ABSTRACT

With the increasing popularity of Internet of Things, the security and privacy issues are of significant concern to users and vendors alike. Although there have been significant progress in the development of technical solutions, the aspect of risk propagation is largely ignored. In this study, we resort to existing literature in network topology, outsourcing, and supply chain management to address the managerial and inter-organizational issues of IoT security. The theories and their applications to IoT as well as their implications are presented and discussed.

KEYWORDS: Internet of Things, information security, supply chain, scale-free networks, outsourcing

INTRODUCTION

Internet of Things is the network of physical objects accessed through the Internet, or the interconnections between all manners of devices with an addressable interface that can communicate online. IoT literally covers almost everything around us: there are Internet of Home, Health, Fashion, Traffic, Environment, Logistics, Design, Manufacturing, and so on. Although a lot is expected in the future, many are already available; commonly cited examples of IoT devices range from Nest thermostat to refrigerators with Internet connections to wearables such as FitBit to driverless cars.

Optimistic forecasts for IoT abound. Gartner projected there will be 4.5 billion connected devices by 2015 and 25 billion by 2020. It is estimated that IoT products and services will generate $300 billion in 2020 and add $14.2 trillion by 2030 to world economy when industrial IoT is included. Hype aside, the importance and potential of IoT are well recognized by industry players, as evidenced by the large commitment made by major IT companies such as Cisco, IBM, and even SAP.

But with the development of IoT come risks, chief among which are the concerns for security and privacy. Without strong security protection for all the devices and the data that they
collected and transported, it is likely that the development of IoT may be bogged down by strong resistance and endless litigation. Indeed there are early warning signs. Worms targeting small IoT devices such as Linux.Darlloz and Linux.Aidra have been discovered. In 2014, HP tested 10 popular IoT devices and found that 70% of them contained security vulnerabilities (at an average of 25 holes each). Such vulnerabilities and the exceptional opportunities for data collection through smart devices such as camera, smart TV, medical sensors, and so on pose significant threat not only to the specific IoT users but also to the majority in the society due to the connected nature of the world that we live in today.

There have been a lot of work in this area, most notably those by several industry consortiums. The focus has been on securing individual devices, or the “things” of IoT. But because all the devices are networked, by bypassing the authentication of a weak “smart” device such as an Internet-connected door lock, it is possible to harm thousands other households at once. When one device is under security threat, will other devices be affected? What is the extent of data breach due to a security gap of one node? Can the servers and even whole network be affected? These are all critical questions for securing IoT. In this study, we intend to address them in the viewpoint of risk propagation a network of heterogeneous devices and, borrowing from existing literatures in networking theory, supply chain management, and IT outsourcing. The intention is to provide organizational and management perspective to the issue of IoT security.

CURRENT STATE OF INTERNET OF THINGS SECURITY

Securing Internet of Things is hard. It is so because the number of opportunities available to attackers is numerous, with increasing number of devices and even faster increase of connections. In addition, there are staggering number of threats that can affect IoT, such as physical threats, spoofing, virus, DoS, etc. And the inherent complexity of IoT—heterogeneous entities located in multiple locations managed by various providers exchanging different data and information—complicates the design and deployment of security measures. So to ensure the security of such a complex web of devices, with differentiated technologies, at many locations, and running a plethora of applications, areas such as access control at the node level, communication standards among all devices, protocols for sharing and transporting data, and enforcing the security and privacy policies are just a few requirements that need to be considered.

While all these areas are advancing at various speeds in academia and industry, the majority of the current activities appear to be focused on the following three areas. First, most, if not all, IoT vendors have taken secure access control to heart when they design and produce their “things.” A framework for classifying devices based on their input or output interaction with the network helps developers identify the security and/or privacy requirements for their devices (Rutledge et al., 2014). Secondly, a number of security software vendors are also developing third-party solutions that can be embedded in a variety of devices. To assist the implementation of security measures at the node level, detailed operation procedures and protocols have been developed. For instance, a phased product lifecycle approach (Jambunathan, 2015) and a well-defined security architecture (Farooq, 2015) have been proposed for the integration of security mechanisms into all IoT devices. And guidelines have been developed for the field design and implementation of IoT (Whitehouse, 2014).
The third area of focus is the standards for authentication, access control, and secured routing of data among all devices. To this end, there are dozens of standard-setting bodies and consortiums hard at work, including the IEEE, the Industrial Internet Consortium (IIC), the Open Interconnect Consortium (OIC), AllJoyn/AllSeen Alliance, Thread, and Fast Identity Online alliance (FIDO), just to name a few. They all have specific targets: for instance, OIC has the “goal of defining the connectivity requirements and ensuring interoperability of the billions of devices that will make up the emerging Internet of Things,” while FIDO offers a variation of public key infrastructure (PKI) that authenticates users and devices. In the future, all these standards have to be reconciled to ensure their interworking and compatibility.

