# Augmenting Security of Internet-of-Things Using Programmable Network-Centric Approaches: A Position Paper

Hammad Iqbal, Jamie Ma, Qing Mu, Venkatesh Ramaswamy, Gabby Raymond, Daniel Vivanco, and John Zuena
The MITRE Corporation
202 Burlington Road
Bedford, MA 01730
{hammad,jma,qmu,vramaswamy,graymond,dvivanco,jzuena}@mitre.org

***Abstract*—Advances in large scale computing and communications infrastructure, coupled with recent progress in big data analytics, have enabled linking several billion devices to the Internet. These devices provide unprecedented automation, cognitive capabilities, and situational awareness. This new ecosystem---termed as the Internet-of-Things (IoT)---also provides many entry points into the network through the gadgets that connect to the Internet, making security of IoT systems a complex problem. In this position paper, we argue that in order to build a safer IoT system, we need a radically new approach to security. We propose a new security framework that draws ideas from software defined networks (SDN), and data analytics techniques; this framework provides dynamic policy enforcements on every layer of the protocol stack and can adapt quickly to a diverse set of industry use-cases that IoT deployments cater to. Our proposal does not make any assumptions on the capabilities of the devices - it can work with already deployed as well as new types of devices, while also conforming to a service-centric architecture. Even though our focus is on industrial IoT systems, the ideas presented here are applicable to IoT used in a wide array of applications. The goal of this position paper is to help raise awareness about network-centric approaches to IoT security.**

***Keywords—Industrial IoT, Embedded Systems, Security, SDN, NFV***

## I. INTRODUCTION

The Internet of Things presents the notion of large networks of connected devices, sharing data about their environments and creating a diverse ecosystem of sensor, actuators, and compute nodes. IoT networks are a departure from traditional enterprise networks in terms of their scale and consist of heterogeneous collections of resource constrained nodes that closely interact with their environment. Traditional methods of enterprise security—that rely on endpoint compliance, host based security, and frequent software patch management—are not viable in IoT networks. Instead, network security solutions must satisfy the unique requirements imposed by the nature of IoT devices and the environment that they operate in.

Scalable, connected, IoT networks have applications in a wide variety of industries, ranging from home automation, to healthcare, to industrial control systems. Consumers and producers alike are embracing IoT integration. For industry, initiatives to reduce production costs and increase efficiency pressure manufacturers to incorporate automation into their workflows; market competition and business analytics drive businesses to leverage IoT solutions [5]. Consumers, on the other hand, view IoT as an innovative commodity that allows them to interact with their world easily and continuously; information sharing and collaboration between people and devices drive consumers to leverage IoT solutions.

As IoT becomes pervasive in settings which previously didn't require hardened network security, such as home appliances, industrial infrastructure, and healthcare devices, security tends to be an afterthought while the ability to make data available on the network is prioritized. Security concerns for IoT networks are exacerbated by fast time-to-market development, resource limitations of the devices, and scale of IoT networks.

Product vendors often provide very limited security capabilities in IoT devices. Business demands for fast time-to-market and quick integrations are preferred over rigorous security measures built into devices. This lack of motivation to enforce and support features such as software integrity and updates, authentication protocols, and privacy measures for devices allows attackers to create wide-spread damage [2, 6]. This is exhibited in such cases as CANbus exploitation [8] that resulted in the recall of millions of vehicles and vulnerabilities in infusion pumps that could be accessed remotely through a hospital's network [1,9]. Additionally, consumers receive inadequate training on the security aspects of their devices. Default settings and passwords leave their devices open to attack, as evidenced by the recent influx of IoT botnets.. Recently, millions of IoT devices were hacked by using their default vendor passwords using an Internet worm called "Mirai"[4]. These hacked devices were then used as botnets to launch DDoS attacks against multiple targets.

Endpoint embedded systems devices have limited security features due to tradeoffs with size, weight, power, and cost requirements. Limitations imposed by device hardware and software are explored by Hossain et al in [3]. These constraints make costly computations, such as cryptographic algorithms, prohibitively expensive.

