Security as a Service: Real-time Intrusion Detection in Internet of Things

Shiven Chawla

University of Washington Bothell
Computing and Software Systems
Bothell, WA
chawls@uw.edu

Geethapriya Thamilarasu*

University of Washington Bothell
Computing and Software Systems
Bothell, WA
geetha@uw.edu

ABSTRACT

With the increase in number of Internet connected devices, security and privacy concerns are the major obstacles impeding the widespread adoption of Internet of Things (IoT). Securing IoT has become a huge area of concern for all, including the consumers, organizations as well as the government. While attacks on any system cannot be fully prevented forever, real-time detection of the attacks are critical to defend the systems in an effective manner. In this paper, we propose a novel intrusion detection system that uses machine learning algorithms to detect security anomalies in IoT networks. This detection platform provides security as a service and facilitates interoperability between various network communication protocols used in IoT. In this paper, we provide a framework of the proposed system and discuss the intrusion detection process in detail.

KEYWORDS

Security, Internet of Things (IoT), Intrusion Detection System (IDS), Machine Learning

1 INTRODUCTION

Internet of Things promises to be the next big technological revolution connecting everything from refrigerators, thermostats and toasters to the Internet [4, 10, 13]. Gartner predicts that nearly 21 billion devices will be connected to the Internet by the year 2020 [3]. Despite increased consumer interest, constantly emerging applications, and multi-million-dollar investments, deployment of Internet of Things is shadowed by looming security concerns [1, 9, 15, 16]. IoT devices are manufactured and shipped often without proper security controls in place. Recent HP research report on IoT devices demonstrates that a large percentage of these devices in market have security flaws and vulnerabilities that can be easily exploited by hackers. The scale and complexity of the IoT networks magnifies the current security threats to the Internet. Hackers can turn deceptively simple devices such as smart hubs, TVs, and cameras into dangerous weapons running malicious code and create a massive network of bots (Botnet) to launch a massive cyberattack. Recent

evidence of this was observed in October 2016 where hacked cameras and DVRs created massive Internet outage and disrupted the availability of popular websites such as Twitter, Amazon and Netflix [6].

The rising growth in the number of IoT devices results in large attack surfaces. However lack of a well-established infrastructure and limited computational and power resources pose serious challenges to the security solutions. While researchers are starting to address the security flaws and vulnerabilities in the IoT devices, most of these solutions are preventive in nature. Traditional cryptographic security solutions cannot be applied to embedded devices in IoT due to their limited resource constraints and computational capabilities. Security solutions that can provide real time attack detection and mitigation are in demand. Recent efforts in IoT security towards detecting attacks are mostly focused on rule-based detection techniques that are well known for their weaknesses and limitations in detecting novel attacks [8, 11, 12]. The goal of our research is to address this security gap by implementing a novel intrusion detection system to complement the preventive security solutions and provide a comprehensive security for IoT systems. Our proposed mechanism differs from the existing research on IDS in IoT by overcoming the weaknesses of traditional signature/rule based techniques in detecting intrusions.

In this paper, we propose to develop an independent Integrated Intrusion Detection system (IID) to provide security as a service for personal area IoT networks. The proposed system uses machine learning based anomaly detection technique to thwart and detect the various security attacks on IoT networks.

2 RELATED WORK

With an increased number of IoT devices and their proliferated ability to collect data, IoT deployment faces a number of challenges including scalability, reliability, privacy, and security [5, 10, 17]. Recent security incidents such as the ransomware against thermostats, tea-kettle attack against car-locks and baby monitor hacks demonstrate that security attacks on IoT devices are continually increasing. Security research community is actively exploring various techniques and solutions to address the various threats and vulnerabilities in this domain. With the rise of sophisticated attackers who are able to overcome even the best security protection measures there is an increasing shift towards minimizing the impact of intrusions in addition to preventing them. Kai Zhao *et.al* proposed to encrypt the data at the perception layer, and implement an IDS at the network layer to identify suspicious activities within an IoT network[19].

*The corresponding author

This work is licensed under a Creative Commons
Attribution-NonCommercial International 4.0 License.

