IOT REVIEW-2

Team 16
Sakshi Jha
Saloni Shah
Sanjana Kambar
Savitri Khyadad

PROBLEM STATEMENT

Comparative study on various techniques for IOT security- Blockchain, machine learning, fog computing and edge computing.

Internet of Things (IoT) is one of the most discussed topic in research field today. The IoT applications designed, increase comfort, efficiency and automation for users, however the security and privacy threats caused by IoT draw our attention. Due to these issues, the emerging IoT applications may lose their potential. Hence, there is a need for effective architecture in the IoT applications that can guarantee security and prevent attacks on the IoT devices.

We have 4 techniques that already exist in order to prevent these threats.

- Blockchain
- Machine learning.
- Fog and edge computing.

We plan on presenting a comparative study of these techniques.

Attacks on IOT devices and IOT security threats

Internet of Things (IoT) is one of the most discussed topic in research field today. The IoT applications designed, increase comfort, efficiency and automation for users, however the security and privacy threats caused by IoT draw our attention. Due to these issues, the emerging IoT applications may lose their potential.Hence, there is a need for effective architecture in the IoT applications that can guarantee security and prevent attacks on the IoT devices.

IoT security issues from a new perspective - IoT features.

“**IoT features**” refers to the unique features of IoT devices, network, and applications, which are quite different from smartphones and computers. For example, IoT devices have much less computing ability, storage resources, and power supply, thus “Constrained” is an IoT feature.

■ Interdependence

Description: The implicit dependence relationship between devices is described as an IoT feature named “Interdependence”.

Threats: Features could be maliciously used by attackers to reduce the difficulty of direct attack the target devices and bypass original defense mechanism.

Challenges: Because the IoT device behaviors could be changed by other devices or environmental conditions, it is difficult to define a certain set of fine-grained permission rules for them. Thus, the overprivileged has become a common problem in the permission model of existing IoT platforms applications.

Solutions and Opportunities:

- ContexIoT, a new context-based permission system for IoT platforms to solve the overprivileged problem. It records and compares more context information such as procedure control flow, data source, and runtime data of every device’s behavior before it is executed, and then let the user allow or deny this behavior according to recorded information.

- However, this method relies too much on user decisions, once the user makes a wrong decision, the system will remember this wrong decision and will not prompt the user again.

■ Diversity

Description: The phenomenon that many different kinds of IoT devices and protocols appear in the current IoT market, we refer to as an IoT feature “diversity”.

Threats: Different protocols have different semantic definitions, the attackers could also take advantage of this point to find security vulnerabilities like BadTunnel when they incorrectly work together.

Challenges: How to discover and deal with so many security vulnerabilities among the various IoT devices needs to be addressed urgently.

Solutions and Opportunities:

- Framework is designed to support dynamic security analysis for a variety of embedded systems’ firmware. However, it cannot simulate all action of the real devices and need to forward action from the emulator to the device by physical connection. Thus, it is unsuitable for large-scale automated firmware analysis.

- Framework exits for large-scale automated firmware dynamic analysis, but it is only applicable to the Linux-based system

■ Constrained

Description: The limitation of the computing/storage resource, power supply and latency of IoT devices as an IoT feature named “constrained” here. .

Threats:

- Lightweight IoT devices do not have the memory management unit (MMU), so memory isolation, address space layout randomization (ASLR) and other memory safety measures cannot be applied to these devices.
- Most complicated encryption and authentication algorithms like public cryptography cannot also implement on such devices, because they occupy too much computing resource and causes a long delay, which seriously affects the normal operation and reduces performance for constrained IoT devices.

Solutions and Opportunities:

- Authentication and key generation algorithm based on physical unclonable functions, which use the unique physical structure of the device to identify itself. This method not only saves key storage space and simplifies the key generation algorithm, but can also effectively resist the side channel analysis.

■ Myriad

Description: The enormous number of IoT devices and the huge amount of IoT data is described as an IoT feature named "Myriad".

Threats: As more industrial and public infrastructures are connected to the Internet, the target of IoT botnets would no longer just be the website, but also the important infrastructures, which would bring grave damages to social security.

Challenges:

- How to detect and resist IoT botnet virus in IoT devices is a great challenge for researchers.
- At the same time, how to stop the spread of IoT botnets is also a tough problem.

Solutions and Opportunities:

- A tool is designed that extracts several attack vectors from the Mirai botnet and uses them to detect potential vulnerabilities in IoT devices.
- Consider constraints of devices and environment when detecting malicious requests in a sensor network. However, their attack assumption is too simplistic. Attackers are unlikely to send requests with the same content, but usually forge normal users' requests with different reasonable content.

■ Unattended

Description: The long-time unattended status of IoT devices is an IoT feature named “unattended”.

Threats:

- It is hard to physically connect an external interface to verify the state of these devices. Thus, the remote attacks targeted them are difficult to detect.
- Stuxnet worms could infect the programmable logic controllers (PLC) used in industrial control systems, which results in considerable physical damage.

Challenges: Building a trusted execution environment (TEE) to ensure security-critical operations be correctly executed under remote exploits and verifying internal state of a remote unattended IoT device become important tasks in many scenarios.

Solutions and Opportunities:

- A lightweight trusted execution environment is built for small embedded devices, but it does not consider how to safely handle the hardware interrupt and memory exception

■ Mobile

Description: The frequent movement of IoT devices is described as an IoT feature named “mobile”.