The scale of IoT networks, low on-device compute resources, and high expected longevity of "things"—especially

in the context of infrastructure systems such as energy grids and transportation—makes it difficult to keep devices patched through their lifecycle. As many of these devices are long-lived, initial security methods will become obsolete early in their lifecycle. The fast evolution of security threats and defensive security technologies exacerbates this problem.

Additionally, IoT devices provide an easier target to an attacker than traditional enterprise endpoints and an attractive foothold inside trusted networks to launch further attacks. The Open Web Application Security Project (OWASP) highlights 17 distinct attack surfaces introduced by IoT infrastructure; these attack surfaces range from physical device interfaces to network traffic to update mechanisms [7]. IoT networks create a system of interconnected devices; as complexity increases, one poorly secured device can cause cascading errors. It is not enough to consider only the security of endpoint devices – security must be considered at the network level.

In this paper, we refer to IoT deployments in industrial settings, military reconnaissance, and Cyber-Physical Systems (CPS), where the physical world is tightly integrated with the IT world as Industrial IoT. This is opposed to consumer IoT, which refers to deployments that are targeted for individuals or families (for example, Google's Nest Thermostat) that are typically deployed in homes. The devices used in Industrial IoT are often resource constrained and expected to be operational for years without any maintenance. Because of their longevity and resource constraints, proper device and security management agents are often unavailable. In addition, these devices are subject to harsh and insecure environments and may be vulnerable to device tampering and modifications. The devices used in consumer IoT typically do not suffer from the above-mentioned constraints. Consumer devices are also expected to be replaced every few years as compared to the devices that operate for decades without any supervision. The security requirements for Industrial IoT are stringent when compared to the consumer IoT; a failure in Industrial IoT system, such as failures in the Supervisory Control and Data Acquisition Systems (SCADA) deployed in power grids, could have devastating consequences. Another important difference is that security is often implemented in the cloud for consumer IoT systems. In many Industrial IoT systems, cloud access may not be feasible or preferred. Also, threats must be detected as early as possible to prevent damage of the mission critical systems, which favors security implementations at the edge rather than in the cloud.

The main goal of this paper is to provide evidence that the traditional approaches to security for IT systems are not effective for IoT systems, especially in the context of Industrial IoT systems. Traditional approaches, where the security is relegated to devices, fail in the above use-cases because of the very limited resources that are available in the IoT devices and the environment they operate in. These devices support diverse use-cases and typically do not implement a universal security policy or practice. We argue that by moving the security implementation point from the devices to the network, we can take advantage of the holistic view of the system available at the network without imposing any demands on the device capabilities. By relying on the recent developments in SDN and Network Function Virtualization (NFV) technology, we can dynamically change the security policies that are appropriate for different applications in an agile fashion.

The paper is organized as follows. In Section 2, we discuss the security implementations for common IoT systems. In Section 3, we discuss salient aspects of IoT traffic characterization and device fingerprinting. In Section 4, we present preliminary ideas that form the basis of our approach to tackle security challenges. The final section summarizes and concludes the paper.

## II. IoT Implementation---Security

In this section, a survey of existing and upcoming IoT solutions for both enterprise and home segments is presented. To highlight some of the security challenges of IoT, we first present the security implementation and gaps in these solutions. Finally, we highlight the need to implement a novel IoT security mechanism to overcome security gaps and vulnerabilities.

### *A. Survey of IoT Enterprise Solutions*

In the enterprise sector, Industrial Internet of Things (IIoT) relies on edge gateways that are designed for industrial protocols such as Modbus and industrial to Ethernet conversion protocols such as MQ Telemetry Transport (MQTT) [21]. Gateways generally integrate security functionality specific to the industrial protocols used, although they do not focus on RF-layer attacks. IIoT gateways are used to convert message protocols to interface disparate, often proprietary, networks. This interface allows industrial devices in one network to communicate with industrial devices in another network, but more commonly allows sensor-to-cloud integration. Analog data generated on edge devices can then be analyzed either by forwarding data directly to the cloud or by first processing data at the gateway and then sending aggregated data to the cloud.

