SAND2016-8524C

Challenges to Securing the Internet of Things

William M.S. Stout, Vincent E. Urias
Sandia National Laboratories
Albuquerque, New Mexico
{wmstout,veuria}@sandia.gov

***Abstract*—Great advances in technology have paved the way for the computerization and interconnectedness of the world around us. The Internet of Things (IoT) describes a network comprised of physical objects or "things" embedded with electronics, software, sensors and connectivity to achieve greater value and service by exchanging data with manufacturers, users, and/or other connected devices. However, it is often the case that some of these devices are constrained by limited processing power, memory, and power consumption. These limitations may enable adverse effects as the IoT becomes pervasive, reaching into infrastructure, vehicles, and homes. As history has shown, the architects of the Internet were focused primarily on the efficiency and scaling aspects of data transfer protocols; at the dawn of the Internet, network and computer security were vacant research areas. The current trend shows the IoT market growing at an accelerated rate - will security again become an afterthought? The goal of this paper is to provide to not only a better understanding of the various IoT domains, but to survey the shortcomings and challenges to securing IoT devices and their interactions with cloud and enterprise applications.**

***Index Terms*—internet of things, cyber security, physical security, cloud, data center, software defined networking**

I. Introduction

Over the course of several decades, the progression of technology paved the way for the computerization and interconnectedness of the world around us, consisting of not only networks of high-power personal computers and servers, but also a connected web of peripheral-like devices. The Internet of Things (IoT) (also referred to as the Internet of Everything and the Internet with Things [1]) describes a network comprised of physical objects or "things" embedded with electronics, software, sensors and connectivity to achieve greater value and service by exchanging data with manufacturers, users and/or other connected devices. However, it is often the case that some of these devices are constrained by limited processing power, memory and power consumption. These limitations may enable adverse effects as the IoT becomes pervasive, reaching into infrastructure, buildings and homes. The current trend shows IoT technologies growing rapidly, will security for these environments grow in tandem? Researchers have deduced that IoT-based companies with no experience in security are diving into the space rapidly by adding connectivity mechanisms to their devices [2]. As reported by Hewlett-Packard in a 2015 report on IoT research [3]:

- Six out of 10 device user interfaces (UI) were vulnerable (such as XSS and weak credentials)
- 80% of devices (with cloud and mobile app components) failed to require passwords of sufficient complexity
- 70% of devices (with cloud and mobile app components) enabled an attacker to identify valid user accounts through enumeration
- 70% of devices used unencrypted network services
- 90% of devices collected at least one piece of personally identifiable information (via device, cloud or mobile app)

The web user interfaces that are deployed to interact with, monitor or control IoT devices have also come under scrutiny [4]. The Open Web Application Security Project (OWASP) [5] has enumerated the following list of the top 10 IoT vulnerabilities:

1) Insecure Web Interface
2) Insufficient Authentication/Authorization
3) Insecure Network Services
4) Lack of Transport Encryption
5) Privacy Concerns
6) Insecure Cloud Interface
7) Insecure Mobile Interface
8) Insufficient Security Configurability
9) Insecure Software/Firmware
10) Poor Physical Security

Current approaches to secure IoT (if at all) have attempted to leverage communication protocol-based mechanisms, such as encryption for data-at-rest or in-transit. But this may not be sufficient if the constrained endpoints themselves are susceptible to modification either by local access or remote connections. Can researchers leverage emerging computer and network security frameworks to incorporate security into this burgeoning domain? Gartner predicts that by 2020 more than 25% of identified attacks in an Enterprise will be against IoT devices or systems, even though IoT will only account for less than 10% of IT security budgets [6]. Since most of the vendor provided platforms and solutions often rely on cloud infrastructure to provide data storage and management portals to consumers, the same inherent risks and vulnerabilities with cloud services reveal themselves in these predicaments.

To begin this survey of challenges, we start by reviewing the make-up of IoT in Section II. Section III delves into current research being done to secure IoT; Section IV looks at industry's approach to IoT. The threat surface of IoT is covered in Section V. Finally, we summarize and make final conclusions in Section VI.

II. Within the Internet of Things

Market analysts for the Internet of Things have proposed that by 2020, 50 billion devices will comprise the IoT [7].

Many consortia and working groups, both in academia and industry have been created and engaged to promote device and communication standardization, power efficiency, as well as security [8][9][10][11][12]. It is often the case that these devices communicate "machine-to-machine" over the typical IP networks used for mission and business space. Like other embedded devices (e.g., sensors) IoT devices are usually constrained by limited processing power, memory or power consumption. The unique platforms, devices and service requirements suggest new challenges for integration as the IoT becomes more widespread. The devices that comprise the IoT can be generally classified into the following four categories [13]:

- PCs, servers, routers, switches and other such devices under the umbrella of Information Technology (IT)
- Medical machinery, SCADA, process control, etc., under the umbrella of Operational Technology (OT)
- Smartphones and tablets used by consumers/employees
- Single-purpose devices used by consumers, IT or OT

The devices may be arranged to describe a general architecture of an IoT; the IoT architecture can be summed up as a system built on layers. Not unlike the layered primitives that exist in communications (such as the OSI or TCP/IP model), each layer may be developed autonomously from the other layers. Thus, the goals and services that the specific layer provides can be implemented and tested with little influence from upper or lower layers. It is the interfaces between layers that must be standardized in order to connect the disparate pieces together to create the supporting IoT structure. A notional IoT model is shown in Figure 1[14], depicting the funneling effect through layers from the plethora of Things, to the single User Interface (or Controlling Device).

