cloud services today (IaaS, PaaS, SaaS). IoT infrastructure can be built and owned or consumed as a service (Internet of Things as a Service - IoTaaS).

A case study is Amazon, born on the World Wide Web with services such as streaming audio and video is arguably as much an IT company as a retailer. Amazon Web Services is the leader in the cloud services sector. Could anyone have predicted ten years ago that a retailer would be the world's largest provider of cloud computing services? Amazon is not resting on its successes. They are redefining warehousing through the use of robotics and analytical software. Next, they may disrupt the logistics sector by investing in their own airplanes, trucks, and delivery drones. Amazon has transformed itself from a web based company to a cloud based organization. They will transform again into an IoT based organization which leverages their information technology and cloud-computing roots. IoT will improve every facet of their current offerings and introduce new ones they have yet to conceive. It is likely Amazon will create IoTaaS offerings with the open sourcing of algorithms and APIs.

Similarly, as other organizations' IoT implementations become central to their operations, cybersecurity, privacy, reliability, resilience, and safety should be considered for virtually everything they do. Sensors will be ubiquitous and will have the capability to see, touch, hear, and smell. Some will be fixed while others will be mobile. Industry standards will enable the use of interoperable components which drive down costs. Algorithms will power intelligence and machine learning which will add a wide-range of capabilities such as determining and maintaining situational awareness.

The development of intelligent algorithms could be cost prohibitive for many firms. However, algorithms released into the open source domain will drive innovation as they are incorporated into new devices. Also, if organizations donate their algorithms to the open source community benefits can be realized, such as algorithms being tested on large scale. For example, the Advanced Encryption Standard (AES) is a widely used cipher (algorithm) which is free for public, private, commercial or non-commercial use. As AES was incorporated into solutions it withstood rigorous testing in varied environments over the years, resulting in achieving more trust and usage globally. Therefore, for IoT projects, organizations should evaluate and incorporate algorithms which are open and well tested, thus having a certain level of trust. Firms should incorporate trustworthy algorithms into trustworthy components and ultimately, into trustworthy SoS.

IoT Risk Model Analysis

IoT are subject to physical, cyber, and hybrid attacks. Attackers will seek to damage the device's physical (physical properties), analog (convert physical data into digital and vice versa), and/or cyber (logical, mathematical, computational) components. System designers and integrators should estimate risk across properties for each component element, physical, analog, and cyber.

The following table is a representation of the NIST CPS Risk Analysis[1] for components physical, analog, and cyber. The risk model analysis considers the impacts for each device and to the entire SoS. Risk models affect goals and requirements. For example, if a risk model favors privacy for the cyber component, that priority should be reflected in the goals and requirements (and design) of the device and/or SoS.

IoT Risk Model Component Analysis

	Component Impact		
Risk Properties	**Physical**	**Analog**	**Cyber**
Cybersecurity (operational/reputational risk)	High	High	High
Privacy (unwanted disclosure rates)	High	Low	High
Reliability (failure rates)	High	Medium	High
Resilience (recovery rates)	Low	Low	Low
Safety (error rates)	High	High	High

1. CPS PWG Draft Framework for Cyber-Physical Systems, Release 0.8 (page 75, Figure 22: Applying Risk Analysis to CPS)

For evaluating risk across the entire system you can consolidate your component analysis or start at a SoS level to gauge where risks are incurred. For example, the risk property impacts for a theoretical chemical plant are presented in the following table. Different chemical plants may have different business priorities, threats, and vulnerabilities resulting in different risk property impacts.

IoT Risk Model System-of-System (SoS) Analysis for a Chemical Plant

Risk Properties	**Impact**
Cybersecurity (operational/reputational risk)	High
Privacy (unwanted disclosure rates)	Low
Reliability (failure rates)	High
Resilience (recovery rates)	Low
Safety (error rates)	High

The goal is to have a traceability of risk property impacts from the component level up to the SoS level and from the SoS level down to each component level. With this information system designers and integrators can focus on those properties which require more effort for risk mitigation.

Wayne Scarano, CISSP, CCSK, SABSA
Cybersecurity Analyst
wscarano@sga.com