The Intel IoT Gateway [29] is a reference design used by products from multiple hardware companies (e.g. Dell Edge Gateway 5000 Series, General Electric Predix). It uses the Wind River Intelligent Device Platform and McAfee Embedded Control security software. The Intel Gateway supports ZigBee radios and MQTT communications.

The Bayshore Networks IT/OT Gateway [30] uses deep content inspection and flexible policy configuration engine [31] to deliver and enforce policies across the industrial environment. This allows the gateway to selectively block network transactions between the Information Technology (IT) and Operational Technology (OT) networks based on content within industrial protocols. Though this gateway performs protocol translation for IoT traffic, it does not act as an RF hub for IoT devices and therefore cannot see the total end-to-end path of IoT traffic.

The IBM Forewind IoT Gateway [32] is a proof of concept gateway with cloud-based security analytics. It uses the IBM Libsecurity library [33] for a secure runtime environment and management interface. First-level analytics are prepared on the gateway with aggregated results passed up to the cloud for storage at regular intervals. When anomalies are detected (e.g. a sensor measurement outside of the expected range), the raw data for a specific sensor is sent to the cloud for further analysis.

In addition to IIoT gateways, there are existing enterprise solutions that target traffic as it transitions from the OT network onto the IT network. These enterprise segmentation products understand IIoT protocols and work as a behavior-based Intrusion Prevention System for IIoT traffic. They do not provide gateway services themselves and can only monitor traffic on wired networks. If, for example, a device that routinely sends MQTT traffic to a specific controller instead attempts to initiate an interactive login session with a payroll system, a behavior-based anomaly would be logged. Corrective actions such as blocking traffic from that device from continuing onto the IT network would subsequently take place.

Eunomic UnomicEdge [34] provides Software Defined Networking (SDN) based micro-segmentation of a network. It can isolate devices, applications, and users using dynamic OpenFlow rules based on a highly granular and flexible policy engine, which describes how network resources and organizational data can be accessed. UnomicEdge interfaces with both the OpenDaylight and ONOS SDN controllers, and supports MQTT and Modbus IoT communications protocols. This product is similar to the Bayshore product in design, with the novel application of SDN to enforce its traffic policy.

Cisco SecureOps [35] provides secure and controlled remote access to industrial networks and systems using centralized user management and role-based security profiles, all delivered as a service. It works in a DMZ between the IT and OT networks, analyzing Netflow data to find anomalies in the traffic to control access to OT devices.

ForeScout CounterACT [36] provides agentless detection and inspection of devices, including IIoT. It can enforce network access control to quarantine suspected compromised devices based on behavior. The ForeScout appliance can reconfigure network switches and routers, adding access control rules to allow or block traffic. There are potential scaling issues as the number of network switches and routers requiring reconfiguration grows.

### *B. Survey of IoT Home Solutions*

In home automation market, current focus is on monitoring traffic with cloud-based analytics. The home IoT gateway market is immature and a research study by Veracode asserts that existing IoT gateways have not included a focus on security monitoring [22]. Therefore, separate security appliances have been developed as stand-alone boxes, although newer entrants are merging their IoT monitoring with home Internet firewall appliances.

Security appliances in the IoT home segment mostly center around a subscription cloud-based security engine that offloads the analysis of IoT traffic from the local appliance. This reduces the performance requirements of the appliance and supports a continuing revenue stream for the appliance vendor. There is a growing list of entrants in this space, including F-Secure (SENSE) [37], Dojo-Labs (Dojo) [38], Cujo [39], Securify [40], Norton (Core) [41], and Untangle (at Home) [42]. Untangle has both hardware appliances and software-only solutions that each require a subscription to their cloud-based security engine.

### *C. IoT Frameworks*

An IoT framework can provide the foundation to build scalable, interoperable, and secure IoT networks. Many open IoT frameworks are in early stages of development, with few that have been standardized. Our assessment is that current frameworks value functionality and interoperability rather than security.

