Technical Report For IoT Security on Application Layer

I. Threats in the Application Layer

THough the concept of Internet of Things(IoT) was first proposed by Kevin Ashton in 1999 with a simple description of "adding RFID and other sensors to everyday objects will create an Internet of Things, and lay the foundations of a new age of machine perception"[6], the world has witnessed a steep increase on the scale of the IoT. According to IBM, the number of connected devices is forecast to grow to almost 31 billion worldwide in 2020 which is a number far more than the world's population[7]. Due to the large scale of promotion in the commercial market, there has been quite a lot of applications serving people's daily life. However, among this large quantity of applications, severe security and privacy problems exist.

The duty of application layer of the IoT is mainly about analyzing and processing the data receiving from the network layer (including the data which is processed in the middleware layer) so that the computer or computer cluster can make right decisions and control the actuators to react automatically[1]. Despite the wide variety of IoT applications, we can still give a classification in general for this domain. The current application domains include(but are not limited to) independent living(smart homes), smart cities, smart energy, smart mobility and transport, smart healthcare, smart manufacturing, retail and logistic, environment monitoring[8]. Although these applications belong to the dispersed fields in the domain of application and service in IoT, they can be divided into service for the consumer and service for the enterprise(mainly know as '2C' and '2B' respectively) and the requirement of the security and privacy is different because of the different environment of each application. As a result, in this section we first analyze some technical problems on security threats on '2B' field and '2C' field respectively, then we will mention some non-technical problems in this domain and finally we try to give some suggestions on the security and privacy problems in the application layer.

A. '2B' threats in IoT application layer

Since the IoT is still basing on the Internet, some previous threats on the conventional Internet still cause extensive damage on the business enterprise's server and network in the brand new IoT ecosystem. October 21, 2016, a large number of IoT equipment which were infected by the Mirai(a kind of computer virus) launched for a huge amount of DDoS attack on DNS servers which were managed by Dyn, Inc. The influence scope covers the U.S. east coast, west coast and parts of Europe, leading to the inaccessibility of Twitter, GitHub, Amazon, PayPal, BBC, Wall Street Journal and many other well-known websites. Also, as IoT advances, cloud computing is placed in high hopes for the solution of worldwide information spread, data process, data analytic and storage. Cloud services such as Microsoft Azure, Amazon Web Services(AWS) and Google Docs are expected to provide interfaces for IoT interconnecting equipment[8]. As a result, in this section, we will discuss some security threats on enterprise's server cluster including DoS / DDoS attack, service vulnerability on SOA structure, data security and cloud computing security threats respectively.

1) DoS / DDoS: DoS attack is a kind of network-based attack which prevents user from accessing the network service. Basically, DoS attack utilizes a large number of network connection requests to 'flood' the server so that the program which is running on the specific server crash down while the resources on the server were exhausted, or otherwise prevent the client from accessing the network service so that the network service does not function properly or even shut down. Common DoS attack sends a single packet to the victim server to exploit its system vulnerabilities or sends large packet blocking bandwidth or using some other techniques such as TCP SYN flood to consume the victim's resources.

DoS attack, especially DDoS attack are more prone to occur in the IoT ecosystem because this new kind of M2M interaction will lead to a bigger amount of equipment being infected by the malicious attacker's virus program and thus provide the attacker abundant potential Zombie nodes effortlessly to implement DDoS attack which will lead to much more serious consequence compared to the previous Internet structure.

2) SOA Structure Security: SOA is the abbreviation of service-oriented architecture which is essentially a collection of services. These services communicate with each other. The communication can involve either simple data passing or it could involve two or more services coordinating some activity. Some means of connecting services to each other is needed.[2] Because of its own characteristic, SOA is often used in the field of distributed computing.

The five main parts of SOA architecture are showed below:

(1) Consumer: acquires the service from producers entities, such as mobile terminals and web client.

(2) Application: provides application interfaces, always the producer's service entities on the client side, such as mobile apps, web apps, and rich client.

(3) Service: the implementation of the entities involved in a specific task, such as data center and enterprise information center.

(4) Service Support: SOA specific application background support functions, such as security, management, and semantic analysis.

(5) Producer: an entity to provide specific services.[9]

The following table shows a five layer architecture of SOA based processing layer of IoT.

Users	Application users
Security Platform	Service access security and user authentication
Service	Application universal interface
	Device management; Service agent
	Data universal interface
Data processing platform	Consistency and standardization of heterogeneous data
	Data validation and decontamination
Device	Smart phone, Smart bracelet, etc.

Fig. 1. Vulnerabilities By Type

In the ecosystem of IoT, on one hand, the IoT physically consist of a large number of terminals with the ability of computing which leads to the birth of edge computing. On the other hand, since the IoT has a wide audience and huge user base, the service provider need to face the need of a massive requests from the users who are using diverse operating system. As a result, the SOA architecture is needed.