CyberSec '18, April 9–11, 2018, Coeur d'Alene, ID, USA
© 2018 Copyright held by the owner/author(s).
ACM ISBN 978-1-4503-6406-5/18/04.
<https://doi.org/10.1145/3212687.3212872>

Kasinathan *et.al* proposed a rules-based IDS framework designed for the 6LoWPAN networks[8]. In this work, dedicated probe nodes within the host 6LoWPAN network use rule based detection to detect DoS attacks [8]. This system however requires the rules database to be updated frequently. Le *et.al* also proposed use of different types of available rules-based intrusion detection system to address three quality-of-service related security threats such as rank-attack, local repair attack, and the resource-depletion attack [12]. Krimmling *et.al* proposed a modular IDS framework using rule based detection technique for securing Smart City IoT networks using the Constrained Application Protocol (CoAP) [11]. Although, their framework is lightweight, the proposed solution is limited to mitigating only the routing attacks. Also, due to the poor performance of their solution, the authors conclude that a hybrid approach towards intrusion detection, involving both the rule-based and the anomaly based intrusion detection can result in a better performance. Raza *et.al* proposed an intrusion detection system, known as SVELTE, for IoT networks based on 6LoWPAN protocol [14]. Although, SVELTE used a hybrid of signature detection and anomaly detection based approach to perform intrusion detection, the system is mainly designed to detect routing attacks such as sinkhole attack, and the selective-forwarding attacks. Zhao *et.al* proposed an intrusion detection for IoT networks installed in coal mine disaster warning systems, using the Back-Propagation Neural Networks (BPNN) and Immune Algorithm (IA)[18]. Although, their IDS has a high accuracy rate, it requires a long period of training (9 weeks) to achieve these results. BPNN algorithm used in this system is computationally intensive and cannot be implemented in a low-powered device. Arrington *et.al* proposed using behavioral modeling in a smart home environment to detect anomalies related to non-playing characters such as human beings in a smart home environment[2]. The behavioral model proposed in this system becomes more complex with the growth of the IoT network, eventually becoming resource-consuming, and heavy on system performance. Hodo *et.al* proposed an artificial neural network based intrusion detection system to detect distributed denial of service (DDoS) attacks on IoT devices by supervised training of a perceptron. In this work, perceptron to work as both host based IDS, and the network based IDS, using statistical analysis, signature-based intrusion detection and protocol verification. The technique focused mainly on detecting DDoS attacks [7].

In this work, we address the problem of lack of an anomaly based intrusion detection system for Internet of Things environment. To this end, we propose a peer-to-peer, spatially independent, and artificially independent intrusion detection system for IoT networks, developed over low-powered resource-constrained devices.

3 PROPOSED INTRUSION DETECTION SYSTEM FOR IOT

In this paper, we propose an independent integrated intrusion detection (IID) system to provide on-demand security as a service to the host network. The primary goal of this system is to provide anomaly based intrusion detection solution for Internet of Things. We assume that the IIDs will themselves be immune to attacks, as

they only establish hidden and passive connections with the IoT devices for a very short duration. In this section below, we discuss the framework for the proposed intrusion detection system in detail.

3.1 System Architecture

Figure 1 presents the intrusion detection system architecture for a personal area IoT network. As shown in the diagram, an IID system can easily be integrated into any network by placing the device within the coverage area of the router and other IoT devices within the network. The IID device works primarily on the transport layer abstraction level and can secure both the ingress traffic (coming into the host IoT network) as well as the exiting traffic (leaving the host IoT network) based on their placement. The IID uses network virtualization to connect to the router, the IoT devices, or the Internet. While other intrusion detection systems commonly rely on the router for data gathering, our system works independently by promiscuous monitoring and analysis of the network traffic.

Figure 1: Intrusion Detection System Overview

Unlike present-day network intrusion detection systems which are mostly hierarchical and distributed middleware software systems, the proposed detection system is peer-to-peer (P2P) and consolidated. The proposed system does not enforce any limitations on a specific network topology and can easily adapt across different network topologies. Due to the varied nature of IoT devices and their corresponding digital communication protocols, a unified intrusion detection system model is challenging in these environments. To enable intrusion detection across the different network topologies and protocols, we design the IIDs to establish different types of network channels with different IoT devices separately. This system thus provides interoperability among the various IoT ecosystems.

Figure 2: IDS Detection Process

3.2 Components of Detection System

The proposed IDS comprises of three phases namely, the Network Connection Phase, Anomaly Detection Phase and the Mitigation Phase.

