Pulse: An Adaptive Intrusion Detection for the Internet of Things

Conference Paper · May 2018

DOI: 10.1049/cp.2018.0035

CITATIONS
114

READS
2,604

3 authors, including:

Eirini Sofia Anthi
Cardiff University
24 PUBLICATIONS **562** CITATIONS
SEE PROFILE

Lowri Williams
Cardiff University
10 PUBLICATIONS **509** CITATIONS
SEE PROFILE

Pulse: An Adaptive Intrusion Detection for the Internet of Things

Eirini Anthi, Lowri Williams, Pete Burnap*†

**School of Computer Science and Informatics, Cardiff University*

Keywords: Internet of Things, Intrusion Detection, Machine Learning.

Abstract

The number of diverse interconnected Internet of Things (IoT) devices keeps increasing exponentially, introducing new security and privacy challenges. These devices tend to become more pervasive than mobile phones and already have access to very sensitive personal information such as usernames, passwords, etc., making them a target for cyber-attacks. Given that smart devices are vulnerable to a variety of attacks, they can be considered to be the weakest link for breaking into a secure infrastructure. For instance, IoT devices have recently been employed as part of botnets, such as *Mirai*, and have launched several of the largest Distributed Denial of Service (DDoS) and spam attacks in history. As a result, there is a need to develop an Intrusion Detection System (IDS) dedicated to monitor IoT ecosystems, which will be able to adapt to this heterogeneous environment and detect malicious activity on the network. In this paper, we describe the initial stages of developing Pulse; a novel IDS for the IoT, which employs Machine Learning (ML) methodologies and is capable of successfully identifying network scanning probing and simple forms of Denial of Service (DoS) attacks.

1 Introduction

The term Internet of Things (IoT) refers to a things-connected ecosystem, where electronic devices are wirelessly connected via various smart sensors [9]. These devices, work without human intervention and continuously exchange data. IoT devices such as smart meters, sensors, chargers, tools, electrical vehicles, wearable devices, provide various functionalities which automate and support our daily activities and needs.

The proliferation in current technologies is the driving force behind the development of an interconnected knowledge-based world; our economies, societies, machinery of government, and Critical National Infrastructure (CNI) [12]. In particular, CNI concepts such as smart homes, smart cities, intelligent transport, smart grids, and health care are heavily dependent on smart technologies and Internet of Things (IoT) devices. Although CNI concepts support the tasks of everyday life, their dependency on Information Communication Technology (ICT) and IoT devices come with tremendous security risks. High severity security attacks to CNI concepts, such as data leakage, spoofing, disruption of service (DoS/DDoS), energy bleeding, insecure gateways, etc., target sensitive information/data [1], can disrupt the system availability and energy resources, can cause system blackouts and also other indiscriminate and long-lasting damage. The effects of these security issues may cause major interference to the operation of services (e.g. public transportation networks can be targeted to cause chaos during peak travel periods, attacks to power grids can result in wasting huge amounts of energy and a possible blackout of the system, etc.) and therefore, require immediate attention.

Our work focuses on developing a novel model that can predict malicious behaviour and detect malicious IoT nodes on a network. More specifically, the model consists of two components. The first component is based on a Machine Learning (ML) approach which learns the networking behaviour of the IoT-based network. The second component is a rule based approach which is established from a security policy configured by the network administrator. The combination of both components creates an adaptive and flexible model, which will allow us to accurately predict malicious activity and prevent security attacks on such systems.

This paper is organised as follows: Section 2 focuses on the related work, Section 3 describes the attack vectors in an IoT ecosystem, Section 4 discusses the different types of IDSs, Section 5 presents the architecture of Pulse, Section 6 discusses our methodology, Section 7 presents the results, and finally Section 8 discusses our proposals of future work.

2 Related Work

2.1 IDSs for Wireless Sensor Networks and Traditional IT

Currently the majority of the available IDSs are designed for either Wireless Sensor Networks (WSNs) or the conventional IT infrastructure. However, none of these systems fit the specifications of the IPv6 connected IoT devices. In the first case, although WSNs are the predecessors of IoT and are considered to be a subset of IoT, they have significant architectural differences. As a result, these IDSs cannot be applied in an IoT ecosystem [2]. On the other hand, IDSs designed for traditional IT systems have not considered the scale, heterogeneity, use cases, or device/vendor constraints that come in an IoT ecosystem.