However, since in the SOA structure, different services are provided by the facilitator which leads to the openness of the service, it also leads to security problems. Since the second level user and the third level user(e.g. the partner's partner) can both access unprotected SOA services, the unknown third-parties in SOA are always exposed to wide range of external service attacks and some other security risks. As a result, the unprotected SOA is easily overloaded. At this time, access control and anti malicious attacks are needed to prevent unprotected SOA from being attacked by DoS attackers.

3) Data Security: With the quickly development of IoT, different user types are added into this interaction network. In this process, extracting data from users and managing this data is important for application layer security analysis.[1]

For business enterprises, especially those service provider companies, they need to face the massive requests from different users asking for the shared data. One security threats is that before provide the user with the specific data, the service provider had better check the level of permissions of the user to ensure that the user is access to the data he is allowed to receive. For example, when urban construction planning department asking for the monitor data of the traffic, they should only be accessible to image of low resolution since they just need to know the general situation of urban congestion. When the traffic management department ask for the data, they are accessible to image of better congestion than the urban construction planning department receive because they need to know the detailed traffic situation. While for the policeman's investigation, they need the clearest image so that they can identify the number of the specific car. The problem here is how to make the decision on the level of permissions for the massive amount of users.

Other data security threats for the business enterprises exist in storage and backup of the data. The current mainstream storage encryption technology includes embedded encryption, database-level encryption, file-level encryption and device-level encryption.There are a number of manufactures(such as EMC) and standard organizations (such as TCG and SNIA) dedicated to the development and promotion of storage encryption standards, hoping to make storage security tools more easily to set a variety of storage architectures work together. At the same time storage encryption algorithms such as AES have also been recommended in the IEEE storage encryption standard P1619. For the data backup, it is generally being addressed by file-level backup, block-level backup, remote file copy and remote disk mirroring. However, these mechanisms are mostly for the data storage problem of traditional Internet structure. Since the IoT is a user-orient network with a much more extensive of data distribution, it is not certain that these methods will be fully applicable to the needs of the IoT for sharing data.

4) Cloud computing: According to the formal definition from the US National Institute of Standards (NIST), the cloud computing is "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. Networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction"[16]. Considering the rapidly inflating data flood in the IoT ecosystem, Caceres and Friday [17] discuss the changing, chances and challenges of an ecosystem of ubiquitous computing 'ubicomp' and figure out the two fundamental of future 'ubicomp' ecosystem are cloud computing and the Internet of Things. Consensus believes that as IoT matures, the cloud computing will take the role of generate data from the various ubiquitous terminals (e.g. sensors and IO terminals), as well as providing services for big data processing, analyzing and interpreting. However, as a gigantic and complex web system, cloud models remain various security challenges such as application services attacks, data intergrity attcak, privacy, trust, identity, standardization, etc[8]. Figure 1. shows the cloud induced vulnerabilities identified from 1999 to present (2017/08) from the common vulnerability database[18] which shows the common attacks on cloud models such as code execution, DoS attack, overflow and XSS.

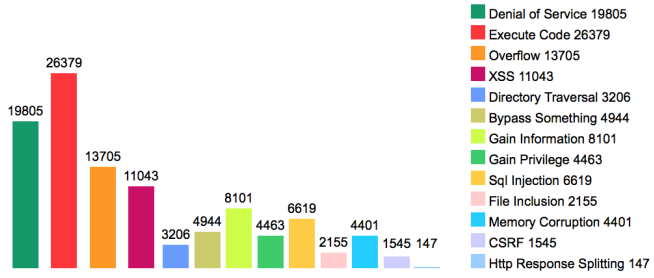

Fig. 2. Vulnerabilities By Type

B. '2C' threats in IoT application layer

Comparing with the '2B' domain, it is believed that the end-user of the IoT are more vulnerable to attacks, since

they lack the technical expertise and the resources to deploy in-depth defense solutions that protect them from potential adversaries[3]. On the other hand, with the highly trained administrators who can utilize the firewalls and intrusion detection system and always pay attention to the enterprises' network, the enterprises won't suffer that much of attacks. As a result, there are a huge variety kinds of '2C' threats in IoT application layer. In this section, we will discuss five kinds of attacks or loopholes of IoT application layer. Some of them have already attracted researcher's attention in the conventional Internet domain. But they have all been exposed to the brand new IoT more or less.

1) Web Interface Attack: Almost every user-oriented IoT application need a user account in order to identify user identities and manage user data. From the point of view of vulnerability on user authentication, this kind of attack aims at account enumeration, account lack of lockout and weak account credentials. Taking advantage of the weak authentication protocol, the attacker could capture the plain-text credentials or account information effortlessly. The main ways of attacks in this domain includes cross-site scripting(XSS), cross-site reference forgery(CRSF), IP misconfiguration and SQL or command injection[8]. Often, attacks in this domain are caused by the insecure design of web interface and weak account authentication and credential protocol.