Threats: The social IoT devices will carry more sensitive information and automatically follow the users joining many different social networks.

Challenges:

- To confront the potential threats, the main security challenge should be addressed is cross-domain identification and trust
- When data carried with mobile IoT devices pass from one network to another, the key negotiation, data confidentiality, integrity protection and other important security issues need to be carefully concerned

Solutions and Opportunities:

- Decrease the probability of mobile IoT devices being attacked in different networks through dynamically changing the security configuration of devices according to different trust conditions.

Types of Security Attacks in IOT

- **Physical Attacks**

1. **Node Tampering:** In this attack the attacker physically alters the compromised node and can obtain sensitive information such as encryption key.
2. **RF Interference on RFIDs:** The attacker performs Denial of service attack by sending noise signals over radio frequency signals.
3. **Node Jamming in WSNs:** By using jammer the attacker can disturb the wireless communication.
4. **Malicious Node Injection:** In this attack, the attacker physically injects a new malicious node between two or more nodes. To prevent this attack, we use a monitoring verification (MOVE) scheme. It can check the monitoring node(s)' result and correctly identify any malicious behavior.

Types of Security Attacks in IOT

- **Network Attacks**

1. **Traffic Analysis Attacks:** The attacker intercepts and examines messages to obtain network information.
2. **RFID Spoofing:** An adversary spoofs RFID signals. Then it captures the information which is transmitted from a RFID tag.
3. **RFID Cloning:** In this attack, adversaries copy data from a pre-existing RFID tag to another RFID tag. It does not copy the original ID of the RFID tag. The attacker can insert wrong data or control the data passing via the cloned node.
4. **RFID Unauthorized Access:** If the correct authentication is not provided in the RFID systems, then the adversary can observe, alter or remove information on nodes.
5. **Sinkhole Attack:** In a sinkhole attack an adversary compromises a node inside the network and performs the attack by using this node. The compromised node sends the fake routing information to its neighboring nodes that it has the minimum distance path to the base station and then attracts the traffic. It can then alter the data and also drop the packets.

Types of Security Attacks in IOT

- **Software Attacks**

1. **Phishing Attacks:** The attacker obtains the private information like username, passwords by email spoofing and by using fake websites.
2. **Virus, Worms, Trojan horse, Spyware and Aware:** An adversary can damage the system by using malicious code. These codes are spread through email attachments, downloading files from the Internet.The worm has the ability to replicate itself without any human action.We can use worm detector, anti-virus, firewalls, intrusion detection system to detect the virus.
3. **Malicious Scripts:** By injecting malicious script the attacker can gain access to the system.
4. **Denial of Service:** The attacker blocks the users from the application layer by denying services.

Types of Security Attacks in IOT

- **Encryption Attacks**

1. **Side-channel Attacks:** The attacker uses the side channel information that is emitted by encrypting devices. it contains information about power, the time required to perform the operation, faults frequency, etc. Attacker uses this information to detect the encryption key.
2. **Cryptanalysis Attacks:** In this attack, the adversary obtains the encryption key by using either plaintext or ciphertext.
3. **Man in the Middle Attacks:** When two users are interchanging the key the attacker intercepts the communication and obtains the key.

IOT Security using BlockChain

The IoT devices provide real-time data from sensors and blockchain provides the key for data security using a distributed, decentralized and shared ledger.

The basic idea behind the blockchain is simple: it is a distributed ledger (also called replicated log files). The entries in the blockchain are chronological and time-stamped. Each entry in the ledger is tightly coupled with the previous entry using cryptographic hash keys.

IOT Security using Fog Computing

The main task of fog computing is to handle the data generated by IoT devices locally for better management and thus requires an architecture consisting of different layers. It has two frameworks that are Fog-Device framework and Fog Cloud-Device framework. The former framework consists of device and fog layer and the latter framework consists of device, fog and cloud layer. The arrangement of layers is done based on their storing and computational powers. The communication between different layers is done using wired (e.g., optical fiber, Ethernet) or wireless communication (e.g., WiFi, Bluetooth, etc.).

IOT Security using Edge Computing

The solutions that edge computing can provide to overcome these security threats are:

1. Data breaches
2. Data Compliance Issues
3. Safety Issues
4. Bandwidth Issues

IOT Security using Machine Learning

The solution provided by ML to overcome these security threats are:

1. DoS attack
2. Eavesdropping
3. Spoofing
4. Privacy Leakage
5. Digital Fingerprinting

REFERENCES

[1]. https://securityboulevard.com/2020/03/an-eye-on-iot-security/

[2]. https://www.onetech.ai/en/blog/10-types-of-cyber-security-attacks-in-the-iot

[3]. https://nearshore.perficient.com/software-development/a-guide-to-iot-security-attacks/

[4]. https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/magazine/internet-threats

Papers Referred:

[1]. Hassija, Vikas, et al. "A survey on IoT security: application areas, security threats, and solution architectures." *IEEE Access* 7 (2019): 82721-82743.

[2]. Deogirikar, Jyoti, and Amarsinh Vidhate. "Security attacks in IoT: A survey." *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)*. IEEE, 2017.

[3]. Zhou, Wei, et al. "The effect of iot new features on security and privacy: New threats, existing solutions, and challenges yet to be solved." *IEEE Internet of Things Journal* 6.2 (2018): 1606-1616.