More specifically, the traditional IT security ecosystem consists of static perimeter network defences (e.g. firewalls, IDS), end-host defences (e.g. anti-virus), etc., that can not handle IoT deployments [16]. Moreover, the diversity of IoT devices and their vendors means that traditional approaches of discovering attack signatures (e.g. honeypots), will be insufficient or non scalable [16]. Popular IDSs for traditional IT such as SNORT and Bro only work on conventional IP-only networks [16], they are not adaptable, and they are applicable only to a single platform/protocol. Therefore, there is a need to implement new mechanisms that will be able to adapt and learn signatures in such large scale heterogeneous ecosystems.

2.2 IDSs for IoT

Other recent studies have recently attempted to develop IDSs tailored to the needs of IoT networks. For instance, [13] have proposed a lightweight, hybrid, and centralised approach that successfully detects Hello Flood and Sybil attack in IoT networks. Pongle and Chavan [8] developed a centralised and distributed architecture, based on simulations, to detect the Wormhole attack. Furthermore, Razza et al. [10] implemented a real-time IDS for the IoT called SVELTE. This system has three main components and its results in detecting various attacks seem promising. Jun and Chi [4], proposed an event processing based IDS for the IoT. This system is designed based on the Event Processing Model (EPM) and is mainly a rule-based IDS. Nevertheless, all the above come with limitations such as they only address specific attacks, they are rule-based and as a result they are not adaptable, or they are based on simulations and have not been validated against a real IoT environment.

3 Cyber Attacks in IoT ecosystems

Studies [15, 7] have shown that IoT devices are vulnerable to various attacks. Some of the reasons that make these devices insecure are: limitations in computational power, lack of transport encryption, insecure web interfaces, lack of authentication/authorisation mechanisms, and of course heterogeneity, as it makes applying security mechanisms uniformly in IoT devices extremely challenging. Below we discuss few of the most popular attacks to which IoT are vulnerable:

- **Denial of Service (DoS) Attack** [5]: During this attack, the devices/resources are no longer available to legitimate users. When multiple nodes on the network take part in such an attack then it is called Distributed Denial of Service (DDoS). This attack affects network resources, bandwidth, CPU, etc.
- **Hello Flood Attack**: In an IoT network, a routing protocol broadcasts a hello message in order to declare its presence to its neighbour nodes. An attacker can forge such a message and send it to a device, in order for it to recognise that a device is within range and add it in its neighbour node list.
- **Sybil Attack** [17]: During this attack, a node appears to have multiple identities. The routing protocol, the detection algorithm, and co-operation processes can be attacked by this malicious node.
- **Sinkhole Attack** [14] : During this attack, a malicious IoT node will attempt to attract all the network traffic from its neighbour nodes towards it.

4 Types of IDSs

IDS, regardless of the environment they are designed to be employed (e.g. conventional IT, IoT, WSN, etc.), are built based on the same concept [11]. A data collection module collects data from the network, an analysis module processes the collected data and is looking to identify attacks, and finally an attack reporting mechanism notifies the network administrators. The main differences amongst the IDS lie in their implementation approaches and the chosen techniques associated with it such as [6]: **Data source**: host-based, network-based, hybrid, **Detection Method**: signature-based, anomaly-based, **Time of Detection**: offline, online, **Architecture**: centralised, distributed, **Networking Type**: wired/wireless, ad-hoc, etc.

More specifically, host-based IDSs run on the host device and usually require software to operate as opposed to network-based that perform their task by analysing network traffic. Signature-based method of detecting attacks, analyse the network traffic and try to recognise patterns of already known attacks/abnormalities. Although this method is considered to be very simple to implement and it is very accurate, it is not efficient in detecting unknown attacks. Finally, anomaly-based techniques firstly built a baseline of normal behaviour of networking features and then monitor the traffic to identify any unusual behaviours.

5 Pulse

The purpose of this research is to develop Pulse; a novel predictive and adaptive IDS system tailored for IoT ecosystems. Our proposed model, is a real-time network-based, both signature and anomaly-based detection system. It is built in two phases. During phase one an IoT smart-home testbed was built and we monitored its benign network activity, in order to create a baseline of normal network behaviour for each of the devices connected on the network. In the second phase, various attacks and other malicious operations such as network scanning etc., were deployed on the same network whilst the network traffic was still recorded. These two phases generated two data-sets, one with benign network traffic and one with malicious. Following the data collection process, we built a Machine Learning (ML) model which is the core of the proposed IDS. Specifically, to train our model, we used supervised ML algorithms. This model is able to recognise abnormalities on the network traffic, even when unknown attacks are being deployed on the network for the first time. Additionally, it is also able to learn over time, increasing Pulses accuracy to detect attacks. The

