Demo Abstract: A Distributed Power Side-channel Auditing System for Online IoT Intrusion Detection

Woosub Jung
William & Mary, USA
wsjung@cs.wm.edu

Yizhou Feng
Old Dominion University, USA
yfeng002@odu.edu

Sabbir A Khan
Old Dominion University, USA
skhan@cs.odu.edu

Chunsheng Xin
Old Dominion University, USA
cxin@odu.edu

Danella Zhao
Old Dominion University, USA
zhao@cs.odu.edu

Gang Zhou
William & Mary, USA
gzhou@cs.wm.edu

ABSTRACT

As the number of IoT devices has increased rapidly, IoT botnets have exploited the vulnerabilities of IoT devices. However, it is still challenging to detect the initial intrusion on IoT devices prior to massive attacks. Thus, a new approach that monitors these initial intrusions is needed. Power side-channel information can be used because it does not require any modification in programming languages or operating systems on diverse IoT devices.

We propose a distributed power side-channel auditing system for online IoT intrusion detection. To meet the real-time requirement, we develop a lightweight power auditing device. We then design a distributed CNN classifier for online inference in a laboratory setting. Two distributed protocols are also proposed in order to protect data leakage and reduce networking redundancy. In this work, we demonstrate the feasibility of our real-time distributed system for intrusion detection on IoT devices.

KEYWORDS

Power Intrusion Detection System, Distributed Online System, Privacy-preservation, Internet of Things

1 INTRODUCTION

On IoT devices, identifying and understanding various characteristics of abusive botnet attacks remains a challenge. Poor security on many IoT devices makes them soft targets, and often victims may not be even aware of whether they are infected [5]. While network-based studies often targeted specific devices or protocols, IoT devices are not being controlled by just a few standardized operating systems or protocols [1]. Therefore, new research is needed to find a universal security solution for diverse IoT devices in practical deployments. Furthermore, IoT devices are not capable of deploying sophisticated detection algorithms that often require significant resources. It is also inefficient to deploy a dedicated system for a single IoT device. Thus, cloud-based mechanisms can be a solution to leverage their tremendous computing power to detect misused IoT devices.

In this work, we propose a distributed Power Auditing System that detects intrusion on IoT devices in real-time. We first utilize the power side-channel information for the detection of stealthy attacks. Power consumption data is universal since it can capture accumulated tasks on heterogeneous devices, such as different hardware, vendors, operating systems, etc. Meanwhile, it is nearly impossible for attackers to generate power draw in normal operation modes while attacks. Next, we leverage the cloud environment for online classification to offload CNN inference computations. Overall, this demo is the real-time implementation of our recent work "Deep-Auditor: Distributed Online Intrusion Detection System for IoT devices via Power Side-channel Auditing", which was accepted to IPSN'22. More technical details and results are addressed in the regular paper [3].

2 SYSTEM OVERVIEW

Figure 1 illustrates the system overview. Our system includes a smart auditor that can be interfaced with an IoT device, specifically between the IoT device itself and its power supply, as illustrated in Figure 2. The power consumption data of IoT devices are then transmitted to a cloud classifier for real-time intrusion detection. In addition, for the online classification of the power consumption data, we propose a privacy-preserved CNN classier in a cloud setting. This CNN model was partitioned and deployed in two non-colluding servers, the Data Inferencer and the Computing Cloud, to offload the computing requirements of the CNN inference computations to more capable means of performing them.

In the cloud setting, it should be noted that the servers may try to infer IoT device behavior based on the power trace input, and users try to learn the server's model parameters based on the server output. In order to protect the private data from IoT devices, the present system is configured to include a privacy-preserved protocol via Packed Homomorphic Encryption (PHE) [2, 4]. This protocol is secure assuming a semi-honest model. Specifically, the Computing Cloud is then not permitted to learn IoT private data received from the Data Inferencer, whereas the Data Inferencer similarly is not permitted to learn the model parameters held by the Computing Cloud or primary remote server. Furthermore, the system is also configured to apply a sliding window protocol for better classification accuracy and real-time inference. This sliding window protocol segments raw power traces and transmits the segmented packets to the cloud. Then, the cloud site assembles the segmented packets prior to online inference. Altogether, the proposed distributed components accomplish the online intrusion detection on multiple IoT devices via power side-channel auditing.

3 IMPLEMENTATION

We implemented a prototype system in a lab setting. A Raspberry Pi 3 device was utilized for power auditors and IoT devices since it is widely used for IoT prototyping purposes. Using a current sensor, the Power Auditor measures the power consumption of

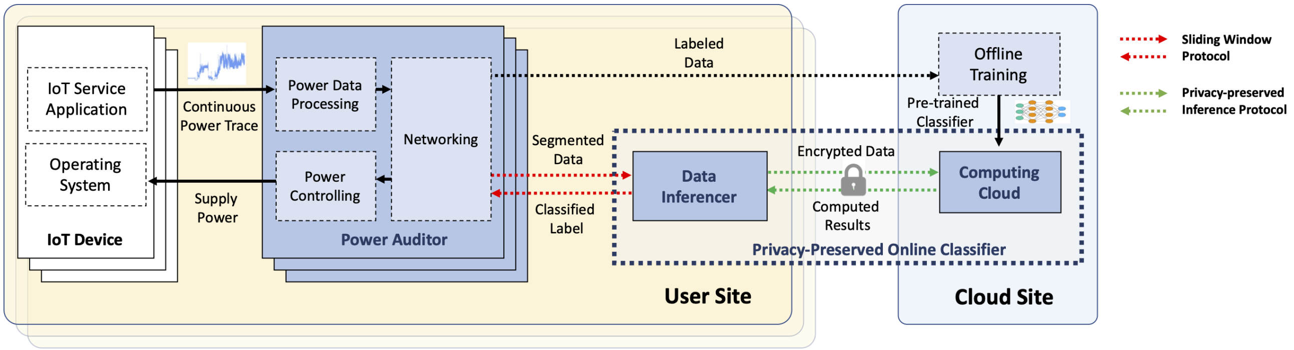


Figure 1: System Overview — The system consists of three subsystems with two distributed protocols.

