Data Exfiltration using Side Channels in IoT devices

Madhukant
Department of CSE
IIT Kanpur

Nilesh Vasita
Department of CSE
IIT Kanpur

Pratyush Varshney
Department of CSE
IIT Kanpur

Tushar Gupta
Department of CSE
IIT Kanpur

***Abstract*—In this paper, we discuss the usage of IoT devices and their impact on our day-to-day life. We then explore various side-channel attacks that IoT devices are prone to, and what are some different types of attacks which can be done on IoT devices. We also discuss some already implemented attacks on IoT devices in the past that have led to leakage of private data. Further, we discuss some possible techniques to covertly exfiltrate a given message string using the Magic Blue Bluetooth bulb using both Non-invasive and Semi-invasive methods.**

***Index Terms*—Side-channel attack, IoT, Smart Bulb, Covert attacks**

I. Introduction

The Internet of Things (IoT) refers to the interconnection of smart devices which aims to reduce the gap between the real and virtual world. The ability of these devices to collect data and make intelligent decisions has completely changed the way in which we humans interact with technology today.

Given the huge benefits of using such devices, the adoption rate of these devices has been very high. However, along with increasing use cases of IoT devices, it is manufacturers' responsibility to make them secure in terms of private data leakage which can be highly catastrophic in some cases. Security breaches are not only dangerous for highly sensitive industries like defence, but also for all the other places where IoT devices are used frequently and are vulnerable to security threats at the same time.

Household appliances like refrigerator, TV, smart bulbs can be compromised to exfiltrate personal information of the family living in the home. Various wearables like smart watches and Google lens deal with large amounts of personal data generated by the minute, and are hence one of the major attractions for IoT related security exploits. Medical industries are investing in developing IoT based use cases in various applications. These include general devices to measure body conditions such as heartbeat, body temperature and blood pressure as well as application specific products like pacemakers and Smart Beds. All of these are vulnerable since they are often connected to the internet. Devices employed in medical use cases, if compromised, can put the users' privacy as well as lives at risk.

IoTs are also used in industry level machinery to monitor the physical condition of their components for their proper functioning. Be it the field of Agriculture or heavy construction, IoT devices are used in some or the other form.

Incidents like [1] [4] (earliest side channel attack) that happened in the past instill apprehensions for the adoption of these interconnected devices. The research in securing these IoT devices is an active area, most of which address the mainline vulnerabilities. To secure sensitive information and data, organizations often air-gap their computer networks. This means that there is no physical or logical connection of these devices with the outside world i.e. the internet. However, researchers have found various workarounds to breach these air-gapped [2][11] networks. Detecting data leakage through covert channels is a challenging task for security researchers around the world. In this paper, we study some techniques to exfiltrate data using covert side channels in IoT devices and propose an implementation of the same for the case of smart Bluetooth bulbs.

II. Overview of Covert Channel Attacks

In this section we describe various attacks possible on IoT devices by exploiting covert channels.
IoT devices can be exploited by number of methods, some of which are described in this section.

A. Timing-based

The processing time of an algorithm in a processor varies with different events. The timing-based attack works on a similar principle as various events of a program take different amount of time to process through which we can guess which event has occurred. There are many ways in which these time-stamps can be detected and used to identify a desired event.

This kind of attack can be used to unlock smart doors which open on entering a series of code. Main idea of this attack is that if a correct code is entered in lock then it will take more time to process as compared to a wrong sequence of code entered. One main challenge is to find ports in the device which can be directly related to time taken in processing of an input code.

Oscilloscope, a device which is used to measure voltage or current, can be used efficiently for this problem. We can measure voltage across the main power supply in micro-controller and deduce the time taken in processing a program. Given the fact that the key is matched sequentially, if first digit is matched, the time taken will be slightly longer as compared to the case in which the first key was wrong. Hence, we can figure out the complete sequence of code.