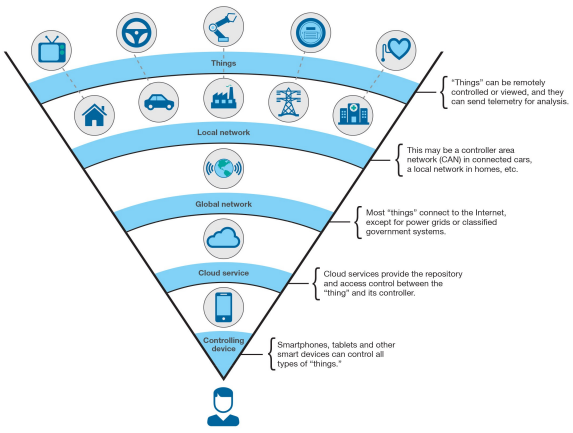

Fig. 1. IBM IoT Model.

The model is notional in that any IoT architecture may add nuances, or remove components. In the case of machine-to-machine communications, the Thing's data may never extend past the local area network. In the case of Cloud processing, data from a Thing may hit the Cloud, which may in turn leverage machine learning algorithms to effect change on other Things. One size does not necessarily fit all, contributing to the difficulty of IoT standardization; the difficulty is further compounded when considering the diverse hardware, operating systems/software, and gateway requirements needed for an IoT. To abstract the intricacies of the IoT model, the five layers above may be distilled into three: Application, Network and Perception [15]. High level overviews for each system are described below.

A. The Perception Layer

The Perception Layer includes the physical world and each Thing in the IoT that involves information gathering. This layer may consist of actuators, sensors, smartphones, etc. When considering a "device," it may be interpreted as a single device, modular device, or a collection of sensors. As such, the effect of a device may be modeled as a single discrete event (open door, actuation, etc), or as a "room" with all included sensors (photosensor, temperature, etc). An example of the density of devices in the context of a Smart Home may be viewed in [16], where a vast number of different devices might occupy a relative small space. The IoT application for a particular device may require many different considerations, such as cost, device role (sensor, actuator), power budget, and networking environment/requirements (cabled, WiFi, cellular, modem, mobile). The collection of data from said device should take into consideration: data formatting, packaging (security), data validation, sorting functions, data enhancement, and/or summarizing/conflating data. Typically, device data will include [17]:

- Device metadata (often static), such as:
  - Device id
  - Class or type
  - Model
  - Revision
  - Manufacture date
  - HW serial number
- State information of the device (e.g., what is it doing?)
- Telemetry collected data from a sensor (each telemetry source results in a channel)
- Commands or actions performed by the device
- Operational information relevant to operation of the device (CPU operating temp, battery state)

The difficulty in managing the IoT device will be choosing the appropriate device for the application and ensuring it is configured correctly in order to preserve power, data flow, and security. Also, physical protection, authentication and data provenance are also notions to consider with regard to device security.

B. The Network layer

The Network Layer transmits the information gathered in the Perception Layer. All the networking elements are integrated in this layer; device addressing, pre-filtering, packet forwarding, routing, and security protocols are some of the key functionalities of this layer. Based on the IoT application, the

transmission medium, collection/aggregation, distribution and format may vary heavily. For example, vehicles may require the support of telematics data and controller area network (CAN) buses, wearables and eHealth may require the support of Personal Area Network (PAN) protocols, and assets may require the use of mobile communications. Often it is the case that devices will not have the capability to connect directly to the Internet, as such gateway devices must be installed to provide translation (i.e., between networks of different protocols and/or mediums). IoT gateways are primarily placed between end devices and the Cloud, especially for devices that lack full TCP/IP network stacks. For example, Bluetooth Low Energy (BLE) devices do not support SSL/TLS to transmit back to the Cloud, nor have the power profile to continuously do so. Gateways can condense data, store data in a local database, provide a realtime clock for timestamps and synchronization, and local caches for device firmware updates.

Beyond the gateways are metropolitan and wide area networks to transport data to edge or central processing centers. These networks can be disparate or overlapping, based on the IoT model. One such example is a Smart City. The Smart City industry is projected to be a $400 billion market by 2020, with 600 cities worldwide [18]. A Smart City IoT may include sensors, actuators and similar technology to connect components across an entire metropolis, impacting every layer of that city, from tunnels beneath the streets, to the air that citizens breathe. The Smart City networks that may be deployed include smart energy, transportation, environment data, infrastructure, mobility, as well as general smart IoT. One may see that as captured city data increases, so do the requirements for bandwidth in the network layer - as well as the need to protect the integrity of the data.

