2013 5th International Conference on Cyber Conflict
K. Podins, J. Stinissen, M. Maybaum (Eds.)

Threat Implications of the Internet of Things

Michael J. Covington
Security Intelligence Operations
Cisco Systems, Inc.
San Francisco, California, USA
Michael.Covington@cisco.com

Rush Carskadden
Click Security
Austin, Texas, USA
Rush@clicksecurity.com

Abstract: There are currently more objects connected to the Internet than there are people in the world. This gap will continue to grow, as more objects gain the ability to directly interface with the Internet or become physical representations of data accessible via Internet systems. This trend toward greater independent object interaction in the Internet is collectively described as the Internet of Things (IoT).

As with previous global technology trends, such as widespread mobile adoption and datacentre consolidation, the changing operating environment associated with the Internet of Things represents considerable impact to the attack surface and threat environment of the Internet and Internet-connected systems.

The increase in Internet-connected systems and the accompanying, non-linear increase in Internet attack surface can be represented by several tiers of increased surface complexity. Users, or groups of users, are linked to a non-linear number of connected entities, which in turn are linked to a non-linear number of indirectly connected, trackable entities. At each tier of this model, the increasing population, complexity, heterogeneity, interoperability, mobility, and distribution of entities represents an expanding attack surface, measurable by additional channels, methods, and data items. Further, this expansion will necessarily increase the field of security stakeholders and introduce new manageability challenges.

This document provides a framework for measurement and analysis of the security implications inherent in an Internet that is dominated by non-user endpoints, content in the form of objects, and content that is generated by objects without direct user involvement.

Keywords: *Internet of Things, attack surface, threat evolution, security intelligence*

1. INTRODUCTION

There are currently more objects connected to the Internet than there are people in the world [1]. This gap will continue to grow, as more objects gain the ability to directly interface with the Internet or become physical representations of data accessible via Internet systems. This trend toward greater object interaction in the Internet is collectively described as the Internet of Things (IoT). As with previous global technology trends, such as widespread mobile adoption and datacentre consolidation, the changing information landscape associated with the Internet of Things represents considerable change to the attack surface and threat environment of the Internet and Internet-connected systems.

The precise definition of the Internet of Things is a subject of some debate, due to the influence of several contributing trends, as well as various interpretations of the phrase in everything from scientific research to marketing materials [2]. For purposes of attack surface and threat analysis, let us confine our discussion to two component trends within the larger IoT landscape, namely ubiquitous network-connected technologies, and object-embedded information produced and consumed by those pervasive technologies.

The past decade has seen staggering growth in the number of devices that humans use to directly produce and consume network information. As of 2010, there were over 12.5 billion such devices on the Internet, up from 500 million in 2003, and we estimate that there will be 50 billion by 2020 [1].

However, there are also an increasing number of technologies that do not require human interaction to produce and consume network information. In 2020, we estimate that there will be over a trillion such systems.

Further, the number of objects that do not directly connect to the Internet, yet contain embedded information, is also on the rise. Much focus in the context of the Internet of Things has been placed on RFID tags, of which over 15 billion have been produced [3]. However, objects may also contain embedded information in the form of barcodes (representing over 5 billion machine-object interactions per day [4]), serial numbers, and other forms of machine-consumable object symbology, which are present on the vast majority of objects involved in commerce.

The Internet of Things is defined as much by its interconnectivity as by its comprising entities. Early attempts at understanding the relationship between entities of the IoT were focused on their statistical relationships. Using this approach, one might project a world population of 7.6 billion in 2020, and each person matched up with 6 connected devices, over 130 sensors, and innumerable embedded information objects. Simple statistical relationships, however, do not

reflect the actual distribution of objects and technology, or the dynamic nature of the interactions between IoT entities. Usman Haque has suggested that we think of the IoT in terms of environments, as opposed to objects or sensors [5]. In order to assess the threat implications of the IoT, we will first discuss the relevant surface characteristics of these environments, and their dynamic nature. What systems and information are present in this environment at this time? What interactions are possible between them? Then, we will consider the agency of those characteristics in the frequency and effects of various cyber attacks.

2. RELEVANT SURFACE CHARACTERISTICS

Comprehensive enumeration of the Internet of Things' characteristics, even in comparison with previous eras of network evolution, is beyond the scope of this document. Rather, we seek to identify those characteristics most likely to have agency in cyber attacks.

