SGA
CYBER SECURITY

The IoT Shadow Trust Framework (IoTSTF)

Abstract

The Internet of Things (IoT) shadow [1] model is disrupting the design, development, maintenance, quality, and support of the devices they mirror. Next, IoT shadows will disrupt how we secure these devices as an integral part of the device lifecycle, incorporating the concept of security by design. The use of IoT shadows in the security domain is the foundation of The IoT Shadow Trust Framework (IoTSTF).

IoTSTF embodies the **concept of pursuing device trustworthiness through the analysis of IoT shadows and their associated data streams**. Following in the footsteps of IoT engineers, security professionals should embrace the IoT shadow model to develop and implement shadow based solutions for cybersecurity, privacy, reliability, resilience, and safety. Moreover, this conceptual framework offers opportunities for IoT vendors to develop new device shadow products and services.

Definitions

[1] IoT Shadow - a cloud-based functional representation (mirror) of, with operationally driven data from, an Internet of Things (IoT) device. Also referred to as, although not always synonymous with, a device mirror, device twin, cyber twin, virtual twin, digital twin, digital clone, device shadow, or avatar.

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.

Trustworthy – Fred B. Schneider describes trustworthy as "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."

Data Lake - a large storage repository and processing engine. They provide "massive storage for any kind of data, enormous processing power and the ability to handle virtually limitless concurrent tasks or jobs"

Analysis

The Convergence of Technologies

The challenge of securing IoT devices is multiplied exponentially when considering data interoperability with respect to data and metadata being created, maintained, exchanged, and stored in many domains (IoT device, system, and system-of-systems).

As the IoT environment grows so does the need to track, monitor, and manage more devices and an ever larger volume of streaming data. It’s no coincidence that the emergence of cloud computing, big data technologies, next generation wireless technologies, and sophisticated analytical algorithms exist at a time when the IoT market is expected to explode in numbers. These technologies are ripe for meeting the demands of the IoT. Now, **massive amounts of data created by IoT devices can be stored, managed, and analyzed on flexible and scalable cloud computing platforms**.

Who will define this technological evolution? The Open Group helps firms take advantage of the convergence of cloud computing, social computing, mobile computing, big data analytics, and the Internet of Things. Their view is *“There is a recognized convergence of technologies by industry analysts and practitioners creating the opportunity for a new federated architecture model. Gartner identified this as a ‘Nexus of Forces’, while IDC is calling it the 3rd Platform. At The Open Group, we are referring to the convergence as Open Platform 3.0.”*

This convergence is **enabling the low-cost creation of virtual representations of devices in the cloud** which offers numerous benefits for engineering, operations, and security.

IoT - Timing Is Everything

Timing is inherent in all computing systems and accuracy is critical for system time and used by many applications, such as calendars. Security professionals rely on accurate timing for the synchronization of log file timestamps for Security Information and Event Management (SIEM). For the IoT, accurate timing is important at the device physical, analog, and cyber layers and throughout the System of Systems (SoS), including cloud computing. Moreover, secure time is critical for IoT systems as it affects control, the correlation of acquired data, and is instrumental in the pursuit of trustworthiness - cybersecurity, privacy, reliability, resilience, and most importantly, safety.

NIST recommends incorporating microprocessors with support for time in systems hardware. Network hardware, such as routers, should support clock synchronization. Increasingly, the cloud be a key part of IoT deployments, which requires mapping from local to global timescales. Complicating the issue is the fact that cloud computing virtualization may degrade timing performance, including use of Software Defined Networking (SDN) and Network Function Virtualization (NFV).

Finally, NIST advises a “time-aware IoT should guarantee bounds on latency of data delivery and guarantees on synchronization accuracy as it applies to timing correlation of physical I/O”.