C. The Application layer

The Application Layer provides the processing and presentation of the data. Its functions include communication synchronization, data processing, resource allocation, logging and presentation and/or control to a user or graphical interface. This layer includes everything from the Cloud, to the APP on a smartphone. The path through which IoT enters this computing space may be varied, but is normally based on a platform solution. Platforms may be broadly categorized into the following [19]:

- "White-box" solution: white-box products are ingested into larger, often proprietary, IoT solution framework
- Stand-alone solution: "one-off" devices are integrated into a network and managed on an as-needed basis.
- DIY-type solution: a user-generated/managed platform is created from one or many disparate vendors
- Service-based solution: a service provider provides for IoT devices and services (user may manage)
- Market disrupter: Large-scale companies provide readily accessible IoT solutions for consumers

The introduction of IoT into conventional enterprise and functionally-static environments complicates the traditional approach to building and monitoring infrastructure. Integrating any number of these solutions may be difficult as the underlying technologies may not be standardized or compatible with in-place infrastructure, or the platform and/or devices may not be suitable for accreditation into certain networks. The latter may be exacerbated when considering the rate at which new devices (either upgraded or added) must undergo reaccreditation. With respect to the network, the swath of devices generating traffic may saturate bandwidth. Devices such as smart locks, lights and thermostats may trickle data, but as more critical physical processes transmit state-of-health data over wired and wireless networks, the sum of the whole will begin to reveal itself. The ingestion of copious amounts of status-of-health data may also spill into datacenter compute and storage resources, as the need to conduct data distillation, mining and analysis will be paramount to ensuring efficiency and uptime.

Remarks: Device management may be challenging as provisioning devices may require credentials, authentication and registration; operations must ensure secure collection of information, data provenance and the ability to monitor, log, audit, and report errors efficiently; updating of devices' firm/software remotely over-the-air may cause downtime or even device failure. Furthermore, there may be cases where device management may not even be possible due to lack of standardization or lack of device capability. For devices that do provide interfaces for connectivity and management, fusion with other sources and/or systems may prove fruitless. Connectivity may consist of many different means, configurations and protocols leading to a management and troubleshooting nightmare. In the processing and cloud space, developing applications for the devices may require several skill sets in programming languages, from web runtimes to native, to managed runtime languages. All of these factors have in and of themselves vulnerability risks that may be exploited, whether through software or firmware flaws, physical access, misconfiguration, social engineering or human error.

III. IoT Research Efforts

As the spread of IoT grows, many shortcomings have surfaced. The gaps have inspired the research community to take an active role in surveying, developing and implementing many different techniques to address deficiencies in security, privacy and resiliency.

A. Software Defined Networking Approaches

With the entrance of novel ways to control network infrastructure and services, many researchers have attempted to draw software defined networking (SDN) technologies into their solution space for IoT problems [21][22]. SDN and network function virtualization (NFV) been leveraged heavily to support operations in the datacenter [23][24][25]. The flexibility and centralized management aspects of SDN make it ideal in distributing not only customized network paths and flows, but also policy. The authors of [26] leverage SDN

to improve the communication performance and resilience of IoT, defining a method that automatically performs dynamic switching between the redundant non-SDN communication edges. In [27], SDN and NFV are taken further into specific layers of IoT infrastructure services. The authors describe: a Service Layer that embeds all service-level functions; the IoT referential and the presentation of infrastructure services; a Global OS layer that embeds the infrastructure services' inventory and description; the network/IT orchestration and SDN controllers; an NFV Orchestrator that manages the resources to fulfill the infrastructure services' lifecycles; the SDN controller, responsible for the end-to-end control of the network and IT resources; and finally, the virtualization layer which organizes the hardware resources onto virtual machines made available to the above layers. The authors do allude to the necessity of standardization to address the management of many infrastructure services. In 6TiSCH [28], the notion of standardization is the impetus for incorporating SDN features. The paper works off of the Internet Engineering Task Force (IETF) standards to define architecture heavily dependent on precise scheduling, leveraging a Path Computation Element (PCE) under the Deterministic Networking (DetNet) paradigm.

B. Wireless/WSN Problems

6TiSCH and the PCE are often tied to the needs for industrial Wireless Sensor Networks (WSNs). WSNs and wireless-based communication technologies are expected to be a major component of the Things and Network tiers of the IoT, and also present security challenges. Wireless endpoints could be as simple as Radio Frequency Identification Tags (RFIDs). In [29], several protection mechanisms in the form of encryption have been outlined for low-cost RFID tags. The authors of [30] and [31] present many obstacles in the domain of securing WSN. The former presents three integration approaches in Confidentiality, Integrity and Availability (CIA) and analyzes various related security issues. The latter paper explains methods of integration for a front-end proxy solution, a gateway solution and TCP/IP solutions, to include security issues. The authors also provide security strategies for WSNs connected to Internet and suggest key management schemes like PKI, IBE or some combination of both can provide secure communications between the sensors and internet hosts. The developers of fabryq [32] move the wireless conversation to deploying cellphones as network gateway devices for Things. Their approach uses smartphones as bridges that connect devices using BLE to the Internet. The use of smartphones lends itself to the question of using cellular network connectivity to push acquired data to a processing node. In [33] the issues of security are highlighted when using this transport medium. While provider architectures benefit from the existing authentication methods, there still exists an alarming lack of basic security features in certain applications for IoT systems. These are often manifested in devices or gateways that tend to include legacy protocols lacking effective security mechanisms (such as 2G).

