ITL BULLETIN FOR SEPTEMBER 2016

DEMYSTIFYING THE INTERNET OF THINGS

Jeffrey Voas, Larry Feldman,[1] and Greg Witte,[1] Editors
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

Introduction

From agriculture, to manufacturing, to our homes, to healthcare, and beyond, technology is advancing towards 'smart' and 'smarter' systems. Generally speaking, 'smart' technology refers to numerous sensory devices working together through larger infrastructures. Rapid advances in computer science, software engineering, systems engineering, networking, sensing, communication, and artificial intelligence are not only evolving – they are also converging.

Historically, there has been little in the way of formal, analytic, or even descriptive information about the building blocks that govern the operation, trustworthiness, and life cycle of Internet of Things (IoT). A composability model and vocabulary that defines principles common to most, if not all networks of things, is needed to address the question: "What is the science, if any, underlying IoT?" NIST Special Publication (SP) 800-183, *Networks of 'Things,'* offers an underlying and foundational science to IoT that is based on a belief that IoT involves *sensing*, *computing*, *communication*, and *actuation.*

SP 800-183 uses two acronyms, IoT and NoT (Network of Things), extensively and interchangeably. The relationship between IoT and NoT is subtle—IoT is an instantiation of a NoT, whereby IoT has its 'things' tethered to the Internet. A different type of NoT could be a Local Area Network (LAN), with none of its 'things' connected to the Internet. Social media networks, sensor networks, and the Industrial Internet[2] are all variants of NoTs. This differentiation in terminology helps to separate use cases of varying vertical and quality domains (transportation, medical, financial, agricultural, safety-critical, security-critical, performance-critical, high assurance, to name a few). The distinctions are useful since there is no singular IoT, and it is meaningless to speak of comparing one IoT to another.

Primitives

System primitives allow formalisms, reasoning, simulations, and trade-offs to be formulated and argued. In SP 800-183, five core primitives belonging to most distributed systems are presented. These primitives are the basic building blocks for a NoT (including IoT) and are described as:

- ***Sensor*** **-** an electronic utility that measures physical properties such as temperature, acceleration, weight, sound, location, presence, identity, etc. All sensors employ mechanical, electrical chemical, optical, or other effects at an interface to a controlled process or open environment.

[1] Larry Feldman and Greg Witte are Guest Researchers from G2, Inc.
[2] Information about the Industrial Internet is available from: https://www.ge.com/digital/industrial-internet.

- ***Aggregator*** **-** a software implementation based on mathematical function(s) that transforms groups of *raw* data into *intermediate, aggregated* data. Raw data can come from any source. Aggregators help in managing 'big' data.

- ***Communication channel*** - a medium by which data is transmitted (e.g., physical via Universal Serial Bus [USB], wireless, wired, verbal, etc.).

- ***eUtility*** (external utility) **-** a software or hardware product or service, the current definition of which is deliberately broad to allow for unforeseen future services and products that will be incorporated in types of NoT yet to be defined.

- ***Decision trigger*** – a mechanism that creates the final result(s) needed to satisfy the purpose, specification, and requirements of a specific NoT.

SP 800-183 presents each primitive along with its definition, assumptions, properties, and role. The publication describes the relationship among these five primitives as: the sensor feeds data to the aggregator, which executes on various *e*Utilities of a NoT. This data is transmitted via communication channels that are the veins and arteries connecting sensors, aggregators, *e*Utility, with the decision trigger. Information can flow either unidirectionally or bidirectionally, depending on the purpose of the sensor application. Together, the sensor, aggregator, communication channel, eUtility, and decision trigger all have events firing at specific snapshot times and thus require synchronization as would any distributed system.

Sensors can be grouped in an abstract fashion called a *cluster* that can be created or decommissioned as needed. These sensors or clusters can also be *weighted*, such that a particular sensor or cluster's data can have varying impact on an aggregator's computation based on the predetermined values (e.g., worth of the particular sensor data, its uniqueness, or its relationship to mission goals). While this model may seem highly abstract, the model helps maintain simplicity and avoids over complicating IoT's small handful of building blocks.