3.2.1 Network Connection Phase. During the network connection phase, the host network is probed to determine the network protocols that are currently in use and to establish connectivity using virtual network channels. The components of this phase are:

- **Connection Prober:** The connection prober module is responsible for sending probe-signals and broadcast beacons to all the devices within the host IoT personal area network. On receiving a handshake or a session request, the connection prober module translates the data-packet into the appropriate network protocol.
- **Virtual Network Client:** The VNC module is a client based network emulator responsible for establishing compatible network channels with various IoT devices after gathering information about their network protocols. VNC module transforms the network packets from different network channels and switches the network protocol according to a specific IoT device.
- **Controller :** The Controller module is responsible for controlling and interfacing the exchange of data-packets or commands between the Data Collection & Transformation module and the VNC module. All the modules other than Connection Prober and VNC module are autonomous and not governed by the Controller module.

3.2.2 Anomaly Detection Phase. In Anomaly detection phase, data packets are collected and transformed to be fed into the machine learning module. This module enables highly-optimized data collection and transformation technique allowing the IIDs to be developed on low-powered, resource-constrained hardware, unlike existing IDSs which require dedicated and specialized hardware setup at the gateway of host networks. The components of this phase are described below.

- **Data Collection and Transformation (DCT):** DCT module is responsible for stripping the data-packets, extracting the header tags as features, populating the cached database and feeding these tuples into Machine-Learning based Anomaly Detection module. The proposed data collection, and transformation technique has the advantage of reduced size of the collected network traffic which permits the IID to be placed anywhere within the coverage area of the host network to function inaudibly. Thus, IID is not required to be placed at the edge of host network anymore.
- **Machine-Learning based Anomaly Detection (MLAD):** MLAD module comprises of the machine-learning engine that is responsible for differentiating the benign tuple from the malicious tuple. If the detection module observes an anomalous behavior and has a decision trigger associated with the tuple, it activates the Actuator module for further action. Otherwise, it triggers the Trainer module which requires human intervention for further training the learning module.

- **Trainer:** This module is invoked when MLAD is required to train for an unknown tuple and it requires human intervention.

3.2.3 Mitigation Phase. This phase is responsible for mitigating the attack and initiating a proper response. The Handler component in this module is responsible for executing the mitigation response if flagged by the Actuator module.

3.3 Detection Mechanism

Figure 2 illustrates the detailed detection process flow of the various soft-component modules developed on the independent mobile processing and sensing unit (IID). During the Network connection phase, the IID probes host network to detect the various protocols used for communication by the IoT devices within the host network. After identifying the various communication protocols, the IID uses virtual network-channels to establish connectivity with all the devices in the hosts' personal area network. Virtual Network Connection (VNC) module lists all the virtual network channels required to monitor the host network, and then triggers a connection-successful flag to IIDs Controller module, signifying successful mapping of network demographics. The IID then enters the Anomaly Detection phase during which the VNC module continues to capture the real-time network-traffic from the host PAN. Once the IID enters Anomaly Detection phase, the Data Collection and Transformation (DCT) module is activated and the real-time network traffic is captured from the host network by the VNC module. The DCT module in parallel, strips the received data-packets, extract various tags from their headers, and populates the database with the extracted header-tags. The DCT module is also responsible for transmitting the transformed data-tuples from the database to the Machine-Learning based Anomaly Detection module. The learning module either classifies the input tuple as benign or anomalous, or triggers the Trainer module if it cannot make a decision. If the tuple is classified as malicious, the learning module activates the Actuator module. When the learning module activates the Actuator module, IID enters, the Mitigation phase which is responsible for mitigating the intrusion and providing an active response.

3.3.1 Machine Learning based Anomaly Detection. In our machine learning module, we employ deep learning algorithms to identify attacks. Specifically, our framework uses a 5-layer artificial deep learning model that comprises of one input layer, three hidden layers, and one output layer. The input contains 56 nodes that represent a total of 56 features received from the data collection and transformation module. Each hidden layer uses the data from the previous layer as input and filters the most significant features. The third hidden layer also acts as a soft-max layer and fine tunes the results to classify the attack. The output layer contains two nodes to represent the network traffic into malicious and benign categories. This layer uses the information from the third hidden layer and outputs the classification result.

4 CONCLUSION AND FUTURE WORK

In this paper, we proposed an intrusion detection security framework to provide autonomous and integrated security service to the

consumers of IoT networks. Specifically we developed the framework for an independent intrusion detection device that uses machine learning algorithms to detect anomalous network behaviors. As the system can be integrated into any network, we are able to achieve smart connectivity with smart security helping us realize the vision of secure ubiquitous computing. We are currently developing a prototype IID to test our detection modules against a number of security attacks specific to IoT. Future work also includes evaluating and further strengthening the machine learning detection module to enable more accurate identification of anomalies in an IoT network.