But information security in IoT goes beyond technical solutions to the problems of device authentication and secured networking. When billions of devices are connected with one another, all security issues are interconnected. In a vast network of IoT with heterogeneous devices and connections, many nodes may be affected when even one node is breached. In some extreme cases, the integrity of the whole network may be impacted. To address the interconnected nature of security and privacy, one needs to understand the trust, governance, and enforcement of information security in IoT (Roman et al., 2013; Sicar et al., 2015; Weber, 2010). Such issues involve interactions and coordination among IoT vendors, users, and devices themselves not just technically but also managerially and organizationally, and there is a void in literature when it comes to the management of security across IoT. In the next section, we examine how risk propagates throughout the network and attempt to apply existing theories from multiple disciplines to the issue of interconnected information security in IoT.

MANAGING RISK PROPAGATION IN INTERNET OF THINGS

Risks propagate through interconnections. For instance, a virus can spreads from one IoT device to many others when they are all interconnected, and, as such, vulnerability in one device can be exploited to access the rest of the network. The characteristics of how IoT devices connect and interact with one another determine the spread of security threats and vulnerabilities. But the technical networking view is not sufficient to paint the whole picture of risk propagation; operational and financial risks can cascade throughout the network in any information security event. For example, when a wearable device such as heart rate monitor or even a pacemaker is breached, the monitoring hospital, device manufacturer, and even a health app vendor can be affected due to operational errors or liability. So to address the interconnected nature of information security in IoT, it is important to examine how risks propagate throughout not only the physical network but also the business interconnections among individuals and organizations.

Despite the dearth of literature in the area of risk propagation and management in the context of IoT, we find that concepts and theories from other disciplines offer rich insights. In particular, we propose that the literature in network topology, supply chain, and outsourcing are particularly applicable in the case of IoT security. We discuss each in the following sections.

IoT Security: Network Topology Perspective

For IoT to work, many devices and servers have to share data and exchange information, mostly on a real-time basis. As such, the security of any node—which can be a stationary device, a mobile device, a server, or a router—in the network of IoT depends not only on its own security measures and management but also on the rest of the network. Key factors to consider
can include the network resiliency, risk propagation patterns, and so on, and they can be significantly affected by the topology of the network.

When devices are attached to one another, a network is formed, and it grows when new devices are added. When constructing and growing a network, the simplest and most intuitive model is the random graph, proposed by Paul Erdos and Alfred Renyi in 1959. They posit that when a new node is to connect to the existing network, it is equally likely to connect to any existing nodes in the network. Because of the random nature of connections, Erdos-Renyi network exhibits a bell-shape distribution of the number of links each node possesses; as a result, “hubs”—those nodes directly connected to a great number of other nodes—are exponentially rare. Despite the simplicity of such a network construction, it turns out to be a poor model for most existing networks. In 1998, Albert, Jeong, and Barabasi discovered that the structure of the World Wide Web is not random. Rather, more than 80 percent of the pages have fewer than four links, while less than 0.01 percent of the nodes have more than 1,000 connections (Albert et al., 1999). Such a node-and-hub structure is the direct result of “preferential attachment,” where new nodes coming to the network tend to seek out to link to those existing nodes that have the largest number of links. Subsequently, such “scale-free network” topology is found in a wide variety of real-world systems, ranging from the Internet, telephone graphs, and the power grid, to the network of citation and collaborations in mathematics, to protein interaction and human sexual contacts. In the case of IoT, the majority of the devices (nodes) connect to only one or a small number of servers or processing centers that collect, process, and manage data and activities, while those servers or processing centers (hubs) have direct connections to a large number of nodes. Moreover, when a new device is added, it is likely to connect to those hubs instead of to other random nodes. As such, it is reasonable to expect IoT to resemble a scale-free network, and it is important to examine the information security implication of such a topology.

A scale-free network as a whole demonstrates high degree of tolerance against random failure of its nodes, a property that is not shared by randomly interconnected networks. That is, if a number of devices are down due to security attacks, the IoT as a system can still function as normal. This is due to the fact that random elimination of several nodes—more than likely to have small number of links—does not alter such a node-and-hub topology. However, if only a small number (or even one or two) of hubs are taken down, the whole network cannot survive as it quickly collapses into isolated fragments (Barabasi and Albert, 1999). As a real-world example, the Internet traffic in the U.S. had a stunning 40% drop when Google.com went down for about four minutes close to midnight on August 16, 2013! In other words, IoT as a scale-free network is robust against random attacks but is highly susceptible to targeted attacks against its hubs. Therefore, an informed adversary who attempts to damage the IoT network would not direct his/her attacks randomly; instead, the attacker can target the hubs—given the fact that the connectivity of nodes is very hard to hide—with a real likelihood of bringing down the whole system with a just few successful targeted attacks. To avoid such a large-scale disruption of IoT due to cyber attacks, it is critical for those highly connected hubs to be held to a higher security standard and be significantly more protected than other devices.