Elements

Beyond the building blocks of the five primitives, SP 800-183 defines six elements that are key players in forming trust factors impacting NoTs. These elements, listed below, play a major role in fostering the degree of trustworthiness that a specific NoT can provide:

- **Environment -** the universe in which all the primitives of a specific NoT operate. The environment is essentially the *operational profile* of a NoT and is particularly important to the sensor and aggregator primitives since it offers them context. An analogy is the various weather profiles that an aircraft operates in, or a particular factory setting that a NoT operates in.

- **Cost -** the expenses, in terms of time and money, that a specific NoT incurs in terms of the non-mitigated reliability and security risks; additionally, the costs that are associated with each of the primitive components needed to build and operate a NoT. Cost is an estimation or prediction that can be approximated or measured, and helps drive design decisions in building a NoT.

- **Geographic location -** a physical place where a sensor or *e*Utility operates. For example, a system might use radio-frequency identification (RFID) technology to determine the physical location in which a 'thing' actually resides. Note that the operating location may change over time. A sensor's or *e*Utility's geographic location, along with communication channel reliability and data security, may affect timing

aspects of dataflow throughout a NoT's workflow. Specific geographic location may sometimes be difficult or impossible to determine.

- **Owner -** a person or organization that owns a particular sensor, aggregator, communication channel, eUtility, or decision trigger. There can be multiple owners for any of these five. Note that there is also a role for an **operator**; for simplicity, we roll up that role into the owner element.

- **Device_ID -** a unique identifier for a particular sensor, aggregator, communication channel, eUtility, or decision trigger, typically originating from the manufacturer. While the identifier is important, those relying upon the Device_ID for authentication should be aware that the identifier could be modified or forged.

- **Snapshot -** an instant in time, utilized for synchronization of events fired by any of the five primitives.

Additional Considerations

SP 800-183 Section 4 provides some additional considerations that build on the concepts of the primitives and elements described above. It explores the relationship between the safety and trustworthiness of a "closed" NoT (i.e., not intentionally interconnected with any elements outside of the network) as compared to one that is "open," or somewhere in between.

The publication looks at composability, considering a future demand for, and potential benefits of, design patterns that allow larger NoTs to be built from smaller NoTs. Notably, the document describes the ongoing need to explore issues of trust with NoTs (and especially IoTs, which bring additional connectedness).

The section also describes several considerations regarding testability challenges, given the huge number of potential permutations in a NoT, and the influence of factors from outside a network's native environmental boundaries.

Reliability and Security Primitive Scenarios

The elements lay out key contextual issues related to trustworthiness of a specific NoT. And, as mentioned before, the primitives are the building blocks of NoTs. Because trustworthiness is such a broad concept, SP 800-183 has mainly focused on two factors related to the five primitives: security and reliability. It provides examples of simple, hypothetical reliability and security scenarios associated with each primitive. These examples cover different NoT applications from modern cars, through smart building, smart city to wearables and others.

Conclusion

NIST SP 800-183 offers an underlying and foundational science for IoT-based technologies on the realization that IoT involves *sensing*, *computing*, *communication*, and *actuation*. It presents a common vocabulary to foster a better understanding of IoT and better communication between those parties discussing IoT.

NIST SP 800-183 presents five primitives and six elements that impact IoT trustworthiness. Primitives are the building blocks; elements are the less tangible *trust* factors impacting NoTs. Primitives also allow for analytics and formal arguments of IoT use case scenarios. Without an actionable and universally accepted definition for IoT, the model and vocabulary presented expresses how IoT, in the broad sense, *behaves*.

Use case scenarios employing the primitives provide quicker recommendations and guidance concerning a NoT's potential trustworthiness. Primitives and how they can be composed create a design vocabulary for how to apply existing technologies that support IoT trustworthiness.

ITL Bulletin Publisher: Elizabeth B. Lennon
Information Technology Laboratory
National Institute of Standards and Technology
elizabeth.lennon@nist.gov