B. Traffic based attacks

Many IoT devices share their environment conditions and accept commands via the internet. For example, some

thermostats[12] can connect to the internet through WiFi and can accept commands for turning on or off from a distant location. Traffic based attacks are side channel attacks in which one analyzes the flow of network packets and extracts useful information from it. The principle of traffic based attacks is that information in the form of data packets is always flowing and by analysing these packets, we can extract some useful information. This makes a thermostat connected to the internet a highly tangible system for web as well as traffic based attacks. [5] describes a side channel traffic based attack on Nest[13] Thermostat and Nest[5] Protect, which include fire alarms and other security solutions. [13]Researchers dumped the network traffic of 3 days and analysed it using various packet analysers such as wireshark and BRO. Upon rigorous analysis, they were able to find the peak time intervals where the payloads sent to and from the device were maximum and accurately figure out the state in which the thermostat was at any given time. This information is dangerous, as it can be used to predict when the occupants were not in the house, which is bad for their privacy as well as security.

C. Electromagnetic

Various IoT devices are required to perform signal analysis in their respective use cases, which include encryption and decryption mechanisms, receiving signals and interpreting them appropriately. Whenever some signal is processed on a device, various electromagnetic waves are released, which can be used to exfiltrate some data. Electromagnetic based side channel attacks assume that this data is representative of some secret key stored in the device. The first EM based attack was demonstrated in 1985 [8]. EM attacks can be as simple as placing the circuit in a magnetic coil and measuring magnetic field fluctuations as computation is done in the device. A popular attack on chips executing the RSA encryption measures EM field fluctuations arising due to differences in power consumption while exponentiation depending on the current bit, as the square-and-multiply operation takes more processing power than square. This makes the otherwise mathematically tough problem of finding out the RSA key trivial.

D. Acoustic

Voice based assistants like Siri, Alexa are vulnerable to the acoustic attacks. These assistants require microphones that measure the difference of sound pressure to convert human voice into commands. This can be used as to attack the IoT device in two ways - noise based attacks and hidden voice attacks. In noise based attacks, adversary can obfuscate malicious commands into sound signals that seem to be noise for humans. In [10] the authors show the Man-In-the-Elevator attack. They target the attacker by playing a background noise inside an elevator as the target enters. The noise has been crafted such that it activates the voice assistants and sends malicious commands. Due to the limited sensing range of humans, any sound below 20Hz and above 20KHz are inaudible. An adversary can synthesize malicious commands that are outside the audible range of humans. These commands can be crafted by using the sampling frequencies of the microphone. In [9] the authors have shown that an ultrasound non-linear signal when processed by the microphone of the victim, introduces new frequencies in the system. The ultrasound signal can be crafted in such a way that when the victims microphone processes the signal, the new frequencies induced amount to a malicious command.

E. Power-analysis

Power analysis refers to exploiting the power consumption patterns of semiconductor devices to exfiltrate precious data. Since power consumption by such semiconductor devices is typically small and power consumption fluctuates at high frequency, sensitive equipment is required for such analysis. Simple Power Analysis refers to the technique where we directly map the devices power consumption to either the operations being carried out inside the device or some secret key/message stored inside the device.
Power analysis attacks can fall into **Simple power analysis (SPA)** and **Differential Power Analysis (DPA)**.

- **Simple power analysis** is used in systems where the power fluctuations (which are in turn dependant on the covert data to be exfiltrated) are large enough to be examined visually. Usually, different instructions consume different amount of power when executed on a microprocessor, and hence can be traced with the standard available oscilloscopes. A few common examples include DES encryption key leakage and RSA key leakage, where square and multiply operations can be differentiated easily.
- **Differential power analysis** is used in cases where direct visual interpretation of power traces is not useful, usually due to low signal to noise ratio. However, careful processing and error correction can extract such data.

Non invasive and passive Simple and Differential power analysis attacks are typically hard to detect. SPA attacks can be avoided by taking care that the program execution does not take widely different paths depending on some secret value. Avoiding DPA attacks is difficult, since it is sensitive to even small variations. Modifying the algorithm in such a way that power consumption becomes invariant of the secret is the only plausible approach.

