De-Mystifying IoT

(*IoT Connection* column article for IEEE *Computer* Magazine)

J. Voas, *IEEE Fellow*

Introduction

What is the Internet of Things (IoT)? Is IoT the next technology re*volution*? Is it a technology *evolution*? Is it only an acronym? Is it definable, and if so, what is the definition? Claims about its potential impact reminded me of claims for previous "hot" technologies such as object-oriented programming, agile programming, design patterns, Y2K solutions, E-commerce, World Wide Web, etc.

Some of what spurs the need for answers, which are widely adoptable and acceptable, is: (1) IoT's predicted trillion dollar economic benefits[1], and (2) warnings of unprecedented security and privacy concerns[2]. However the economics and warnings offer little insight as to what IoT is - they merely suggest IoT's noteworthiness.

When there is a "definitional" vacuum for a new technology, suggestions for definitions arise. As evidence, here is a minimal sampling of new IoT definitions have surfaced since May 2015:

1. "***The term Internet of Things generally refers to scenarios where network connectivity and computing capability extends to objects, sensors and everyday items not normally considered computers, allowing these devices to generate, exchange and consume data with minimal human intervention."***

The Internet of Things (IoT): An Overview, Karen Rose, et.al. The Internet Society, October 2015. p. 5.

2. **"*Although there is no single definition for the Internet of Things, competing visions agree that it relates to the integration of the physical world with the virtual world – with any object having the potential to be connected to the Internet via short-range wireless technologies, such as radio frequency identification (RFID), near field communication (NFC), or wireless sensor networks (WSNs). This merging of the physical and virtual worlds is intended to increase instrumentation, tracking, and measurement of both natural and social processes."***

"Algorithmic Discrimination: Big Data Analytics and the Future of the Internet", Jenifer Winter. In: *The Future Internet: Alternative Visions*. Jenifer Winter and Ryota Ono, eds. Springer, December 2015. p. 127.

3. ***"Industrial Internet of Things (IOT) is a distributed network of smart sensors that enables precise control and monitoring of complex processes over arbitrary distances.***"

---

[1] "IDC expects the worldwide market for IoT solutions to grow at a 20% CAGR from $1.9 trillion in 2013 to $7.1 trillion in 2020" [4].

[2] "By 2020, addressing compromises in IoT security will have increased security costs to 20 percent of annual security budgets, from less than one percent in 2015". "By 2020, a black market exceeding $5 billion will exist to sell fake sensor and video data for enabling criminal activity and protecting personal privacy." [5]

"Ensuring trust and security in the industrial IoT", Bernardo A. Huberman. *Ubiquity: An ACM Publication*, January 2016, p. 1.

4. ***"The concept of Internet of Things (IOT) … is that every object in the Internet infrastructure is interconnected into a global dynamic expanding network."***

"An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment", Mohammad Sabzinejad Farasha, et.al. *Ad Hoc Networks* 36(1), January 2016. p. Abstract

5. "***In what's called the Internet of Things, sensors and actuators embedded in physical objects—from roadways to pacemakers—are linked through wired and wireless networks, often using the same Internet Protocol (IP) that connects the Internet."***

"The Internet of things", M. Chui, M. Löffler, and R. Roberts. McKinsey Quarterly, Sept. 23, 2015. As cited in: "Control Systems and the Internet of Things", Tariq Samad. *IEEE Control Systems Magazine*, 36(1), February 2016. p. 14.

6. ***"The Internet of Things (IoT) … refers to the trend to include networking and computing in a wide range of devices, such as watches, appliances, health monitors, toys, etc."***

"A Hands-On Introduction to the Internet of Things", Bill Siever and Michael P. Rogers. *Proceedings of the 47th ACM Technical Symposium on Computing Science Education (SIGCSE '16)*, February 2016. p. 715

7. ***"We must first define what we mean by 'things.' It could be very simple objects or complex objects. Things do not need to be connected directly to the public Internet, but they must be connectable via a network (which could be a LAN, PAN, body area network, etc.). The IoT is the network of physical objects that contain embedded technology to communicate and interact with the external environment. The IoT encompasses hardware (the 'things' themselves), embedded software (software running on, and enabling, the connected capabilities of the things), connectivity/communications services, and information services associated with the things (including services based on analysis of usage patterns and sensor or actuator data). An IoT solution is a product (or set of products) combined with a service either a one-to-one or a one-to-many relation. Meaning one service is combined with one (set of) product(s), or one service is combined with multiple (sets of) products."***

"Internet of Things in Energy Efficiency", Francois Jammes. *Ubiquity: An ACM Publication*, February 2016, p. 2

Common themes amongst these definitions include: "things", interconnected, Internet, cyber-physical, devices, sensors, smart, physical objects, virtual world, etc. But these definitions still do not define IoT well, or at least not at a foundational level. Therefore I started my research from the belief that IoT is fundamentally *communication*, *computation*, and *sensing*. The remainder of this article shows the reader where that thinking led me.