IoT Shadow

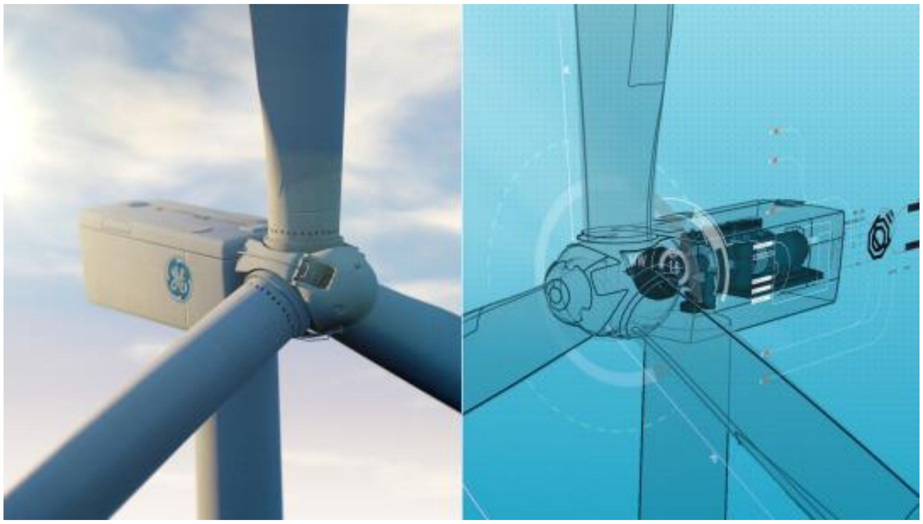
The concept of a digital twin was introduced in 2003 by Dr. Michael Greives in his whitepaper: "…a 'Digital Twin' as a virtual representation of what has been produced. Compare a Digital Twin to its engineering design to better understand what was produced versus what was designed, tightening the loop between design and execution."

John Vickers, NASA's leading manufacturing expert and manager of NASA's National Center for Advanced Manufacturing, provides a manufacturing perspective in The Economist.

"The ultimate vision for the digital twin is to create, test and build our equipment in a virtual environment. Only when we get it to where it performs to our requirements do we physically manufacture it. We then want that physical build to tie back to its digital twin through sensors so that the digital twin contains all the information that we could have by inspecting the physical build."

GE is on the forefront of building not only digital twins but "digital wind farms". Following is an excerpt from an article about their wind turbine digital twin:

Just like Apple's Siri and other machine learning technologies, the digital twin will keep crunching data coming from the wind farm and providing suggestions for making operations even more efficient, based on the software's insights. The data comes from dozens of sensors inside each turbine monitoring everything from the yaw of the nacelle, to the torque of the generator and the speed of the blade tips. The digital twin, which can optimize wind equipment of any make, not just GE's, gobbles it up and sends back tips for improving performance.



A GE wind turbine and its digital twin. Image credit: GE Power & Water

With analytics and machine learning the IoT shadow (digital twin) will be able to predict the life span for components and to schedule maintenance accordingly. Performance information can be compared across many devices to discover deviations and opportunities for improvements in design. Shadows could be used for training or cloned for testing with varying operating parameters for quality improvements. Clearly, **IoT shadows will become a key component in many IoT projects.**

Shadow Trustworthiness

The Internet of Things (IoT) shadow model is disrupting the design, development, maintenance, quality, and support of the devices they mirror. Next, IoT shadows will disrupt how we secure these devices as an integral part of the device lifecycle, incorporating the concept of security by design. The use of IoT shadows in the security domain is the foundation of The IoT Shadow Trust Framework (IoTSTF).

IoTSTF embodies the **concept of pursuing device trustworthiness through the analysis of IoT shadows and their associated data streams**. Analysis focuses on the following NIST trustworthiness risk properties:

Cybersecurity - Operational and Reputational Risk – Protect, detect, respond, and recover to ensure confidentiality, integrity, and availability of data for the System of Systems (SoS) and subsystems.

Privacy - Unwanted Disclosure Rates – Account for adverse impacts affecting disclosure of personal information.

Safety - Error Rates – Protect life, health, property, and data of stakeholders and the physical environment.

Reliability - Failure Rates – Detection, protection, and mitigation of device component failures (fault tolerance) in a predicted set of operational conditions.

Resilience - Recovery Rates – Ability of the device to withstand instability, unexpected conditions, and gracefully return to predictable, but possibly degraded, performance.

IoT shadows and the pursuit of trustworthiness should be integral parts of an IoT device lifecycle (design, development, implementation, operation, maintenance, and retirement). **Therefore, the pursuit of trustworthiness of an IoT shadow offers opportunities for new types of analysis and benefits.** One benefit is the ability to do analysis without the need for direct access to the device, which may impact its performance or operation. A second benefit is the fact that shadows are delivered via cloud computing platforms; therefore, new shadows can be created on demand to run through various scenarios for deeper analysis. A third benefit is the ability to run shadows with different versions of source code to discover behavioral changes or anomalies.