III. Attacking the Smart Bulb

A. Attack Scenario

We are making the following assumptions regarding the attack scenario:

- We have an *insider* planted in the company who has the rights and the means to control the bulb. However he, being inside of the company has no access to any of his personal devices, and hence cannot communicate with us by any means except the bulb.
- Both the bulb and the *insider* are on the internal air-gapped network, and cannot communicate with any outsider directly.

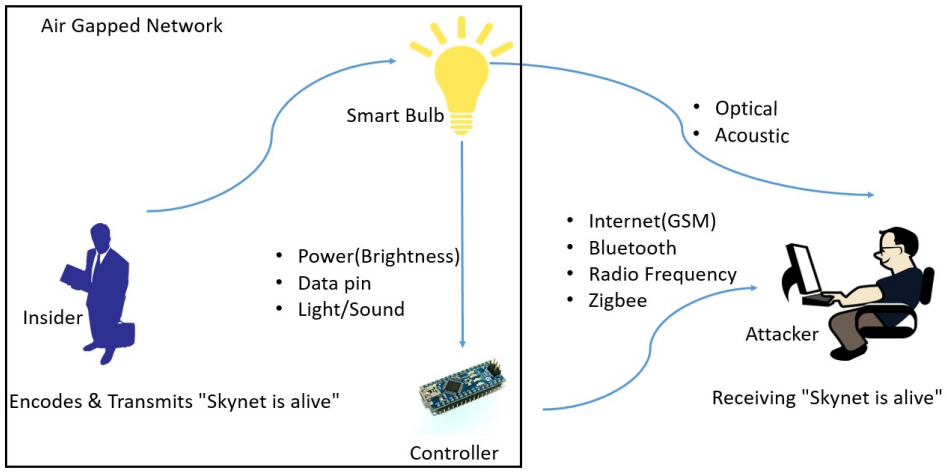

Fig. 1. Side Channel Attacks Possibilities

- The *insider* has access to the message while he is inside the company, and wants to communicate it to the attacker. For simplicity, we assume the message to be the string "Skynet is alive!".
- Encoding and decoding scheme of the data is pre-decided between the *insider* and the *attacker*.
- The company requires the bulb to glow at a particular colour and brightness and not play any sounds. Hence we cannot tamper with the visible properties of the bulb too much (to avoid direct suspicion).
- The company can either be 'open' (meaning the bulb can be seen/heard from outside, or 'walled', (meaning that the bulb cannot be seen/heard from outside).

B. Attack Description

Side channel attacks can be broadly classified in the categories of *invasive*, *semi-invasive* and *non-invasive*. Invasive attacks include tampering with the device to the point of destroying it, but these have to be ruled out in light of our assumptions. In the semi-invasive attacks, we tamper with the device, but the device can still function normally. Non-invasive attacks are the ones where information is gathered using externally accessible factors like light intensity, audio waves, heat waves, etc.

We propose to exploit the following side-channels available with the smart bulb. These channels will be used to transmit the information from the bulb to an attacker who is sitting outside the air-gapped building and readily receiving the information sent by the bulb.

1) Non-Invasive: Assuming the building to be 'open', non-invasive side channel attacks should be preferred as they are the most covert in nature.

- **Optical**: Minor changes in the intensity of colors emitted by the smart bulb can be used as a channel to transmit information outside the building. Consider the case where the company requires the bulb to glow at 50% brightness. If we encode the string "Skynet is alive!" in binary, and map 0's to 49% and 1's to 51%, we can covertly transmit the message outside (assuming that the optical receiver is sensitive enough).
- **Acoustic**: The smart bulb can generate sound in the ultrasonic frequency range (above 20 kHz) which is outside the human audible range and will go unnoticed. Now, again encoding the message string in binary, we can map 0's to 21 kHz and 1's to 22 kHz to send the message. The message can then be decoded by the receiver.