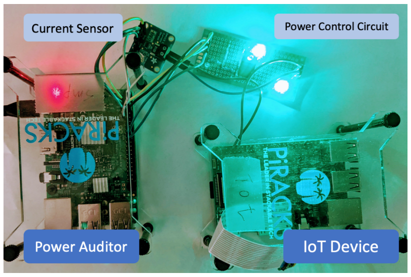
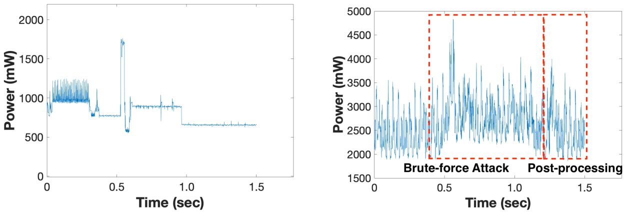


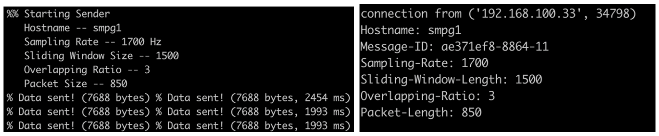
Figure 2: Power Auditor Testbed



(a)

(b)

Figure 3: Power Traces collected by our Power Auditor



```
%% Starting Sender
   Hostname -- smpg1
   Sampling Rate -- 1700 Hz
   Sliding Window Size -- 1500
   Overlapping Ratio -- 3
   Packet Size -- 850
% Data sent! (7688 bytes) % Data sent! (7688 bytes, 2454 ms)
% Data sent! (7688 bytes) % Data sent! (7688 bytes, 1993 ms)
% Data sent! (7688 bytes) % Data sent! (7688 bytes, 1993 ms)
```

```
connection from ('192.168.100.33', 34798)
Hostname: smpg1
Message-ID: ae371ef8-8864-11
Sampling-Rate: 1700
Sliding-Window-Length: 1500
Overlapping-Ratio: 3
Packet-Length: 850
```

(a) Data Collecting **(b) Online Classification**

Figure 4: Online Classification Displays

connected IoT devices [1]. The system also used a UNIX server for the Data Inferencer in the same local network. The Computing Cloud is a more powerful computing server, located in the cloud. All the software modules were implemented in Python. According to our system experiments, our power auditing device requires only 2W during the real-time inference, and the network bandwidth is also only 120Kbps, which is lightweight enough for real-time inference. In this embodiment, we collected a power consumption dataset of IoT devices and trained a CNN classifier with the dataset collected. The 1D CNN classifier was then deployed in the Data Inferencer and the Computing Cloud server. As illustrated in Figure 1, we also implemented the proposed protocols between networking interfaces in Python for online privacy-preserved inference.

4 DEMONSTRATION

Two scenarios are used in our demonstration. First, we plan to show that the power auditor device can capture real-time power consumption changes as it measures different behavior of IoT devices. By doing this, participants can have a sense of what the input data look like in our classification system. Figure 3 illustrates various displays of the power consumption data.

Next, we will show real-time classification results where the proposed CNN classifier gets involved. The intermediate server and primary cloud server compute predicted labels given the power input. This scenario will also include the procedures of the two proposed protocols: a sliding window between Power Auditor and Data Inferencer in user site, and a privacy-preserved inference protocol between Data Inferencer and Computing Cloud. Figure 4 illustrates potential displays of the online classification procedure.

Overall, our demo session can demonstrate how power consumption data can tell malicious behavior on multiple IoT devices without data leakage.

ACKNOWLEDGEMENTS

This research is partially supported by COVA CCI Cybersecurity Research and Innovation Funding, COVA CCI Cybersecurity Innovation Bridge Fund (Grant #HC-4Q21-005), COVA CCI Dissertation Fellowship, and NSF grant CNS-2120279. We would like to thank all the anonymous reviewers for their valuable comments.

REFERENCES

[1] M. Antonakakis. Understanding the Mirai Botnet. *USENIX Security Symposium*, July 2017.

[2] J. H. Cheon, A. Kim, M. Kim, and Y. Song. Homomorphic encryption for arithmetic of approximate numbers. In T. Takagi and T. Peyrin, editors, *Advances in Cryptology – ASIACRYPT 2017*, pages 409–437, Cham, 2017. Springer International Publishing.

[3] W. Jung, Y. Feng, S. Khan, C. Xin, D. Zhao, and G. Zhou. DeepAuditor: Distributed Online Intrusion Detection System for IoT devices via Power Side-channel Auditing . *arXiv preprint arXiv:2106.12753*, 2021.

[4] microsoft Research. *Microsoft seal (release 3.2)*, Feb. 2019. https://github.com/Microsoft/SEAL.

[5] Wikipedia. 20-year-old flaw found in ubiquiti networking gear running ancient php., 2020.

[1] Power-auditing source code is available at https://github.com/woossup/Power-Auditor