The International Telecommunication Union Telecommunication Standardization Sector (ITU-T) defined an IoT reference model in recommendation Y.2060 [23]. This model offers an abstract understanding of IoT architecture by dividing IoT into four layers: Application, Service and Application Support, Network, and Device. The ITU-T model focuses on the Device layer (which includes IoT devices and Gateways) with minimal depiction of the upper layers. The security requirements outlined in recommendations Y.4100 [24] and Y.4101 [25] follow the same layered approach where each layer manages a set of security functions similar to traditional enterprise network.

Cisco issued an IoT Reference model [26] for the IoT World Forum (IoTWF) and a whitepaper on IoT security framework [27]. The reference model provides a detailed breakdown of the IoT architecture resulting in seven layers compare to the four layers described in the ITU-T model. Fog Computing is introduced as a core architecture component to enable distributed intelligence close to IoT devices. The proposed security framework comprises of four components: Authentication, Authorization, Network Enforced Policy, and Secure Analytics. While network-centric approach such as anomaly detection from statistical analysis and predictive analysis is mentioned under Secure Analytics, the framework is still in development and concrete details on reference implementations are needed .

IoTivity [28] is an evolving open source framework for device-to-device connectivity. It provides a common platform and data model for different IoT devices. Within the framework, IoTivity uses a RESTful architecture, where resources (i.e. physical devices) are identified by Uniform Resource Identifiers (URLs). Constrained Application Protocol (CoAP) is used by IoTivity, which runs on top of UDP over IP. The core of IoTivity is divided into three parts: The Base Layer, the Resource Model, and the Service Layer. The Base Layer provides essential device-to-device communication including discovery, messaging and security. The resource model contains device profiles and are represented in combination format of RESTful API Modeling Language (RAML) and JavaScript Object Notation (JSON). Lastly, the Service layer provides higher level services including resource encapsulation, device management and notification. IoTivity supports unconstrained and constrained devices, where unconstrained devices use the full IoTivity stack and constrained devices only include the Base Layer and the Resource Model. The IoTivity stack provides transport layer security via Datagram Transport Layer Security (DTLS), authentication and access control. Being an interconnectivity

framework, network-centric security capabilities is out of the scope of the framework.

In the next section, we discuss how it is possible to extract unique characteristics of IoT traffic and fingerprint IoT devices and, how we can develop effective security solutions that take advantage of the profiles that can be built by using patterns available in the IoT traffic.

## III. IoT traffic And Device Characterization

IoT solutions use different wireless technologies to address application-specific requirements with regards to range and bandwidth. For example, ZigBee technologies are good solutions for residential IoT requirements, where low range (i.e. < 100 meters) communication are sufficient. On the other hand, LPWAN solutions such as LoRa [48], and SigFOX [49] may be better solutions for long-range industrial applications to avoid the use of repeaters and therefore reduce the size of the network.

IoT networks are envisioned not to only to connect "things" to the internet, but also to autonomously exchanges data among them. IoT traffic characteristics relies strongly on the surrounding environment and the application requirements. IoT systems can be categorized according to their applications to event-driven or scheduled events [46][47]. In an event-driven IoT system, traffic is generated when specific phenomena of interest (i.e. temperature, vibration) is detected and reported. On the other hand, the traffic generated by a scheduled event has a periodic traffic flow according to the detection and delivery periodicity configured by the network operators. Many IoT systems can be considered as a combination of event-driven and scheduled events systems. These IoT systems transmit data periodically during normal circumstances. However, bursts of traffic at much faster rates are generated on the occurrence of specific events. Examples of this type of IoT systems may include real time surveillance applications.

Typically, the traffic generated by IoT devices is deterministic and exhibits unique characteristics that can be utilized to identify them. For instance, many devices are expected to transmit a radio signal at a certain power level at a specific interval (for example, a static temperature sensor that transmits the temperature at a given location every hour). Also, the size of the information transmitted is known a priori. Any deviation from the expected behavior could be considered as an abnormality that can set off alarms. Similarly, the IoT devices also exhibit unique characteristics as supported by recent studies such as the MITRE Challenge [49]; these characteristics were leveraged to design policies that could identify security breaches and tampering of the devices deployed in industrial and military scenarios. It is important to note that the deterministic nature of the traffic and the a priori knowledge of the device fingerprints are typically not available in enterprise settings. But, IoT devices are typically microcontrollers designed to perform specific functions, such as light sensing. Each situational design provides contextual information on expected behavior; these behaviors can thus be utilized to detect anomalies.