Manadhata and Wing have provided an attack surface metric that is applicable to specific software systems, but when we apply it to dynamic networks, we must necessarily accept less granular definition [6]. It's not likely that we would be able to assess the attack surface of each entity comprising a specific environment in time (at the very least, we're unlikely to have access to all of the necessary source code). We can, however, abstract Manadhata and Wing's concepts of channels, methods, and data items (collectively, resources), and apply them, without weight, to generic IoT environments in comparison with previous network environments. Relevance is denoted by material change in the number of system resources. Admittedly, this would be a crude metric for measuring the absolute attack surface of a specific environment, but this approach allows us to assess the relevance of IoT surface characteristics in general terms.

A. *POPULATION*

The first concern associated with an IoT environment is the population of entities. As previously discussed, the population of entities is expected to grow rapidly, as users embrace more connected devices, more sensors are deployed, and more objects are embedded with information. Each entity, depending on its type, carries with it an associated set of channels, methods, and data items, each of which is subject to potential abuse. This increased population has the effect of creating an explosion in the total number of potential target resources across the Internet, as well as within any specific environment.

B. COMPLEXITY AND COST

Each new entity can be classified into one of three tiers, defined by its characteristics, see Table I. Each tier inherits the characteristics of the lower tiers.

Table I. Classification Tiers

Tier	2020 Population	Examples	Characteristics
3	50 billion	Desktop, Laptop, Smartphone	Entity has channel(s) and method(s) for interaction with users
2	1 trillion	Sensor, Controller	Entity has channel(s) and method(s) for interaction with other entities
			Entity has channel(s) and method(s) for interacting with its environment
1	No estimate	Barcode, RFID	Entity contains data item(s) that may be consumed by other entities via an automated method
			Entity has a unique identity

These tiers represent the level of complexity inherent in the entities, as defined by their resources. As this table indicates, the anticipated population of entities is greatly skewed towards lower complexity entities. In the context of attack surface analysis, entities with a comparatively low complexity also have a comparatively small attack surface. There simply aren't that many channels, methods, and data items to consider for each entity, which is good for any specific low-complexity entity. However, when you take into consideration the massive population of tier 1 and 2 entities, the aggregate number of attack vectors is still daunting. Even a single attack vector for each tier two system, compared with 14 attack vectors for a tier 3 Linux system (based on Manadhata and Wing's estimate), still results in tier 2 systems presenting over 42% more attack vectors in aggregate than tier 3 systems.

Population and complexity also imply cost, and hence available compute and storage resources, as well as quality of components and materials. As we will later see, the balancing act between cost and resources has an important impact on the resources available for system security, encryption methods, key size and distribution, and software updates.

C. HETEROGENEITY AND INTEROPERABILITY

The number of distinct tier 3 system types has been increasing as a result of their pervasiveness, but the explosion of tier 1 and 2 entities also represents increased heterogeneity across the Internet of Things. However, heterogeneity may not hold true within a specific environment. A dam that is embedded with a network of

sensors to measure its integrity would be a fairly homogenous environment. So, though a dramatic increase of tier 1 and 2 entities increases the heterogeneity of the IoT in aggregate, specific environments may still be highly homogenous.

Given this anticipated heterogeneity across the IoT, we are due some further consideration of interoperability between entities within an environment, and across the IoT at large. While some have advocated the need for, and made some early progress towards, universal interoperability and open standards in the IoT, the extent to which it's possible is largely dependent on how – and how rapidly – the IoT evolves [7]. The National Intelligence Council (NIC) outlines four possible scenarios for this evolution: Fast Burn, Slowly But Surely, Connected Niches, and Ambient Interaction [8]. Of all of the scenarios, Slowly But Surely, which predicts pervasiveness in 2035, is the only scenario that permits universal interoperability. However, our projections for entity population growth and the vertical nature of extant stakeholders are much more indicative of the Connected Niches scenario, in which interoperability is challenged by reluctance of industries to cooperate. Interoperability struggles present a challenge to accountability and manageability. As the number of system stakeholders increases, accountability for preventing, identifying, and resolving security issues will be more distributed. Similarly, the channels and methods for interaction will grow more voluminous and complex.

D. MOBILITY AND DISTRIBUTION

The increase in mobile tier 3 entities, such as laptops and mobile phones, coupled with the increase in tier 1 and 2 entities, will result in more dynamic operating environments. Systems and data items will shift rapidly between environments. This exacerbates the challenges of establishing appropriate access control, monitoring, and automated decision-making within limited domains of visibility and control. However, mobile entities that do not maintain connectivity to the broader Internet will have a smaller window of compromise in any one environment.