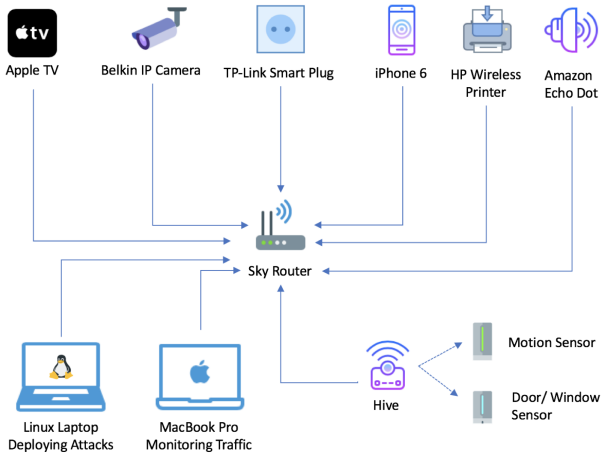

Fig. 1: IoT Smart home testbed consisting of various commercially available IoT devices.

last component of our system is a rule-based algorithm. This algorithm consists of various rules, which will be used in combination with the outcome that the ML model will produce. We anticipated that this would increase the accuracy of the overall prediction.

6 Methodology

6.1 IoT Smart Home Testbed

In order to initiate the development of Pulse, we built a smart home based IoT testbed. This was necessary for two reasons; (a) in order to collect data from real IoT devices and (b) to create a realistic environment which will allow us to evaluate the feasibility of our system. The IoT testbed that we built, consisted of a range of commercially relevant and representative IoT hardware. Such devices included a TP-Link NC200 IP camera, the Hive which was connected to two sensors; a motion sensor and a window/door sensor, a TP-Link Smart Plug, an Apple TV, an HP wireless printer, and an Amazon echo. Additionally, on the same network there were connected two traditional IT devices. One of them constantly recorded the network traffic and automatically generated and saved the log files. The other machine was used to deploy various attacks. Figure 1 displays the smart home testbed setup that we used for our experiments.

6.2 Generating Data

In order to generate the two data-sets; one with benign network traffic and one with malicious, to train the ML model of our system we monitored the network traffic on the IoT testbed for four consecutive days using the software *Wireshark*. For the first two days, we recorded and observed how the network operated under normal conditions. For the next two days, we randomly deployed attacks while the traffic was still being recorded. More specifically, we focused on performing various types of network probing/scanning using *Nmap* such as Quick Scan, Ping Scan, Regular Scan, and Intense Scan. The reasons why we decided to include these diverse scans in our attack vector are; (a) these scanning techniques differ in their intensity and in the information they gather (some are more detailed than others) (b) network scanning is the first course of action that any botnet perform in order to attack IoT devices. That is because they are looking to identify the network devices in range, which ones of them have open ports, what operating system they are using, etc. For our initial experiments, we also considered simple versions of DoS attacks such as SYN and UDP Flood Attacks.

6.3 Machine Learning Model

We aimed to create an IDS that will automatically learn its ecosystem, learn what is normal behaviour and what it is not using machine learning.

More specifically, the data log generated in Section 6.2 formed the basis for the feature vectors used to perform classification experiments. These feature vectors consisted of: the time of the attack, the destination IP address of the devices, the protocols used, and the size of the packets transmitted, and were subsequently amended with their class label, i.e. whether they were benign or malicious. We decided to focus on the above features based on previous studies that attempted to identify anomalies on the network traffic in traditional IT ecosystems .

Given that our dataset was unbalanced, we used Wekas inbuilt function to sub-sample an even number of both classes. We performed our classification experiments by using Weka [3], a popular suite of ML tools. In order to determine the best classification model for this case, we performed 10-fold cross-validation experiments by applying a variety of classifiers distributed as part of Weka. A Nave Bayes classifier outperformed other methods. Consequently, we report the results achieved by this method here, evaluating its classification performance in terms of precision, recall and F-measure.

7 Results

The results from our initial experiments demonstrated that our model was effective at identifying network probing and SYN/UDP flood attacks. Table 1 displays in detail the results:

Attack	Precision	Recall	F-Measure
Quick/Quick Plus scan	97.7	97.7	97.7
Regular/ Intense scan	95.5	95.5	95.5
SYN Flood	80.8	68.8	65.8
UDP Flood	81	68.8	65.8

The results show our model is better at detecting probing attacks than it is for flood-type attacks. In particular the drop in recall for flooding as opposed to scanning shows around a third of attacks were missed. Nevertheless, the initial experiment demonstrates utility in using these data for this problem

and in future we will use more theoretical reasoning to devise new features that represent network behaviours and enable to reason around the effective behaviours to monitor for attack detection in diverse IoT environments. By enhancing these features beyond packet metadata, we expect the classification performance to increase with the number of false negative reduced..