By understanding traffic characteristics and device fingerprinting, security aspects of the network can be enhanced to detect events that diverge from the expected models. IoT system characterization can be extended to lower layers of the protocol stack (PHY and MAC) to enhance existing intrusion detection systems by relying on the uniqueness of IoT traffic and device characteristics.

In this paper, we propose a network centric approach for securing IoT networks. Our proposed solution will monitor and model events specific to IoT deployment scenarios and will implement policies at every layer of the IoT protocol stack to detect anomalies in the system. For instance, device RF fingerprint characterization can be used to detect attacks at the radio layer. After an attack is detected, MAC layer mitigation solutions such as blocking the radio channel can be executed by the IoT gateway. Another use case of the proposed solution is to detect traffic anomalies at the IP layer that differ from the expected traffic pattern of a specific IoT system. These anomalies may consist of unexpected change of packet size, packet inter-arrival rate, or destination-port. Upon detection of one or more of these anomalies, traffic policies may be executed. Traffic policies may consist of traffic redirection and port blocking. We envision a network function virtualization-based approach to implement policies at every layer that can be dynamically deployed using software-defined networking.

By profiling at every layer of the protocol stack based on the characteristics unique to IoT systems coupled with the dynamic deployment of security policies using SDN, our design improves on the frameworks discussed above. In the next section, we describe our design approach and system architecture for the IoT security gateway.

## IV. A Proposed Network-centric Approach to IoT Security

This section describes a network centric framework for securing IoT networks. Network connection are the vector behind most IoT security vulnerabilities; additionally, the network provides a channel through which attacks originating from IoT devices could be launched against the wider enterprise network infrastructure. By disrupting attacks that use a device's network connection, we expect to address challenges discussed in the earlier sections. However, it is possible to posit other scenarios where physical compromise of IoT devices leads to service disruptions. We argue that, given the scale of IoT deployments, physical attacks will be limited in scope relative to the attacks that traverse the network. Such vulnerabilities are addressed by building better security features in IoT devices, such as tamper resistant hardware and secure credentials storage. However, focusing exclusively on device security features is futile in the long-term as device longevity and patching difficulties lead to obsolescence of deployed security methods.

We argue that an ideal IoT security framework should protect devices over their lifecycle, scale to the network, and provide an extensible set of security functions that can be updated and revised independently. These characteristics point to a framework that relies on intelligence within the network to identify IoT devices, differentiate between normal and compromised behavior, and adapt network configurations.