There are many potential techniques to assess IoT shadow trustworthiness. Following are two examples:

Shadow Behavior Anomaly Detection (SBAD) - A device shadow offers the opportunity to model and observe a device's behavior holistically, across its physical, analog, and cyber components. Machine learning algorithms will study the shadow's operation to infer normal patterns of behavior in order to detect anomalies which affect trustworthiness.

Data Lake Trustworthiness – Algorithms which mine the rich data lake, fed by continuous data streams from the physical and shadow devices, to discover issues which may affect the cybersecurity, privacy, reliability, resilience, and safety of the device.

Widely Accepted Standards

The IoT market holds great promise, but to be fully realized standards have to be widely accepted and implemented. There are established and emerging standards for securing IoT devices, promoted by various organizations. For example, The Trusted Computing Group (TCG) recommends the following fundamental security capabilities required for IoT use cases in their Guidance for Security IoT Using TCG Technology:

- Establishing and Protecting Device Identity
- Protection Against Malware Infection
- Protecting Against Hardware Tampering
- Maintaining Confidentiality, Integrity, and Availability of Data at Rest
- Reselling or Decommissioning a Device
- Meeting Cryptographic Protocol Requirements
- Supporting Multiple Models of Provisioning
- Maintaining Audit Logs
- Providing Remote Manageability
- Securing Legacy Hardware

Regardless of how risk is managed and how cybersecurity activities are tracked, there is a new standard emerging which is complementary to any risk management program. The *NIST Framework for Improving Critical Infrastructure Cybersecurity* is a risk-based approach to managing cybersecurity risk activities. It provides the opportunity for risk and cybersecurity professionals worldwide to strengthen and communicate the management of risk while aligning with industry best practices. While lacking in many respects, **over time it will become the universally accepted method of conveying an organization's cybersecurity posture**.

Profiles establish a roadmap for reducing cybersecurity risk and they align Functions, Categories, and Subcategories with the business requirements, risk tolerance, and resources of the organization. The framework is flexible and useful for comparing baseline and target profiles to identify gaps. The framework does not prescribe Profile templates, allowing organizations to be creative in their approaches.

Nevertheless, the **IoT demands a risk based approach that extends beyond cybersecurity to include risk properties for privacy, reliability, resilience, and safety**. Proper management of these risks provides the desired level of IoT trustworthiness. Categories and subcategories need to be reviewed and updated in this context to represent the **equivalence of a NIST Framework for Improving Trustworthiness**.

An IOT project could have profiles for each device and roll up all device profiles into a project level view, and finally, roll up all projects into an organizational level view. The profile can be customized, such as adding columns to show status.

The table below is an example of a partial profile for a hypothetical device at a given moment in time. It has been customized with additional columns and with color to aid in viewing current gaps and their priority to reduce them. Note that the size of a given gap does not dictate its priority (e.g., a large gap may have medium priority).

IoT Device Trustworthiness Profile (01-Jan-16)				
Function	Category	Subcategory	Gap	Priority
Identify	Governance (ID.GV) Policies, procedures, and processes to manage and monitor regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of trustworthiness risk.	ID.GV.1: Governance and risk management processes address trustworthiness risks.	Large	Medium
Protect	Data Security (PR.DS): Information and records (data) are managed consistent with risk strategy for trustworthiness.	PR.DS-1: Cybersecurity (and safety) for Data	Large	High
		PR.DS-2: Privacy for Data	Medium	High
	Awareness and Training (PR.AT): Personnel and partners are provided trustworthiness awareness education and training.	PR.AT-1: All users are informed and trained	Small	Low
Detect	Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood.	DE.AE-1: A baseline of device operations and expected data flows for the device, and corresponding shadow, is established and managed.	Medium	High
Respond	Response Planning (RS.RP): Response processes and procedures are executed and maintained to ensure timely response to detect trustworthiness events.	RS.RP-1: Response plan is executed during or after an event.	Medium	Medium
Recover	Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure timely restorations of systems or assets by trustworthiness events.	RC.RP-1: Recovery plan is executed during or after an event.	Large	Medium

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