Primitives and Elements

To begin, I first broke communication, computation, and sensing into core distributed system components termed "primitives" [1]. I then defined a class of "elements" that allow for the foreshadowing of the *trustworthiness* of systems built from IoT components, services, and commercial products [1].

But before I explain the primitives and elements, I should mention one additional problem I saw. l was not satisfied with the acronym IoT, since it's not possible to compare one IoT to another. Therefore I needed a replacement, which became Network of Things (NoT). The relationship between NoT and IoT is subtle. IoT is an example of a NoT, more specifically, IoT has it's '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.[3] Social media networks, sensor networks, and the Industrial Internet (II) are all variants of NoTs. This differentiation in terminology provides ease in separating out use cases from varying vertical and quality domains (e.g., transportation, medical, financial, agricultural, safety-critical, security-critical, performance-critical, high assurance, to name a few). That is useful since there is no one, singular IoT. With this adjustment, I can then compare one NoT to another.

1. THE PRIMITIVES

Primitives are building blocks that offer the possibility of comparing NoTs. Primitives offer a unifying vocabulary that allows for composition and information exchange among differently purposed networks, i.e., NoTs. They offer clarity regarding more subtle concerns, including interoperability, composability, and continuously-binding assets that come and go on-the-fly. Because no simple, actionable, and universally-accepted definition for IoT exists, the model and vocabulary proposed here reveals underlying foundations of the IoT, i.e., they expose the ingredients that can express how the IoT behaves without defining IoT.

The *primitives* proposed in Draft NIST 8063 [1] are: 1) Sensor, 2) Aggregator, 3) Communication channel, 4) *e*Utility, and 5) Decision trigger:

1. A **sensor** is an electronic utility that digitally measures physical properties (e.g. temperature, acceleration, weight, sound, etc.) and outputs raw data.
2. An **aggregator** is a software implementation based on mathematical function(s) that transforms/consolidates groups of raw data into *intermediate* data.
3. A **communication channel** is a medium by which the data is transmitted (e.g., physical via USB, wireless, wired, verbal, etc.) between sensor, aggregator, communication channel, decision trigger, or *e*Utility.
4. A ***e*Utility** (external utility*)* is a software or hardware product or service, providing computing power that aggregators will likely not have.
5. A **decision trigger** creates the final result(s) needed to satisfy the purpose, specification, and requirements of a specific NoT.

In our 3-part model, **sensor** handles *sensing*, **communication channel** handles *communication*, and **aggregator**, ***e*Utility**, and **decision trigger** handle *computation*. Additionally, **aggregator** handles NoT issues associated with *big data* [2].

2. THE ELEMENTS

[3] A similar idea is discussed in [3].

To complete the model, Draft NIST 8063 [1] proposes six elements: *environment, cost*, *geographic location*, *owner*, and *Device_ID,* and *snapshot*. Although not primitives, these elements play a major role in fostering the degree of *trustworthiness* of a purposed NoT.

1. **Environment** – The universe that all primitives in a specific NoT operate in; this is essentially the *operational profile* of a NoT. Analogies are the various weather profiles in which an aircraft operates or a particular factory setting in which a NoT operates. Environment will likely be very difficult to define correctly.
2. **Cost** – The expenses (time and money) that a specific NoT incurs in terms of non-mitigated reliability and security risks; additionally, the costs associated with each of the primitive components needed to build a NoT. Cost is an estimation or prediction. Cost drives the design decisions in building a NoT.
3. **Geographic location –** Physical place where a sensor or *e*Utility operates or was manufactured. Manufacturing location is a supply chain trust issue. Note that the operating location may change over time. Note that a sensor's or *e*Utility's geographic location along with communication channel reliability may affect the timeliness of dataflow throughout the workflow. Geographic location determination may sometimes not be possible.
4. **Owner** - Person or Organization that owns a particular sensor, communication channel, aggregator, decision trigger, or *e*Utility. There can be multiple owners for any of these five primitives. Note that owners may have nefarious intentions that affect overall trust. Note further that owners may remain anonymous.
5. **Device_ID** – A unique identifier for a particular sensor, communication channel, aggregator, decision trigger, or *e*Utility. This will typically be created by the originator of the entity, but it could be modified or forged.
6. **Snapshot** -- an instant in *time*, utilized for synchronization of events fired by sensor, aggregator, communication channel, decision trigger, or *e*Utility.