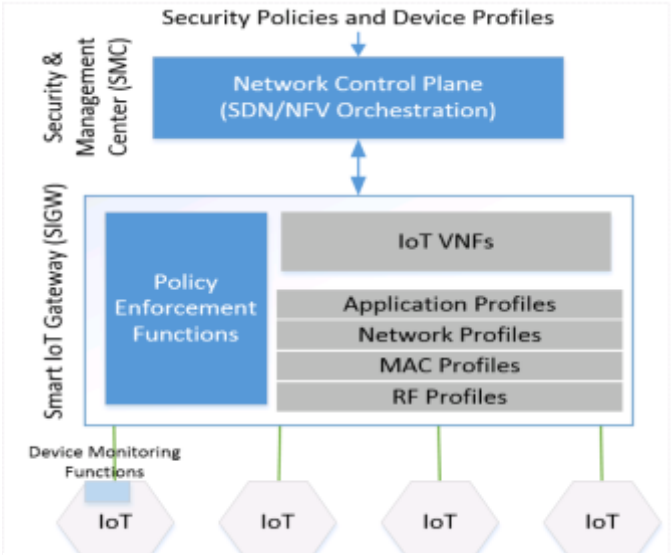


**Figure 1: NESES system architecture**

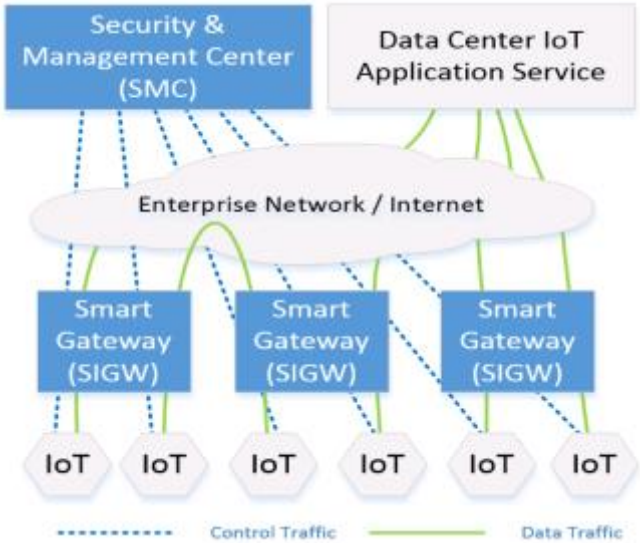


**Figure 2: Major components and traffic flows in NESES architecture**

Characteristics of IoT networks assist in to create such a framework. First, as shown in [44], IoT networks are typically deployed in a hub-spoke architecture with a local hub or gateway acting as the first hop. Second, purpose-built devices have well-defined functions, which facilitate fingerprinting of traffic profiles, and well-defined behaviors, which characterize normal states of operation. However, as IoT networks are reliant on Operational Technology network interfaces, fingerprinting and profiling functions need to be extensible to go beyond the traditional IP Intrusion Detection Systems (IDS) role and cover a variety of physical and MAC layer technologies.

### *A. Conceptual Design: Network Enabled Security for Embedded Systems (NESES)*

This section provides a high-level framework for securing IoT devices and embedded systems using NESES, Network Enabled Approach for Embedded Systems. This framework hinges on logical centralization of security policy management at a network control plane and distributed policy enforcement at smart IoT gateways.

As shown in Fig. 1, policy enforcement functions within the gateway interface with the entire protocol stack to enforce policies specific to the connected IoT devices. Policies will be downloaded from the Network Control Plane, which will contain a repository of policies and device signatures. The placement of the policy enforcement function at network edge is designed to increase the scalability of the system. The Policy Enforcement function at the gateway is also expected to utilize input from the Device Monitoring Functions that reside within IoT devices. Such monitoring functions could be used to periodically report metrics on device resource usage (e.g. power, CPU, memory) to ensure that the device is operating within normal parameters and has not been physically compromised. Other Virtual Network Functions (VNF) such as protocol translation functions, performance enhancing proxies, and encryption modules can be added to the gateway and configured via the policy enforcement function.

The NESES system, as diagrammed in Figure 2, has two major components: a logical centralized Security Management Control (SMC) and many distributed Smart IoT Gateways (SIGW). The SMC is responsible for managing all the security policies and the SIGW in the NESES system. It has a global, holistic view of the system and is aware of all SIGW capabilities, operation status, and connected IoT devices. The SMC is expected to be programmable so that operators can express policy intentions through abstract policy expression languages and define expected device profiles for the IoT devices. The SIGW consists of Policy Enforcement mechanisms in addition to standard gateway functions. The IoT gateway handles radio access and protocol stack translation. The Policy Enforcement Functions receive policy delegation from the SMC and perform access control and policy enforcement across the protocol stack. The SMC is a software solution; it could be deployed on a hardware appliance, or a virtual appliance in either private or public cloud. The SIGW is a hardware appliance deployed on the same site as the IoT deployment. SMC and SIGW communicate via a secured channel over either enterprise network or Internet.

## V. SUMMARY AND CONCLUSIONS

IoT security is a prominent research area because of the pervasiveness of IoT devices, long device lifecycle, and weak security methods currently used to protect them. This paper proposes an approach for securing large IoT networks using a network-centric security framework built on the recent advances in SDN/NFV technologies. This position paper contributes an overview of challenges in IoT security, presenting a brief survey of currently available methods of securing IoT networks and describes our proposed solution. The NESES framework is envisioned to scale to the size of IoT networks and extensible to cover heterogeneous use-cases and device types. This framework is expected to shift the focus of IoT security from patch management to proactive specification and enforcement of devices expected behavior throughout their lifecycle.