A scale-free network such as IoT also exhibits interesting behaviors with respect to the spread of security attacks. When studying the traditional Erdos-Renyi network under threat, researchers found the existence of an “epidemic threshold,” below which the attacks would not spread throughout the network, even when defensive mechanism is absent. Therefore, other than those highly “contagious” attacks, it is expected that most security events will stay localized in such a random network. However, in a scale-free network, the epidemic threshold is zero;
the reason is that since all nodes are connected to hub(s), an attack can immediately propagate
to a hub and consequently to the rest of the network. Therefore, even an attack with low
capability of spreading on one sparsely connected node—say, a badly designed worm that does
not replicate itself very effectively—can infect many node in IoT, as long as it propagates to and
infects a hub. This property has a significant implication for the security of IoT: To prevent even
the most rudimentary attack from spreading through the whole network, all IoT devices need to
maintain certain (minimal) level of information security. That is, no device should be allowed to
connect to the network unless its robustness is “certified,” because one weak node can cause
the whole network to be infected. Such a minimum security standard may be difficult to
establish and enforce, but it is necessary to uphold the resiliency of the whole IoT.

**IoT Security: Outsourcing Perspective**

In IoT, each device is connected to a server and/or multiple other devices. The security of one
device therefore depends on not only its own but also those that it connects to. In other words,
the security of one node is influenced by, or “outsourced to,” the security measures of the others
that it connects to. This setting is not unlike IT outsourcing, with the added complexity that (1) in
IoT, each node can be a client and a vendor at the same time, (2) the relationships among
nodes are often distributed, dynamic, and multilayered, and (3) the negotiations and
agreements of the equivalent of “outsourcing arrangement” are, for the most part, indirect and
implicit. This realization allows us to turn to the rich literature in IT outsourcing to again insight
into IoT security.

Devices and hubs in an IoT can generate and collect large amounts of data from disparate
locations run by diverse organizations located in virtually anywhere and then autonomously flow
the data between other devices. The theory of transaction cost economics (TCE) suggests that
opportunistic behavior of organizational participants can be a prominent factor that threatens the
security of IoT. Such opportunistic security behaviors can include failing to fulfill standard
security conducts, poor security compliance, and inappropriate allocation of resources and
skills. Although all parties in the IoT understand the need to maintain certain security
requirements when it comes to interconnections with other nodes, most are not willing to
allocate more resources than is absolutely needed for maintaining its own security as long as
there is penalty involved. In a recent case where New York Time’s website experienced a 20-
hour disruption, Syrian hackers used the New York Times’ outsourced hosting service company
in Melbourne IT as the weak spot for the attack (Brustein 2013). So from the outsourcing
perspective, key security challenges with IoT may arise from coordinating and managing
relationships between involved parties, coping with lack of security awareness, and auditing the
performance (Thalmann et al., 2012). In other words, effective interorganizational governance
relationships should be developed to curb such opportunistic exchange hazards (Williamson,

The first step to such a governance structure is a service level agreement (SLA) that provides
formal policy and agreement to place credibly enforceable limits on the actions of each
participant. This provides basic, minimum requirements to foster cross-organization data
exchange while establishing baseline privacy and security protections for organizations
engaged in exchanging data. However, the SLAs that one finds in a typical outsourcing
relationships may not be as effective in complex arrangements such as IoT. SLAs are most
effective between parties (“vendors” and “clients”) with contractual agreements; indirect (or
“subcontract”) relationships that are common in IoT do not allow SLAs to be easily enforceable
or audited. Thus, contractual governance, while necessary, may not suffice to ensure security and compliance in the IoT environment.

Both relational contract (Macaulay, 1963) and social exchange (Scanzoni, 1979) theories suggest that the use of social mechanisms can play a key role to complement formal contracts (Poppo and Zenger 2002). However, one may find that relational governance such as trust and commitment is difficult in IoT due to characteristics such as the large number of parties involved, the network-like structure of the arrangements, and the lack of direct bilateral contact. One plausible approach is to build through institutional trust (Gefen et al. 2006; Goo and Huang 2008; Goo et al. 2009; Zucker 1986), which starts with a common set of trust expectations codified into an enforceable legal framework that all IoT participants agree. For example, to nurture institutional trust in the IoT, all device vendors and owners can agree that each node has an identity in the network which can be monitored by other nodes. By specifying the parameters—physical proximity, fulfillment, consistency of answer, hierarchy on the trusted chain, common goals and warrants, history of interaction, availability, and so on—to be available to all other nodes at all times, a trust chain can be established among users. From there, it is then possible to develop a comprehensive, robust trust framework based on agreements with devices, owner of devices, and users that ensure common data privacy and security standards are followed across the IoT. This collaborative approach ensures that the agreement reflects a broad consensus across a range of stakeholders that may have very different agendas and priorities, strengthens trust across participants, and works to minimize, if not eliminate, the need for point-to-point agreements.