Primitives, Reliability, and Security

To get a feeling for one simple reliability and security concern associated with each primitive, consider the following:

Sensor: *Reliability* – Failures and wrong inputs due to malfunctions caused by exposure in environmental conditions. For example, a speed sensor of a modern-sensor-equipped car gets exposed to heat and possibly water and dust. After years it starts providing inconsistent readings due to this naturally occurring corruption*; Security* - Physical tampering and altering firmware (if the sensor has such). For example, the temperature sensors (part of the temperature regulation system) of a smart-building are easily accessible. The chosen system does not provide technical means for validating the authenticity of the firmware. An ill motivated person substitutes the firmware with one that responds to remote commands. These sensors become part of a botnet and will contribute to DDoS attacks orchestrated by an attacker.

Aggregator*: Reliability* – Unpredicted conditions that will lead to undefined behavior thus wrong output. For example, in a smart city environment thousands of sensors are transmitting data to a series of smart gateways that effectively compress several GB of raw data into meaningful information. A blackout that occurred in part of the city creates an unexpected condition that results in division by zero. This causes the application to keep crashing for the entire duration of the blackout; *Security* - Injection attacks (e.g. Buffer overflows) that will lead to undefined behavior thus wrong output. For example, an attacker manages to introduce a rogue sensor on the network that produces fake readings. These readings are passed as inputs to the aggregator function without any validation. The attacker

launches a buffer overflow attack to gain root access to the entire middleware infrastructure (i.e., gateway).

Communication channel: *Reliability* – Loss of service due to overpopulation and connection of the medium. For example, sensors inside a smart building for regulating the intensity of the lights and temperature communicate wirelessly via IEEE 802.11 with the remainder of the system. During a conference, a large number of attendants are gathered inside a room having enabled wifi of their smartphones. Due to overpopulation of the channel frequent disconnections and degradation of the quality of service are noticed. The sensors are unable to provide readings with their predefined frequency; *Security* - eavesdropping of the communication channel. For example, the activity tracker is a wearable device attached to a person's wrist that measures the heart beats per minute and the blood pressure of a patient. It communicates via Bluetooth Low Energy with the bearer's smartphone and forwards these data to his physician. Despite the fact that BLE takes specific actions to randomize the MAC address of the devices the manufacturer neglected this feature. An attacker with a high-gain antenna can track the presence of the specific person within a crowd and create a movement profile.

***e*Utility**: *Reliability* – System failures that make the resource unavailable (system maintenance or hardware failure). For example, a PoS system that is conducting automatic smart payments depends on a cloud service for verifying the identity of the clients checking out and for charging their credit card. System maintenance of the server happens to occur on working hours which causes annoyance; *Security* - DoS so that it cannot provide input to the system (especially applicable in the cases where the *e*Utility is a service exposed to the network). For example, in the front door of a smart home a security camera is installed. The data of the camera is sent to a corresponding cloud application which forwards notifications along with video to the device of the user in case motion is detected. An attacker hires a hacking squad to conduct DDoS on the servers of the application provider for 2 hours. Then they break into the house without the user getting notified.

Decision trigger: *Reliability* – Defective code – For example, the logic implemented is **a or b** versus **a and b**; *Security* – Code tampering. For example, the software that implements the decision trigger accepts malicious inputs, or the outputs from the trigger are sniffed and released to competitors unbeknownst to the legitimate owner of the trigger.

Summary

This short column article has offered arguments against taking a "one size fits all" approach to defining IoT. Currently, IoT, as an acronym, is closer to a *marketing brand* or *catalogue* of services and products than it is to a singular, well-defined technology.

Acknowledgment

The author thanks Prof. Constantinos Kolias for suggestions on reliability failures and security attacks.

References

[1] J. Voas, "Primitives and Elements of Internet of Things (IoT) Trustworthiness, DRAFT NIST IR 8063, http://csrc.nist.gov/publications/PubsDrafts.html#NIST-IR-8063

[2] http://www.ecnmag.com/blog/2016/01/iots-special-gift-big-data

[3] http://techcrunch.com/2016/03/05/can-you-take-the-internet-out-of-the-internet-of-things/

[4] http://www.business.att.com/content/article/IoT-worldwide_regional_2014-2020-forecast.pdf

[5] http://www.gartner.com/newsroom/id/3185623