Our ongoing work is focused on prototyping and demonstrating the feasibility of NESES approach. We expect NESES to be oriented towards government, military, and large enterprise networks, which would benefit from the scalability of this approach and would have the infrastructure and resources for policy management. Areas of future work include the assessment of this approach to other sectors such as home automation and industrial settings.

## VI. Distribution Statement

Approved for Public Release; Distribution Unlimited. Case Number 17-1185.

## VII. References


[1] M. Asplund, and S. Nadjm-Tehrani. "Attitudes and Perceptions of IoT Security in Critical Societal Services." *IEEE Access* 4 (2016): 2130-2138.

[2] C. Warren Axelrod,. "Enforcing security, safety and privacy for the Internet of Things." *Systems, Applications and Technology Conference (LISAT), 2015 IEEE Long Island*. IEEE, 2015.

[3] M. Hossain, M. Mahmud, M. Fotouhi, and R. Hasan. "Towards an analysis of security issues, challenges, and open problems in the internet of things." *Services (SERVICES), 2015 IEEE World Congress on*. IEEE, 2015.

[4] B. Krebs. *Krebs on Security*, https://krebsonsecurity.com

[5] I. Lee, and K. Lee. "The Internet of Things (IoT): Applications, investments, and challenges for enterprises." *Business Horizons* 58.4 (2015): 431-440.

[6] R. Mahmoud, T. Yousuf, F.Aloul, and I. Zualkernan "Internet of things (IoT) security: Current status, challenges and prospective measures." *Internet Technology and Secured Transactions (ICITST), 2015 10th International Conference for*. IEEE, 2015.

[7] D. Miessler, and C. Smith. "OWASP Internet of Things Project." *OWASP Internet of Things Project - OWASP*. OWASP, 15 Feb. 2017

[8] C. Miller, and C. Valasek. "Remote exploitation of an unaltered passenger vehicle." *Black Hat USA* 2015 (2015).

[9] US Food and Drug Administration. "Cybersecurity Vulnerabilities of Hospira Symbiq Infusion System: FDA Safety Communication." *Retrieved* 2.23 (2015): 2016.

[10] F. Callegati et al., "SDN for dynamic NFV deployment," in IEEE Communications Magazine, vol. 54, no. 10, pp. 89-95, October 2016.

[11] S. S. Jung et al., "Attacking Beacon-Enabled 802.15.4 Networks," in Proceedings of the 6th International ICST Conference on Security and Privacy in Communication Networks, Springer Berlin Heidelberg, 2010.

[12] R. Sokullu, O. Dagdeviren, and I. Korkmaz, "On the IEEE 802.15.4 MAC layer attacks: GTS attack," in Proceedings of the 2nd International Conference on Sensor Technologies and Applications (SENSORCOMM '08), pp. 673–678, Cap Esterel, France, August 2008

[13] D. Cheriton.D and D.Faria "Detecting identity-based attacks in wireless networks using signal prints," in Proceedings of the ACM Workshop on Wireless Security (WiSe), September 2006.

[14] P. Jokar, N. Arianpoo and V. C. M. Leung, Spoofing prevention using received signal strength for ZigBee-based home area networks, IEEE SmartGridComm, 2013.

[15] IEEE Std. 802.15.4-2006, IEEE Standard for Information technology - Telecommunications and information exchange between systems – Local and metropolitan area networks - Institute of Electrical and Electronics Engineers, Inc., New York, September 2006.

[16] ZigBee Alliance, ZigBee Specification, 2009.

[17] K. Gill et al., ''A ZigBee-based home automation system,'' IEEE Trans. Consum. Electron., vol. 55, no. 2, pp. 422–430, May 2009.

[18] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," Comput. Netw., vol. 54, no. 15, pp. 2787–2805, 2010.

[19] J. Li and Q. Yang, "I'M A NEWBIE YET I CAN HACK ZIGBEE," in Def Con, Las Vegas, 2015.