REFERENCES

- [1] M. Abomhara and G. M. Koien. 2015. Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks. *Journal of Cyber Security and Mobility* (Jan. 2015).
- [2] B. Arrington, L. Barnett, R. Rufus, and A. Esterline. 2016. Behavioral Modeling Intrusion Detection System (BMIDS) Using Internet of Things (IoT) Behavior-Based Anomaly Detection via Immunity-Inspired Algorithms. In *2016 25th International Conference on Computer Communication and Networks (ICCCN)*.
- [3] Gartner. 2015. IoT Connected Devices to Triple to Over 38Bn Units - Juniper Research. <http://www.informationweek.com/mobile/mobile-devices/gartner-21-billion-iot-devices-to-invade-by-2020/d/d-id/1323081>. (2015).
- [4] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami. 2013. Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems* (Sept. 2013).
- [5] T. Heer, O. Garcia-Morchon, R. Hummen, S. L. Keoh, S. S. Kumar, and K. Wehrle. 2011. Security Challenges in the IP-based Internet of Things. *Wireless Personal Communications* (Sept. 2011).
- [6] S. Hilton. 2016. Dyn Analysis Summary Of Friday October 21 Attack | Dyn Blog. (2016). <http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/>
- [7] E. Hodo, X. Bellekens, A. Hamilton, P. L. Dubouilh, E. Iorkyase, C. Tachtatzis, and R. Atkinson. 2016. Threat analysis of IoT networks using artificial neural network intrusion detection system. In *Networks, Computers and Communications (ISNCC), 2016 International Symposium on*. IEEE.
- [8] P. Kasinathan, G. Costamagna, H. Khaleel, C. Pastrone, and M. A. Spirito. 2013. DEMO: An IDS Framework for Internet of Things Empowered by 6LoWPAN. In *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*. ACM.
- [9] A. Khan. 2016. Overview of Security in Internet of Things. *3rd International Conference on Recent Trends in Engineering Science and Management* (April 2016).
- [10] R. Khan, S. U. Khan, R. Zaheer, and S. Khan. 2012. Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges. In *2012 10th International Conference on Frontiers of Information Technology (FIT)*.
- [11] J. Krimmling and S. Peter. 2014. Integration and evaluation of intrusion detection for CoAP in smart city applications. In *2014 IEEE Conference on Communications and Network Security (CNS)*.
- [12] A. Le, J. Loo, A. Lasebae, M. Aiash, and Y. Luo. 2012. 6LoWPAN: a study on QoS security threats and countermeasures using intrusion detection system approach: IOT, 6LoWPAN, RPL, QOS SECURITY THREATS, IDS. *International Journal of Communication Systems* (Sept. 2012).
- [13] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac. 2012. Internet of things: Vision, applications and research challenges. *Ad Hoc Networks* (Sept. 2012).
- [14] S. Raza, L. Wallgren, and T. Voigt. 2013. SVELTE: Real-time Intrusion Detection in the Internet of Things. *Ad Hoc Networks* (Nov. 2013).
- [15] R. Roman, J. Zhou, and J. Lopez. 2013. On the features and challenges of security and privacy in distributed internet of things. *Computer Networks* (July 2013).
- [16] S. W. Shieh. 2016. Emerging Security Threats and Countermeasures in IoT. *ACM Asia Conference on Computer and Communications Security* (Aug. 2016).
- [17] T. Xu, J. B. Wendt, and M. Potkonjak. 2014. Security of IoT Systems: Design Challenges and Opportunities. In *Proceedings of the 2014 IEEE/ACM International Conference on Computer-Aided Design*. IEEE Press.
- [18] J. W. Zhao, Y. Hu, L. M. Sun, S. C. Yu, J. L. Huang, X. J. Wang, and H. Guo. 2013. Method of choosing optimal features used to Intrusion Detection System in coal mine disaster warning internet of things based on Immunity Algorithm. *CRC Pr I Llc*.
- [19] K. Zhao and L. Ge. 2013. A Survey on the Internet of Things Security. In *2013 9th International Conference on Computational Intelligence and Security (CIS)*.