C. Encryption/Systems

Many legacy and rush-to-market IoT devices may lack the ability to enable encryption; however, standards bodies are beginning to require such capabilities for device interoperability and security. The encryption requirements are normally well-established point-to-point algorithms, and do not necessarily address continuous, updated encryption through the lifetime of a device, key distribution, or full-path security within an IoT ecosystem. The authors of [34] move away from endpoint Things and review the need for security and encryption for servers and services supporting IoT infrastructure. In [35], the authors apply HIMMO [36] to the IoT, due to its low resource needs and easy integration with modern protocols. The scheme provides full collusion resistance, device and back-end authentication/verification, pairwise key agreement, and support for multiple TTPs and key escrow. The need for an end-to-end solution provides a greater security footprint by attempting to ensure the full path between two communicating parties is hardened against eavesdropping, leakage or man-in-the-middle (MITM). In this thesis work [37], the author describes an encryption system and methodology to take data from the device to the intended destination server, leveraging several different encryption algorithms.

D. Authentication

Although encrypted links provide security for the data in transport, the recipient must be able to confirm that the endpoint is who (or what) it says it is. Two key factors in verifying the authenticity of IoT data are: (1) the identity of the sending node (e.g., device identifier or sensor number), and (2) the integrity (authenticity) of the data transmitted. The notion of authenticating objects and entities is a ripe area for research in IoT. The authors of [38] provide an authentication model for IoT clouds, relying on Trust Module Platform (TPM) to provide a chain of trust from hardware device(s) to software elements. In [39] the authors enumerate a handful of IoT communication scenarios and investigate the threats to the large-scale, unreliable, pervasive computing environment. They primarily focus their research on identity management and authentication. In their paper they assess authentication models by: (1) gateway, (2) security token, (3) trust chain, (4) global trust tree, and provide pros and cons for each technique. The authors of [40] consider the authentication problem when there is no user in the loop to confirm or engage authentication processes. Not only do they address the security challenge of secure distribution of access credentials (e.g., WiFi networks, SIM cards, network access credentials), but also the insecurities of secure bootstrapping of new devices; that is, provisioning of secure connectivity (and the secure exchange of access keys) without out-of-the-box connectivity available to the device.

E. Dynamic Systems

Finally, mechanisms and systems to address security in the immediate sense, but how may the policies and approaches be updated dynamically to address new devices,

security postures, environments, or changes in personnel over time? The authors of [41] devise a framework for adapting security for IoT in healthcare applications. Their framework is based on a generic system model that addresses security and quality of service, using context-aware adaptive algorithms as security solutions for the IoT in eHealth. The framework can quantify the characteristics and requirements of a given health situation. Their paper presents assessments for adaptive security solutions in eHealth, to include context, data-communication, the devices, and the actions of the involved actors. In [42], dynamism is contained by the shifting of the security landscape, in particular for safety-critical infrastructures. The authors propose the use of a cyclic cyber physical security model that allows knowledge transfer between regulatory bodies through the sharing of best practices. This continuous sharing enables system operators to identify exploits encountered from other industries and maintain high security levels and improve the IoT architectures. The model also lends itself to the need to conduct training for operators and incident responders to distinguish between normal and abnormal behaviors in IoT domains.

Remarks: When dealing with sprawling systems or problems, the researcher often decomposes the problem into smaller subproblems. While this process may work in an academic context, the physical complexity of the IoT, a system-of-systems, cannot be addressed with this methodology. The strongest encryption has no use in a system with weak passwords. Within the IoT, the level of heterogeneity does not lend itself to eased deployment of security; in fact, it complicates the effort exponentially. For example, many Things contain embedded operating systems and software that pose obstacles for IT to configure security and maintain patches [13].

IV. IoT in Industry

According to industry estimates, machine-to-machine communications alone will generate approximately US$900 billion in revenues by 2020 [43]. Thus, as a budding industry, the IoT domain has attracted the interest of many companies, corporations, service providers as well as open-source entities to make investments in the IoT market. Their products range from systems on chips to entire IoT platforms.

The Intel Corporation has developed an IoT Gateway Solution [44] for gathering intelligence at the IoT edge, enabling near real-time analysis and efficient process controls. Their solution provides: (1) connectivity up to the Cloud and enterprises; (2) connectivity to sensors and existing embedded controllers; (3) pre-process filtering of selected data for delivery; (4) localized decision making; (5) a hardware root of trust, data encryption, attestation, and software lockdown for security; and (6) local computing for in-device analytics.

Amazon provides an IoT platform under its Amazon Web Service (AWS) cloud computing service [45]. The platform establishes a conduit for connected IoT devices to securely interact with AWS services (e.g., Lambda, Kinesis, S3, Machine Learning, DynamoDB, CloudWatch, ElasticSearch, and Rules), as well as other connected devices. AWS IoT supports HTTP/S, WebSockets, and MQTT connecting to devices and authentication (SigV4, X.509), end-to-end encryption, and the ability to deploy policy and granular permissions. It also provides a service called Device Shadowing: a persistent virtual device that includes device's latest state so that applications or other devices can read messages and interact with the device (even if offline). Shadowing provides a constantly available REST API for applications to continue to operate.