[20] T. Zillner and S. Strobl, "ZigBee Exploited - The good, the bad and the ugly", Black Hat USA, Las Vegas, 2015.

[21] International Organization for Standardization, ISO/IEC 20922:2016 Standard, 2016.

[22] Veracode, "The Internet of Things: Security Research Study," White Paper, 2015.

[23] ITU-T Recommendation Y.2060, 2012-Overview of the Internet of Things

[24] ITU-T Recommendation Y.4100, 2014-Common requirements of the Internet of Things

[25] ITU-T Recommendation Y.4101, 2014-Common requirements and capabilities of a gateway for Internet of things applications

[26] "The Internet of Things Reference Model." IoTWF, 04-Jun-2014.

[27] "Securing the Internet of Things: A Proposed Framework", Cisco, 2017. [Online]. Available: http://www.cisco.com/c/en/us/about/security-center/secure-iot-proposed-framework.html.

[28] Iotivity.org, https://www.iotivity.org/.

[29] Intel Corporation, "Intel IoT Gateway Technology", https://www-ssl.intel.com/content/www/us/en/embedded/solutions/iot-gateway/overview.html

[30] Bayshore Networks, "Bayshore IT/OT Gateway", https://www.bayshorenetworks.com/products/it-ot-gateway/

[31] Bayshore Networks, "Bayshore SingleKey Policy Enforcement", https://www.bayshorenetworks.com/products/it-ot-gateway/bayshore-singlekey-policy-enforcement/

[32] R. Shmulik and D. Murik, "IoT Security", InterConnect 2016, Las Vegas, 2016.

[33] IBM Corporation, "libsecurity", https://developer.ibm.com/open/openprojects/libsecurity/

[34] Eunomic Networks, "UnomicEdge", \ http://www.eunomicnetworks.com

[35] Cisco Systems, "Cisco Secure Ops Solution", http://www.cisco.com/c/en/us/solutions/enterprise-networks/secure-ops-solution/index.html

[36] ForeScout Technologies, "ForeScout CounterACT", https://www.forescout.com/products/counteract/

[37] F-Secure, "F-Secure SENSE", https://sense.f-secure.com/us/

[38] Dojo Labs, "Dojo", http://www.dojo-labs.com/product/dojo/

[39] Cujo LLC, "Cujo",. https://www.getcujo.com

[40] Securify, "Securify", https://www.securifi.com

[41] Symantec Corporation, "Norton Core", https://us.norton.com/core

[42] Untangle, "Untangle at Home", https://www.untangle.com/untangle-ng-firewall/untangle-at-home/

[43] Tianlong Yu et al., Handling a trillion (unfixable) flaws on a billion devices: Rethinking network security for the Internet-of-Things, Proceedings of the 14th ACM Workshop on Hot Topics in Networks, p.1-7, November 16-17, 2015, Philadelphia, PA, USA.

[44] A.Sivanathan et al., A. Low-Cost Flow-Based Security Solutions for Smart-Home IoT Devices., IEEE Advanced Networks and Telecommunications Systems (ANTS), Nov 2016.

[45] Z. Qin et al., "A Software Defined Networking architecture for the Internet-of-Things," 2014 IEEE Network Operations and Management Symposium (NOMS), Krakow, 2014.

[46] I. Demirkol, F. Alagoz, H. Delic, and C. Ersoy, "Wireless sensor networks for intrusion detection: Packet traffic modeling," IEEE Communications Letters, vol. 10, no. 1, pp. 22–24, January 2006.

[47] Q. Wang and T. Zhang, "Source traffic modeling in wireless sensor networks for target tracking," in Proc. of the 5th ACM International Symposium on Performance Evaluation of Wireless Ad-Hoc, Sensor, and Ubiquitous Networks (PEWASUN' 08), pp. 96–100, October 2008.

[48] LoRa Alliance, "Lorawan specification," Jan. 2015.

[49] Sigfox. [Online]. Available: http://www.sigfox.com/en/

[50] The MITRE IoT Challenge, https://www.mitre.org/research/mitre-challenge/mitre-challenge-iot