One of the chief advantages of the Internet of Things is that you can deploy systems and information where people are not. The utility of such sensors, along with mobility, will cause the population of IoT entities to be more broadly distributed in physical space than previous networks. As we continue to drive down the relative cost and complexity of entities, we will see a related increase in population in previously sparse geographies.

3. CYBER ATTACK IMPLICATIONS

Changes to the operating landscape affected by the Internet of Things will necessarily result in changes to the nature of cyber attacks. The weapon actions that comprise a cyber attack are defined by their objectives [9]. Applegate provides a useful perspective on these objectives by defining cyber maneuvers as "the application of force to capture, disrupt, deny, degrade, destroy, or manipulate computing and information resources" [10]. Privilege escalation, for instance, is defined by the objective of capturing positional advantage. By loosely grouping the objectives of cyber maneuver, we can establish a structure in which we can assess the threat implications of the IoT.

A. CAPTURE

Capture attacks take two primary forms, depending on the targeted resources. Some capture attacks are designed to gain control of physical or logical systems, while others are designed to gain access to information. Attempts to capture systems are intended to gain a positional advantage that can be leveraged in subsequent operations. Attempts to capture information are intended to gain an exploitative intelligence advantage [10].

1. Systems

Systems composing the Internet of Things are uniquely susceptible to capture, due to a number of their characteristics. Their ubiquity and physical distribution afford attackers with greater opportunity to gain physical or logical proximity to targets.

Increased mobility and interoperability amplify the threat to IoT systems, in that they complicate access control by enabling an attacker to introduce compromised systems into the environment or remove systems in order to compromise and reintroduce them without detection. They also provide opportunity for attackers with a foothold in the environment to compromise transient systems in order to spread compromise to other environments. However, mobility may also dampen the threat by narrowing the window of opportunity to attack transient systems.

The heterogeneity of IoT systems is another factor in capture. Heterogeneity can complicate update and patch procedures to the point of increasing the window of vulnerability to a specific attack, but it may also limit threat propagation by requiring different weapon actions to successfully capture different systems, provided the vulnerability isn't found in the common channels and methods of interoperability.

2. Information

Information in the Internet of Things is widely distributed throughout component systems, so that any successful capture of a system will likely result in capture of information to which that system has access. Wide distribution of systems may also necessitate a longer chain and / or a denser mesh of communications, affording attackers greater opportunity to intercept or intercede in information transmission within the environment.

System resource limitations, particularly in tier 2 entities, may limit systems' access to robust encryption, while necessitating frequent, small bursts of information in a standard format. The expected asymmetry between a tier 2 system's encryption resources and the resources of, for instance, an attacker with a multi-core analysis system, aids in the attackers ability to capture information. Further, the frequency of these transmissions affords greater opportunity, and the standard format may aid in cryptanalysis. However, small burst size, combined with frequent key exchange, limits the amount of information that an attacker can capture with a given solution.

B. DISRUPT, DEGRADE, DENY, DESTROY

Disrupt, degrade, deny, and destroy attacks (hereinafter collectively referred to as disrupt attacks) differ from capture attacks, in that they are intended to confer a competitive disadvantage on the target, as opposed to conferring an advantage upon the attacker. When considering the threat of disruption, we must evaluate attacker opportunity, as well as target resistance, resiliency, and assurance.

Attackers seeking to disrupt systems in the Internet of Things share the opportunity advantages of system capture attackers, in that opportunity to capture a system also affords attackers the opportunity to disrupt it. However, disrupt attacks against information are slightly different, as opportunity to capture information does not imply opportunity to disrupt it, unless the attacker has captured either a single point of failure, or all requisite points of failure, for information storage and / or transmission.

The relative low cost and complexity of tier 1 and 2 entities in the IoT are directly related to the entities' resistance to disruption. Unless they exist within a hardened environment, we may assume that these entities are susceptible to physical abuse and tampering. If they are mobile entities, they are also susceptible to displacement.

The combination of heterogeneity and interoperability in IoT entities is key to resiliency. Heterogeneity is generally assumed to result in higher survivability for the network as a whole [11]. In the event of disruption of one entity in the environment,

other entities may resist the attack, and be able to continue functioning. Provided that the participating entities are interconnected and able to route information using a standard set of protocols, the network gains greater transmission resiliency, as well. However, given the current Connected Niches mode of IoT evolution, it's unlikely that we'll have our cake and eat it too, with regards to heterogeneity and interoperability within any specific environment.