Similar to AWS offerings is the Google Cloud Platform for IoT Solutions [17]. Like AWS, it provides its cloud service to be leveraged for IoT purposes (Cloud Pub/Sub, Pipeline, Dataflow, Storage, Rules, Analytics and Dashboards). In the realm of security, the platform employs "Google-Grade Security": device-to-cloud or vice versa; secured by default with full encryption and backed by integrated and pervasive security across entire infrastructure; Cloud Identity and Access Management (IAM) ensures devices have access only to what resources are explicitly designated. What separates Google from Amazon is Google's physical transport infrastructure, the Google Fiber Network, providing 70 points of presence in 33 countries for ultra-low latency and resiliency.

While entities like Amazon and Google have essentially brought their cloud services to IoT, companies like AT&T provide entire platforms, from data center processing to the communications termination point on the device [46]. AT&T's IoT portfolio targets many industry areas, such as vehicles, asset management (supply chain), Smart Cities, and heathcare (e.g., wellness tracking, virtual care). Like the former, they provide data processing services in their clouds and connectivity protocols for data ingestion. However, as a telco and ISP, AT&T provides connectivity and infrastructure down to the device. Global connectivity is provided by custom chips or modules supporting 3G, 4G, 4G LTE, in form factors like LGA, surface mount, and PCIe; their global SIM product may be used for remote deployment, connection, and management of devices end-to-end, with global connectivity (500 carriers, 200 countries, "1 global contract"). For security, AT&T relies on embedding security across four layers: (1) at the endpoint (AT&T Global SIM); (2) at the network (VPN, NetBond, Commercial Connectivity Service (CCS), custom private Access Point Names (APNs)); (3) at data and application (cloud/on-premises firewalls, encryption, DDoS protection, Cloud Web Security); and (4) threat management (behavioral analytics and traffic analysis (device, connection or application)).

Several advantages may be observed when considering platform provided solutions by single companies (e.g., deployment, integration, maintenance). However, such detriments as vendor lock-in, interoperability, service lease agreements, company bankruptcy or buy-out, data governance, policy, and software/firmware vulnerabilities may taint these positive aspects. The notion of "roll-your-own" may be suitable for those companies that have the technical talent and prowess

to own their own solutions. The availability of open-source solutions for this space is not unheard of.

The open-source OpenDaylight (ODL) project [47] is a SDN controller platform that provides solutions to automated service delivery, network resource optimization, cloud and NFV, research, education and government, and visibility and control. One installable feature of the ODL platform is the IoT Data Management (IoTDM) project. IoTDM is an open-source implementation of the oneM2M specification, running on OpenDaylight. It provides a data-centric middleware application that acts as a oneM2M compliant IoT Data Broker, thereby enabling authorized applications to retrieve IoT data uploaded by any device.

The company tcp cloud [48] created an entire smart city platform using open-source software. Their SmartCity project [49] was based in the small city of Pisek, located in the Czech Republic. The deployment consisted of 3,000 endpoints and approximately 300 IoT gateways. A similar deployment was demonstrated at the OpenStack Summit 2016. The endpoint devices leveraged IQRF (wireless mesh technology operating on sub-gigahertz ISM bands) which provided a full mesh network, terminating into IoT gateways (Raspberry Pi) which in turn uploaded data to the Cloud through LTE, GSM, or WiFi protocols. The gateways supported multiple sensor platforms for multiple customers through the use of micro-services segmentation (via Docker containers) and Kubernetes for multi-tenancy support. The Open Contrail SDN controller was used for multitenancy and segmentation of traffic - tying each Docker container to a respective VM for data collection. OpenStack was used as the Cloud platform for hosting all control services as well as all big data processing and frontend visualization units. Their solution provided an open data portal and data API available for third party companies to glean information about:

- Traffic flow, routing, parking
- Monitoring, management, energy savings
- E-commerce, marketing, tourist information
- Environmental analysis
- Lifestyle, social services, social networks

Remarks: It would appear that orchestration takes a top down approach in order to apply the latest models of abstraction (e.g., software-defined-*, cloud); this abstraction is primarily for a user, application or machine to interact with the underlying systems more efficiently and effectively. But it may be unrealistic to stitch together heterogeneous systems and provide adequate management of them; this approach is essentially a "bolt-on" solution and is not persistent. And although the final system may attempt to provide a robust, resilient communications architecture, the many moving pieces may actually be detrimental to system stability itself. Precision timing and accurate state of health for all intermediate and terminating devices is required; however, if an intermediate node fails in the system, the effects will cascade. Finally, if the all-in-one solution is provided by a vendor, benefits may be quickly realized, such as data analytics. However, there is risk in outsourcing control to an external entity; one such example is the effect of software bugs in distributed devices [20]. Since the IoT is still very new, risk also exists with investing in products and vendors that may not survive this initial bubble, which may leave a consumer with unsupported devices prone to failure or security risks.

V. IoT Threat Surface

Just as the boundaries of IoT are impossible to fully define, is it also impossible to fully address all of the parts and pieces contained within it. The devices and systems in the IoT can vastly differ, occupying completely different operating spaces (IT vs. OT). Thus, difficult operations in an enterprise such as protecting legacy devices, software patching, network mapping, device management and technology refreshing become considerably exacerbated in the IoT. Lack of diligence in any one of these areas opens up huge holes in the fabric of system security.