IoT Security: Supply Chain Perspective

IoT devices, servers, hubs, and routers alike are connected to form a complex web of information exchange. Similar to the case of physical supply chains, two main classes of risks—disruption risks and coordination risks—can propagate through such interconnections. The disruption risk of physical supply chain happens when one or more member organizations’ interrupted operations, caused by natural disasters, accidents, system failures, or purposeful human activities, disrupt the whole supply chain. Such disruption risks can happen in IoT, when the communication, coordination, or collaboration activities are crippled due to the breakdown of one or a few hubs and/or nodes. The severity of the disruption is greater when it occurs at a critical node in a complex network due to the propensity to propagate (Craighead et al. 2007). Because such critical nodes are often the highly connected, protecting these hubs is an effective way to minimize the disruption risks of IoT. This is consistent with the result from the scale-free network analysis.

Coordination risks in a physical supply chain occur when supply and demand are mismatched among member organizations. Worse, when such disparities propagate in the supply chain and get amplified in the process, the “bullwhip” effect occurs, resulting in such operational problems as excessive inventories, missed production schedules, lost revenue, and poor customer service (Lee et al., 1997). Similar coordination risks and the ensuing bullwhip effect can occur in IoT when erroneous or poor-quality information propagates throughout the network, resulting in adverse impact on many downstream devices and the financial performance of the parties that depend on the operations of those devices. In particular, when information errors came as a result of sabotage, the propagation of attack can amplify the damage in many parts of the IoT.

From a supply chain perspective, two main configurations of the IoT present different scenarios of risk propagation. First is when sensors and devices on the network edge are connected
directly or through hubs to the Internet. For instance, dedicated devices such as power meters and smoke alarms are connected to the service providers, who are in turn connected with one another via the Internet. As such, security risks can propagate directly and quickly from such edge devices; further, these “remote” devices can be tampered with physically, thereby creating access into the network. In the second configuration, edge devices may be connected to each other, as in the case of humidity sensors and smart home systems. Among these interconnected devices, one or two may be the gateway to the external network. It is possible then to isolate risks within such a self-contained system by managing those gateway devices.

In addition to physical or cyber attacks, the tampering of data, be it intentional or unintentional, can have large impact on IoT. One of the main outcomes of adopting IoT is to monitor and track the performance of “things” and thereby create value to the end user through better performance, reduced costs, and new products/features. This is particularly true in the case of Industrial IoT. To this end, data is being collected, transmitted, analyzed, and acted upon, and introducing false data into the network that could result in creating false or dangerous real-world responses is a significant threat. Imagine that when malicious signals invade a power grid through smart meters, where could result in the shutting down of power supply in a large area. From the perspective of supply chain management, to minimize such risks, it is important to recognize and enforce the separation between operational data and control data. When devices are introduced and connected through IoT, their access to the control channel may need to be restricted to avoid the potential problems of data corruption.

DISCUSSION AND CONCLUSIONS

To address IoT information security due to the nature of extensive and heterogeneous interconnections, we resort to the existing literatures in network topology, IT outsourcing, and supply chain management. In this preliminary investigation, we find the following:

- From the perspective of network topology, it is more important to secure the hubs, which connect to large number of nodes, than to secure average nodes, which connect to only a few others. In other words, those highly connected hubs should be held to a higher security standard and be significantly more protected than other devices.
- From the perspective of network topology, all IoT devices need to maintain certain (minimal) level of information security. That is, no device should be allowed to connect to the network unless its robustness is “certified,” because one weak node can cause the whole network to be infected.
- From the perspective of IT outsourcing, the relational governance such as trust and commitment may be more effective for maintaining security operations throughout IoT than formal contracts such as SLAs. To establish trust, each party/device should have a well-knows identity as well as a history of security performance and compliance that is public to all other parties in the IoT.
- From the perspective of supply-chain management, it is preferred that most devices are interconnected in a local network, which in turn connect to the whole IoT via some gateway devices. Such structure minimized the propagation of disruption risks.
- From the perspective of supply-chain management, to minimize the coordination risks, it is important to separate control data from operational data when devices are introduced into the IoT.
It is our intention to continue and extend this study of the security of IoT through the literature of existing IT and other management disciplines. We believe that such efforts can not only complement the technical development of IoT security but also offer unique insights that help address the gaps that current technical solutions leave.

REFERENCES