2) Data and System Integrity Attack: Data is the sword of Damocles for IoT. It not only bring the IoT vitality but also remain danger of being attacked at any time. Apart from stealing the data, one of the approaches is damaging the data so that the integrity of data is threatened. This kind of attack attempts to compromise system or database data by inserting, distorting or completely deleting data in order to deceive smart device to make wrong decisions or injure its integrity. The typical attacks among this domain are SQL injection, command injection and code execution from remote attackers. Moreover, except for data integrity attack, some attack focus on the integrity of system. Security problems may occur as the system losing its integrity[11]. This kind of security threat may appear as the system is overloaded or some abnormal process situations arising (e.g. multiple alarms, error instruction and network failure).

3) Software Attack: Software is the entity of the service which is provided by the service provider. It is a part of a computer system that consists of data or computer instructions. Since there is not enough computing strength and storage space for the IoT terminals, few of them possess on strong operating system running strong security protocol. As a result, malicious attackers could hack into the software effortlessly. The common approaches of attack in this domain are Trojan horse programs, worms, viruses and logic bombs. These types of attacks have the similarity that they all deliberately inserted code into the software and do great damage to the software, the system and the privacy data of the user[10].

4) App Over-privilege: In order to achieve more complex and user-oriented services, many devices in the IoT ecosystem carry third-party apps. The most common example is the huge variety of IoT apps running on smart phones or smart bracelet. These apps give the smart phone ability to connect with other equipment and control them or perceive and record its own state of motion and the surrounding environment. However, due to the bad design of system authorization, these apps are able to access devices and data they are not supposed to[3]. For example, apps with GPS permission can leak the user's life zone; apps with Bluetooth permission can access any other equipment in its Bluetooth zone; apps with MEMS sensors permission can leak the user's gesture which may help the malicious attacker decrypt the user's door accessing password or bank account password. These information give adversaries chances to make further implementation on attacking basing on social engineering approaches. These kinds of attacks, which is know as the side channel attack, are in essence because of the app is able to access data or channel which beyond the apps needs. App over-privilege problems are normally because of design defects (e.g.failure to achieve the least privilege principle). Therefore, they often require vendors to significantly adjust the system since the design of application's privilege level relates to the system's architecture.

5) Implementation Flaws: This domain is about the loopholes of software during its designing or implementing because of the vendor's careless or unconsciousness. Such implementation flaws may includes leakage of hardcoded credentials, open ports, debugging mode and transmitting data among the IoT ecosystem without encrypting them[3]. Also the implementation should concern its enable independence with the previous layer which means that the status (e.g. sleeping, failed, active) of the device (or application) should not bother the motion of the middleware layer, the network layer and the application layer[11]. Attacker can hack into another device of in the same local area network (LAN) through its open ports or remote login mode. For attacks on hardcoded credentials, home automation equipment such as light bulbs [13] and thermostats [14] are easy to become the victim due to the . hardcoded credentials in the devices firmware [15]. Besides, combining the threats on hardcoded credenetials and plaintext data transmission, hardcoded credentials' disclosure via unencrypted text transmission is also a privacy leakage situation[12].

C. non-technical threats in IoT application layer

This domain is mainly about meeting the policy commitment among different country and to treasure data as the 21st century's brand new property. As a result, there should be more legal protection for data security.

Besides, when we talk about IoT security in the application layer, since this layer are mean to have directly interaction with people(no matter they are average consumer or large company), it is also very important for them to be taught to be aware of the security threats and to be scientific and rational managed to reduce the impair caught by the attacker. As we have discussed before, implementation flaws is one of the serious security threats for the '2C' orientation. Except that the vendor should keep sensitive consciousness about applications' security leakages, they also need to find ways to force the user to install the latest published patch. Researches on the Mirai-base DDoS attack (which we mentioned at the

beginning of the threats in IoT application layer) shows that though some vendor quickly reacted or even offered security patches a year ago[19] (which was before the Mirai attacks), a lot of users never applied the security updates to their devices, allowing the attack to succeed. Thus, to some extent, it is more important to educate the public about awaring the security and privacy issues in their everyday life than to consider the technical approaches to deal with those attacks and threats.

D. suggestions on resolve security threats in IoT application layer

Information security management methods including better approaches to patching, updates, and provisioning of information to application layer of IoT are missing. In some specific cases of IoT appliaction layer such as the smart home, a need for the integration of security in design and of sound secure management processes is typically not included in the development of smart connected homes[4].

For the user, the IoT information is kind of black-box for them. They do not know what data has been grabed by the IoT system, what data has been uploaded and what and where the data or infomation of them was utilized at last. They don't know if the service provider could be trusted. So an authoritative third party auditing supervisory organization should be established.

REFERENCES

[1] Sahar S. Tabrizi Dgan Ibrahim, *Security of the Internet of Things: An Overview*,2016 ACM

[2] *Service-Oriented Architecture (SOA) Definition*