Security threats to IoT can be generally divided into two categories [39]. In the first category, the threats are similar to those in conventional network ecosystems, and revolve around confidentiality, integrity, and availability. But as mentioned, the complexity and severity of the security threats is much greater. The other category of threats arises from the type of data being carried in the IoT. IoT objects often take sensitive readings that pertain to humans; thus, for certain applications, the data in the IoT ecosystem is personal and dynamic. The data readings about device owners (or persons inadvertently monitored) may provide information leakage about persons' geological locations, health, and living habits enabling attackers to extract and disclose personal data. Thus, in this context, security starts at the device. At the device level, attack surfaces may be categorized into:

- Device hardware security vulnerabilities
- Firmware based vulnerabilities
- Mobile and web app security issues
- Radio and network communication based vulnerabilities

To date, hackers have recorded success on such Things as Nest, WiFi Kettle and Coffee Maker, Belkin Smart Plug, Cayla Doll, LG refrigerator, Lifx light bulbs, and Smart TVs. According to [50], an experienced attacker can run code injection on a Fitbit device in less than 10 seconds, which could later plug into a personal computing device and distribute malware across a network.

At the network level, each device must be equipped with a unique ID or address to enable communications over a data network. The unique attribute allows the device to be targeted. Vulnerabilities caused by using simple passwords or relying on default passwords on embedded systems can be easily exploitable. Furthermore, such devices are often never powered down; persistent network connectivity effectively shortens the attack time against vulnerabilities of largely unsecured end point devices. The lack of basic security features has allowed researchers to discover new vulnerabilities and attack vectors against IoT systems, such as allowing remote ignition of a car's engine or getting root access on a home automation

connectivity hub [33]. As a threat in the wild, one of the first botnet of IoT devices was identified in 2013 [51]. Furthermore, over a quarter of identified botnets are formed by devices other than computers, such as electrical appliances, smart TVs, sensors and other household utilities [51].

Disrupting service is also a threat in IoT. DoS/DDOS attacks are already well documented for the Internet and enterprises; IoT is also susceptible to such attacks but will require specific techniques and mechanisms for resilience to ensure that transportation, energy and city infrastructures are not disabled or subverted [52]. Devices with limited and constrained resources may not be capable of averting flood or fuzz attacks. Other threat scenarios include the deletion of service encryption keys stored in the memory of embedded devices to distributing malicious or corrupted software in the M2M core service provider network, or corrupted firmware to endpoints [33]

From the device to the Cloud, interesting vulnerabilities may exist. As mentioned above in [40], security software was often developed with the notion that a user would be physically present at the endpoint, to act as a decision-maker in the data security event (either configuration or attack). With IoT, the device may no longer have a user present to intervene. The problem manifests itself in risks of non-browser SSL certificate verification, and the extent to which widely deployed and relied-upon libraries and software may fail to properly validate certificates.

The authors of [53] provide an extensive and exhaustive list of the threats that exist against the IoT. Each threat may exploit one or more vulnerabilities and result in the final risk for an entire IoT system. The list has been updated from the original scenarios to broadly capture the threats that exist today.

1) Denial of service attack/flood/buffer overflow.
2) Spoofing of credentials/bypass authentication.
3) Large-scale unauthorized data mining, surveillance.
4) Man-in-the-middle attack.
5) Unauthorized access/deletion/modification of data.
6) Side channel attack.
7) Jamming.
8) Fake/rogue scanners/collectors.
9) Worms, viruses and malicious code.
10) Procedures/instructions not followed.
11) Function creep.
12) Profiling.
13) Exclusion of subject from the data processing process.

A survey conducted by the SANS Institute asked 391 individuals from a broad range of industries what they perceived as the greatest IoT threat vectors [13]. 31% felt the IoT and the high level of embedded operating systems and applications would be left vulnerable due to poor patch management practices. Another familiar issue - malware - was the next most highly cited at 26%, with the concern being IoT devices would end up spreading malware into the enterprise. Denial of service (13%) and sabotage and destruction of connected Things (12%) were also concerns; 10% saw user error as the greatest threat vector.

Remarks: The uniqueness of the IoT is not necessarily espoused in the idea of multi-data fusion, but rather the integration of its constituent components. Each individual layer of an IoT subsystem consists of a communications plane or computing device that is either fully represented by or has its roots in previous domain:

- Parallels may be drawn between the endpoint devices and the motes of WSN and the logic controllers of SCADA/ICS.
- Local area networks have been extant since the dawn of the Internet, relying on the conventional network stacks that have carried last hop communications for decades.
- The big pipes of the global Internet have facilitated streams of data between islands of autonomous systems with 5G and direct ISP/datacenter connections being prepped for the upcoming flood.
- Cloud may be seen an extension of grid computing, and has grown to absorb many of the compute responsibilities once handled by companies themselves.
- Controlling devices, drawn from HMIs and PCs have now been placed in the palms of smartphone users.