Assurance is the environment operators' ability to determine that a disruption has occurred and then perform incident management. The challenge is to verify confidentiality, integrity, and availability of all systems and data within the environment. Assurance in the IoT is significantly complicated by entity mobility and the number of stakeholders implied by interoperability challenges.

C. *MANIPULATE*

Manipulate attacks, as distinct from capture and disrupt attacks, are intended to influence opponents' decision cycles [10]. Using Boyd's OODA loop construct as a reference for general decision cycles, we can determine several different forms of manipulate attack within the context of the Internet of Things [12].

At the earliest point in the cycle, an attacker may manipulate the outside information itself. This involves intercession at the entry point in the information collection process, usually via physical means. Outside information manipulation may be something as simple as local environmental manipulation (e.g., heating the environment around a temperature sensor) and analog data manipulation (e.g., modifying a document prior to OCR), or it may be as complex as World War II's Operation Fortitude. Similarly, manipulate attacks may involve manipulating embedded data, whether by physically replacing or modifying tagging information, or infecting a portable data store, as in the events that lead to Operation Buckshot Yankee.

Further into the decision cycle, an attacker may directly manipulate sensors that gather information. As opposed to feeding a sensor manipulated information from its environment, the attack would, in this case, use a compromised sensor manipulate information available to other entities. This same approach applies to manipulation of controllers to change their actions, so that sensors observing the results of the controllers' actions would receive information that is not reflective of an undisturbed closed loop.

The last common form of manipulate attack is manipulation of the feed-forward mechanisms in the decision cycle, through employment of a man-in-the-middle or spoof attack. In this case, the attacker intercedes in the communications between entities, in order to exert control over information transmission.

It's clear that, as with the other types of attacks we've considered, the large population of entities in the IoT presents opportunity for a manipulate attacker, but this is even truer when we consider potential communications interoperability. Due to the network effect, each additional interoperable entity that is added to the network greatly increases the possible intercommunications, and affords greater opportunity for a man-in-the-middle attack. Mobility and distribution in the IoT also increase opportunity for attack, as they make it easier to manipulate entities without fear of detection. Manipulate attacks also present the same assurance challenges that disrupt attacks do, and in that sense, mobility and number of stakeholders also apply here.

4. PRIVACY CONCERNS IN THE INTERNET OF THINGS

The smart, connected objects that will densely populate the Internet of Things will interact with both humans and the human environment by providing, processing, and delivering all sorts of information or commands. These connected things will be able to communicate information about individuals and objects, their state, and their surroundings, and can be used remotely. All of this connectivity carries with it a risk to privacy and information leakage.

A significant body of work has explored privacy issues in ubiquitous computing systems and much of that research is applicable to the Internet of Things. Establishing meaningful identity, using trusted communication paths, and protecting contextual information is all very important to ensure the protection of user privacy in this environment. We will touch briefly on each of these issues as part of the exploration of threats within the Internet of Things.

Beresford and Stajano [13] have explored anonymous communication techniques and the use of pseudonyms to protect user privacy while also working on metrics to assess user anonymity. Their work takes a novel approach by hiding identity from the applications that utilize it in order to better protect the user consuming those services.

In their work on Decentralized Trust Management, Zhao et al [14] propose new technologies that enable the bootstrapping of trust, and subsequently, the calculation of trust metrics that are better suited to mobile, ad-hoc networks. In their model, every member of a community (users, devices, sensors, etc.) can serve as an authority to enroll and authenticate other entities for the community. Their model showcases the inherent problems with establishing trust in ad-hoc networks like those in the IoT where new sensors, services, and users are constantly introduced and asked to share data.

Finally, applications in the IoT, which will be enabled by a ubiquitous computing and communications infrastructure, will provide unobtrusive access to important contextual information as it pertains to users and their environment. Clearly, the successful deployment of such applications will depend on our ability to secure them and the contextual data that they share.

One example of sensitive contextual information is location. When location-aware systems track users automatically, an enormous amount of potentially sensitive information is generated and made available. Privacy of location information is about both controlling access to the information and providing the appropriate level of granularity to individual requestors. The Location Services Handbook [15] explores a variety of location-sensing technologies for cellular networks and the coverage quality and privacy protections that come with each.

5. CONCLUSIONS

The Internet of Things continues to march forward apace, and will accelerate over the coming years. We will see the Internet change in many important ways, and in the context of threat analysis, we will need to continue to explore the impact of these changes on the attack surface of the Internet as a whole, as well as specific environments.