8 Future Work

Although our results are very promising there are still a lot of elements and parameters that we need to consider to fully develop Pulse. To begin with, we need to consider clustering homogeneous devices together and deriving a normal traffic behaviour for every cluster. This will aid detecting abnormalities more accurately on network and also detecting malicious nodes. Furthermore, we need to perform significantly more attacks, and specifically focus on the ones mentioned earlier on in the paper. Additionally, we would like to also consider other features for the ML training such as Payload, Ingoing/Outgoing ratio, etc. Finally, we need to develop the rule-based algorithm, which we mentioned in the generic architecture of Pulse, but we havent yet included in our experiments.

References

[1] Eirini Anthi, Amir Javed, Omer Rana, and George Theodorakopoulos. Secure data sharing and analysis in cloud-based energy management systems. In *Cloud Infrastructures, Services, and IoT Systems for Smart Cities*, pages 228–242. Springer, 2017.

[2] Ashfaq Hussain Farooqi and Farrukh Aslam Khan. Intrusion detection systems for wireless sensor networks: A survey. *Communication and networking*, pages 234–241, 2009.

[3] Mark Hall, Eibe Frank, Geoffrey Holmes, Bernhard Pfahringer, Peter Reutemann, and Ian H Witten. The weka data mining software: an update. *ACM SIGKDD explorations newsletter*, 11(1):10–18, 2009.

[4] Chen Jun and Chen Chi. Design of complex event-processing ids in internet of things. In *Measuring Technology and Mechatronics Automation (ICMTMA), 2014 Sixth International Conference on*, pages 226–229. IEEE, 2014.

[5] Prabhakaran Kasinathan, Claudio Pastrone, Maurizio A Spirito, and Mark Vinkovits. Denial-of-service detection in 6lowpan based internet of things. In *Wireless and Mobile Computing, Networking and Communications (WiMob), 2013 IEEE 9th International Conference on*, pages 600–607. IEEE, 2013.

[6] Daniele Midi, Antonino Rullo, Anand Mudgerikar, and Elisa Bertino. Kalisa system for knowledge-driven adaptable intrusion detection for the internet of things. In *Distributed Computing Systems (ICDCS), 2017 IEEE 37th International Conference on*, pages 656–666. IEEE, 2017.

[7] Daniel Miessler. Hp study reveals 70 percent of internet of things devices vulnerable to attack. *Retrieved June*, 30:2015, 2014.

[8] Pavan Pongle and Gurunath Chavan. Real time intrusion and wormhole attack detection in internet of things. *International Journal of Computer Applications*, 121(9), 2015.

[9] Kathy Pretz. Exploring the impact of the internet of things: A new ieee group is taking on the quest to connect everything. *The Institute*, 2013.

[10] Shahid Raza, Linus Wallgren, and Thiemo Voigt. Svelte: Real-time intrusion detection in the internet of things. *Ad hoc networks*, 11(8):2661–2674, 2013.

[11] Farzad Sabahi and Ali Movaghar. Intrusion detection: A survey. In *Systems and Networks Communications, 2008. ICSNC'08. 3rd International Conference on*, pages 23–26. IEEE, 2008.

[12] Tobby Simon. Chapter seven: Critical infrastructure and the internet of things. *Cyber Security in a Volatile World*, page 93, 2017.

[13] R Stephen and L Arockiam. Intrusion detection system to detect sinkhole attack on rpl protocol in internet of things.

[14] Linus Wallgren, Shahid Raza, and Thiemo Voigt. Routing attacks and countermeasures in the rpl-based internet of things. *International Journal of Distributed Sensor Networks*, 9(8):794326, 2013.

[15] Dave Wichers. Owasp top-10 2013. *OWASP Foundation, February*, 2013.

[16] Tianlong Yu, Vyas Sekar, Srinivasan Seshan, Yuvraj Agarwal, and Chenren Xu. Handling a trillion (unfixable) flaws on a billion devices: Rethinking network security for the internet-of-things. In *Proceedings of the 14th ACM Workshop on Hot Topics in Networks*, page 5. ACM, 2015.

[17] Kuan Zhang, Xiaohui Liang, Rongxing Lu, and Xuemin Shen. Sybil attacks and their defenses in the internet of things. *IEEE Internet of Things Journal*, 1(5):372–383, 2014.