The antecedent technologies of the IoT layers have presented avenues for further development. However, it is our conjecture (and observation) that the lack of baked-in security in these respective areas has led to latent manifestation of security oversights; the security gaps being addressed are often persistent areas that have not yet been tackled. Thus, the amalgamation of these technologies, that is the IoT, is steeped in a vast swath of insecurity across many varied attack surfaces.

VI. Conclusions

In this paper we reviewed the building blocks of the IoT to better understand idiosyncrasies of various IoT domains. We also surveyed current security-based research thrusts in IoT, the ways industry is approaching IoT, and the vast threat surface IoT reveals. Although IoT presents a new paradigm in the integration of OT and IT spaces, its foundations are firmly rooted in the architectural layers that have come before it. It has been the case that security issues not completely solved then are still manifest in the underlying planes of the IoT. Also, the IoT tends toward a layered approach. This layered approach accommodates point (or single-layer) solutions for security, overlooking the benefits that come with cross-layer solutions. As such, system security suffers due to the weakest points in the chain (e.g., endpoint security). Finally, for systems that do attempt to address security across the board, there is risk in the "all-in-one" basket approach. Furthermore, with new methods (SD*), the security for these systems is not yet understood, and may present a larger threat surface in management than in the operations. These are just a handful of the challenges that exist when securing the IoT. Future work will attempt to offer methods or solutions to better secure the IoT.

REFERENCES

[1] R. Saracco, IEEE Communication Society, BLOG: The Internet Of Things (And With Things), http://www.comsoc.org/blog/internet-things-and-things

[2] K. Hill, Forbes, The Half-Baked Security Of Our 'Internet Of Things', http://www.forbes.com/sites/kashmirhill/2014/05/27/article-may-scare-you-away-from-internet-of-things/#688f5bb323dd

[3] Hewlett-Packard, Internet of things research study 2015 report, http://www8.hp.com/h20195/V2/GetPDF.aspx/4AA5-4759ENW.pdf

[4] Open Web Application Security Project (OWASP), Internet of Things Project, https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project

[5] Open Web Application Security Project (OWASP), Top 10 Internet of Things Vulnerability Categories, https://www.owasp.org/images/8/8e/Infographic-v1.jpg

[6] Gartner Inc., The Internet of Things: Check Before You Implement, http://www.gartner.com/technology/research/internet-of-things/

[7] DHL, Internet of Things in Logistics, http://www.dhl.com/en/about-us/logistics-insights/dhl-trend-research/internet-of-things.html

[8] Stanford University, Secure Internet of Things Project, http://iot.stanford.edu/

[9] oneM2M, Standards for M2M and the Internet of Things, http://www.onem2m.org/

[10] A. Keranen, C. Bormann, IETF, Internet of Things: Standards and Guidance from the IETF, https://www.internetsociety.org/publications/ietf-journal-april-2016/internet-things-standards-and-guidance-ietf

[11] ETSI, Internet of Things, http://www.etsi.org/technologies-clusters/technologies/internet-of-things

[12] IEEE Internet of Things, http://iot.ieee.org/

[13] J. Pescatore, SANS Institute, "Securing the Internet of Things Survey," SANS Institute InfoSec Reading Room, January 2014

[14] IBM X-Force, http://www-03.ibm.com/security/xforce/

[15] W. Miao, T.L., L. Fei, S. Ling, D. Hui, "Research on the architecture of Internet of things," IEEE International Conference on Advanced Computer Theory and Engineering (ICACTE), 2010.

[16] Smart Home Energy, http://smarthomeenergy.co.uk/

[17] Google Cloud Platform, Internet of Things (IoT) Solutions, https://cloud.google.com/solutions/iot/

[18] T. Maddox, TechRepublic, Smart cities: 6 essential technologies, http://www.techrepublic.com/article/smart-cities-6-essential-technologies/

[19] J. Ekholm, Gartner Inc., The Connected Home, http://www.gartner.com/technology/research/internet-of-things/

[20] N. Bilton, The New York Times, Nest Thermostat Glitch Leaves Users in the Cold, http://www.nytimes.com/2016/01/14/fashion/nest-thermostat-glitch-battery-dies-software-freeze.html?_r=0

[21] Y. Jararweh, et al. "SDIoT: a software defined based internet of things framework," Journal of Ambient Intelligence and Humanized Computing 6.4 (2015): 453-461.

[22] R. Vilalta, et al. "End-to-End SDN orchestration of IoT services using an SDN/NFV-enabled edge node," Optical Fiber Communication Conference. Optical Society of America, 2016.

[23] Juniper Networks, Integrating SDN into the Data Center White Paper, http://www.juniper.net/us/en/local/pdf/whitepapers/2000542-en.pdf

[24] Cisco, SDN for Data Center (ACI), http://www.cisco.com/c/en/us/solutions/software-defined-networking/sdn-data-center.html

[25] VMware, Software-Defined Datacenter In Depth, http://www.vmware.com/solutions/software-defined-datacenter/in-depth.html

[26] H. Sndor, B. Genge and G. Sebestyn-Pl, "Resilience in the Internet of Things: The Software Defined Networking approach," Intelligent Computer Communication and Processing (ICCP), 2015 IEEE International Conference on, Cluj-Napoca, 2015, pp. 545-552.