Growth in network-capable and consumable entities is the largest potential concern with regards to potential attack surface, as we anticipate an explosive increase in both the breadth and density of the global information environment. Many of these new entities will be fairly unsophisticated in comparison to today's network-connected devices, as increased deployment of tier 1 and 2 devices outpaces miniaturization and cost reduction trends, resulting in entities with constrained security resources. They will be quite diverse in their designs and functions, and it's unlikely that they will broadly interoperate, creating some considerable monitoring and management challenges. They will be increasingly mobile and distributed, meaning that many contemporary security processes and tools that rely on information density will need to change considerably.

Attackers will find that the characteristics of the IoT in general embody an accelerating shift from the relatively controlled technology world that they know today to a world of increasing opportunities. Attackers seeking to capture systems and information will find a broad spectrum of targets from which to choose, and when their objectives require capture of any system, as opposed to a specific system, in an environment, they will likely have a broader set of tools to achieve their goals. Attackers seeking to disrupt IoT systems and environments will likewise

identify new opportunities and approaches to achieve their ends, with their only new concern being potential confluence of heterogeneity and interoperability – an unlikely result. Perhaps the greatest opportunity will be for attackers seeking to manipulate IoT entities, as they take advantage of a broad, dynamic network with exponential channels of communication.

The Internet of Things will bring many great new advances, including whole new ways of thinking about and interacting with our world. However, with those opportunities come many challenges in the world of information security, and we will need to continue to research and develop new approaches to ensuring our safety, security, and privacy.

REFERENCES

[1] Evans, Dave. «The Internet of Things How the Next Evolution of the Internet Is Changing Everything.» *CISCO white paper* (2011).

[2] Uckelmann, Dieter, Mark Harrison, and Florian Michahelles. «An architectural approach towards the future internet of things.» *Architecting the Internet of Things* (2011): 1-24.

[3] Harrop, P., and Raghu Das. «RFID Forecasts, Players and Opportunities 2012-2022.» *IDTechEx, Cambridge, UK* (2012).

[4] Varchaver, Nicholas. «Scanning the globe.» *Fortune Magazine, available at: http:// money. cnn. com/magazines/fortune/fortune_archive/2004-05/31/370719/index. htm* (2004).

[5] Tish Shute, *Pachube, Patching the Planet: Interview with Usman Haque*.: UgoTrade, 2009.

[6] Manadhata, Pratyusa K., and Jeannette M. Wing. «An attack surface metric.» *Software Engineering, IEEE Transactions on* 37.3 (2011): 371-386.

[7] INFSO EU, *Internet of Things in 2020: Roadmap for the Future*.: INFSO EU, 2008.

[8] National Intelligence Council (NIC), *Disruptive Civil Technologies: Six Technologies With Potential Impacts on US Interests Out to 2025*., Official US Government Document, Accession Number ADA519715 (2008).

[9] Cartwright, General James W. «Joint Terminology for Cyberspace Operations.» *Joint Chiefs of Staff (JCS) Memorandum, Nov* (2010).

[10] Scott D. Applegate, «The Principle of Maneuver in Cyber Operations,» in *2012 4th International Conference on Cyber Conflict*, vol. 4, Talinn, Estonia, 2012, p. 13.

[11] Zhang, Yongguang, Harrick Vin, Lorenzo Alvisi, Wenke Lee, and Son K. Dao, «Heterogeneous Networking: A New Survivability Paradigm.» *Proceedings of the 2001 workshop on New security paradigms*. ACM, 2001.

[12] Boyd, John R. «The essence of winning and losing.» *Unpublished lecture notes* (1996).

[13] Beresford, Alastair R., and Frank Stajano. «Location privacy in pervasive computing.» *Pervasive Computing, IEEE* 2.1 (2003): 46-55.

[14] Meiyuan Zhao, Hong Li, Rita Wouhaybi, Jesse Walker, Vic Lortz, and Michael J. Covington. Decentralized trust management for securing community networks. Intel Technology Journal, 13(2):148-169, 2009. Invited Article.

[15] Eladio Martin, Ling Liu, Michael Covington, Peter Pesti, and Matt Weber. Chapter 1: Positioning technology in location-based services. In Syed A. Ahson and Mohammad Ilyas, editors, Location Based Services Handbook: Applications, Technologies, and Security. CRC Press, July 2010.