2) Semi-Invasive: Assuming the building to be 'walled', we have no options but to resort to semi-invasive attacks. Here, we connect a micro-controller (such as an Arduino or a Raspberry Pi) to the appropriate bulb pins (or place it in near the bulb) and transmit the data outside using an appropriate channel. Hence, our choices include choosing the appropriate side channel to exploit and the transmission method we use to send the sensitive data to the attacker.
Possible Side channels:

- **Power consumption**: The power consumption of the bulb is presumably proportional to the brightness. Hence the insider can vary the brightness slightly, again mapping the binary representation of the message string to small variations in the brightness. These variations can be captured and transmitted by the micro-controller and decoded by the receiver.
- **Data pin**: The commands sent to the bulb via bluetooth are converted into electrical signals, which are reflected in the data pin. By hooking the micro-controller to the data pin, we can exfiltrate a message string encoding to the attacker.
- **Optical and acoustic**: We can again encode the message in varying brightness and sound frequencies (as described in non-invasive attacks) and transmit it to the attacker

using the micro-controller, where it can be decoded.

Possible Transmission channels:

- Internet (GSM)
- Bluetooth
- Radio Frequency
- Zigbee

Using any combination of these, we can devise strategies to exfiltrate the message string.

REFERENCES

[1] An unprecedented look at STUXNET, The World's first digital weapon, Wired, 2014

[2] Carrara, B. And Adams, C., "Out-of-band covert channels A survey," ACM Computing Surveys 49, 2, 2016.

[3] Guri, Mordechai and Elovici, Yuval, Bridgeware: The Air-gap Malware, Commun. ACM, vol. 61., March 2018, pp.74–82.

[4] YongBin Zhou, DengGuo Feng Side-Channel Attacks: Ten Years After Its Publication and the Impacts on Cryptographic Module Security Testing in IACR 2005

[5] B. Copos, K. Levitt, M. Bishop and J. Rowe, "Is Anybody Home? Inferring Activity From Smart Home Network Traffic," 2016 IEEE Security and Privacy Workshops (SPW), San Jose, CA, 2016

[6] M. Moukarzel, T. Eisenbarth and B. Sunar, "Leech: A side-channel evaluation platform for IoT," 2017 IEEE 60th International Midwest Symposium on Circuits and Systems (MWSCAS), Boston, MA, 2017

[7] Amit Kumar Sikder , Giuseppe Petracca , Hidayet Aksu , Trent Jaeger , and A. Selcuk Uluagac1 A Survey on Sensor-based Threats to Internet-of-Things (IoT) Devices and Applications arXiv:1802.02041

[8] Rohatgi, Pankaj. (2008). Electromagnetic Attacks and Countermeasures. 407-430. 10.1007/978-0-387-71817-0_15.

[9] Nicholas Carlini, Pratyush Mishra, Tavish Vaidya, Yuankai Zhang, Micah Sherr, Clay Shields, David Wagner, and Wenchao Zhou. 2016. Hidden voice commands. In Proceedings of the 25th USENIX Conference on Security Symposium (SEC'16), Thorsten Holz and Stefan Savage (Eds.). USENIX Association, Berkeley, CA, USA, 513-530

[10] Tavish Vaidya, Yuankai Zhang, Micah Sherr, and Clay Shields Cocaine Noodles: Exploiting the Gap between Human and Machine Speech Recognition, WOOT 2015

[11] Mordechai Guri, Assaf Kachlon, Ofer Hasson, Gabi Kedma, Yisroel Mirsky, and Yuval Elovici GSMem: Data Exfiltration from Air-Gapped Computers over GSM Frequencies 24th USENIX Security Symposium, 2015

[12] Honeywell International Inc. : Wifi Smart Thermostat https://getconnected.honeywell.com/middle-east/wi-fi-smart-thermostat

[13] Nest : Home Security Solutions https://nest.com/home-security-systems/