[27] N. Omnes, M. Bouillon, G. Fromentoux and O. L. Grand, "A programmable and virtualized network & IT infrastructure for the internet of things: How can NFV & SDN help for facing the upcoming challenges," Intelligence in Next Generation Networks (ICIN), 2015 18th International Conference on, Paris, 2015, pp. 64-69.

[28] P. Thubert, M. R. Palattella and T. Engel, "6TiSCH centralized scheduling: When SDN meet IoT," Standards for Communications and Networking (CSCN), 2015 IEEE Conference on, Tokyo, 2015, pp. 42-47.

[29] S. Li, L.D. Xu, S. Zhao, "The internet of things: a survey," Information Systems Frontiers, April 2015, Volume 17, Issue 2, pp. 243259.

[30] P.G. Shah, J. Ambareen, "A Survey of Security Challenges in IoT integration with WSN," Aus Journal, 2015.

[31] D.K. Meghana, M. R. Mundada, "A survey on providing security to the wireless sensor networks integrated with IOT," International Journal of Engineering and Technical Research, Volume 2, Issue 12, December 2014, pp. 202-205.

[32] W. McGrath, M. Etemadi, W. Roy, B. Hatmann, "fabryq: using phones as gateways to prototype internet of things applications using web scripting," In Proceedings of the 7th ACM SIGCHI Symposium on Engineering Interactive Computing Systems (EICS '15), ACM, pp. 164-173

[33] R.P. Jover, "Security and impact of the IoT on LTE mobile networks," Security and Privacy in the Internet of Things (IoT): Models, Algorithms, and Implementations, Taylor & Francis LLC, CRC Press, 2015.

[34] M. Niemeyer, et al., "Security requirements of IoT-based smart buildings using RESTful Web Services," 30th International Kand Conference on 20th November 2014.

[35] O. Garcia-Morchon, et al., "A comprehensive and lightweight security architecture to secure the IoT throughout the lifecycle of a device based on HIMMO," International Symposium on Algorithms and Experiments for Sensor Systems, Wireless Networks and Distributed Robotics, Springer International Publishing, 2015.

[36] O. Garca-Morchon, et al., "HIMMO: A Lightweight Collusion-Resistant Key Predistribution Scheme," Cryptology ePrint Archive, Report 2014/698, pp. 128.

[37] J. King, "A Distributed Security Scheme to Secure Data Communication between Class-0 IoT Devices and the Internet," Master's Thesis, Lulea University of Technology, 2015.

[38] L. Barreto, et al., "An Authentication Model for IoT Clouds," Proceedings of the 2015 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining 2015, ACM 2015.

[39] Z.K. Zhang, M.C.Y. Cho, and S. Shieh, "Emerging security threats and countermeasures in IoT," Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security, ACM 2015.

[40] D. Thomas, G. Paul, and J. Irvine, "Going beyond the user the challenges of universal connectivity in IoT", https://pure.strath.ac.uk/portal/files/45177079/Thomas-etal-WWRF35-going-beyond-user-challenges-universal-connectivity-IoT.pdf

[41] W. Leister, et al., "An Evaluation Framework for Adaptive Security for the IoT in eHealth," International Journal on Advances in Security, Vol 7 no 3 & 4, 2014.

[42] X. Bellekens, et. al., "Cyber-physical-security model for safety-critical iot infrastructures," Wireless World Research Forum Meeting 35, no. WWRF35, 2015.

[43] EY, Cyber Security and the Internet of Things Report, http://www.ey.com/GL/en/Services/Advisory/EY-cybersecurity-and-the-Internet-of-things

[44] Intel IoT Gateway Technology, Turn data at the edge into real value, https://www-ssl.intel.com/content/www/us/en/embedded/solutions/iot-gateway/overview.html

[45] Amazon Web Services, AWS IOT, https://aws.amazon.com/iot/

[46] AT&T, Internet of Things, https://www.business.att.com/enterprise/Portfolio/internet-of-things/

[47] OpenDaylight, IoT Data Management (IoTDM), https://wiki.opendaylight.org/view/IoTDM:Main

[48] tcp cloud, Use cases, http://www.tcpcloud.eu/#use-cases

[49] J. Pavlik, OpenStack Superuser, OpenStack and Kubernetes join forces for an Internet of Things platform, http://superuser.openstack.org/articles/openstack-and-kubernetes-join-forces-for-an-internet-of-things-platform)

[50] B. Moon, Forbes, Fitbit Disputes Claim Fitbit Trackers Can Be Hacked And Infect PCs, http://www.forbes.com/sites/bradmoon/2015/10/21/fitbit-trackers-can-be-hacked-infect-pcs/#5eca0d411764

[51] V. Benson, "Personal Information Security and the IoT: The Changing Landscape of Data Privacy," Computer Communication & Collaboration, Vol. 3, Issue 4, pp. 15-19, 2015.

[52] G.O. Odulaja, "Security Issues in the Internet of Things," Computing, Information Systems, Development Informatics & Allied Research Journal, Vol. 6 No. 1. March 2015, pp. 33-40.

[53] D.J. MacInnis, V.M. Patrick, and C.W. Park, "Looking Through the Crystal Ball," Review of Marketing Research, Volume 2, Emerald Group Publishing Limited 2, 2006, pp. 43-80.