Internet of Things (IoT): A New Frontier for Identity

Loshima Lohi,
Asst.Professor on Contract
Department of Computer Science
Carmel College, Mala

***Abstract* -- Cyberspace and real life are merging. With the Internet of Things (IoT), individuals and devices are increasingly connected to the Internet and physical objects are effortlessly integrated into information networks. Robots andMachines are able to sense and analyze data, enable control of the physical world from a distance. The IoT will modify the way we live, communicate andwork. No business will be unaltered in the long term. But these big changes raise new challenges, mainly with respect to security.**

Security is essential for IoT, especiallywith respect to identity. If we are going to connect our houses, cars, company and factories to the Internet, they must secured. Individuals, machines, home appliance and devices must be securely identified so that only allowed access is permitted. Private user data and corporate secret must be protected from theft and fraud. And all of this must be easy to use – not compromise user experience. Therefore, security should be planned into IoT systems from the beginning, not track on later.

Keywords -- Identity, IoT, Security

I. INTRODUCTION

In the Internet of Things (IoT), everything real becomes virtual, which means that each person and thing has to be locatable, addressable, and readable counterpart on the Internet. These virtual entities can generate and consume services and collect toward a common target. The user's phone knows about his physical and mental state through a network of devices that surround his body, so it can act on his behalf. The entrenched system in a swimming pool can share its state with other virtual entities. With these features, the IoT promise to extend "anywhere, anyhow and anytime" computing to "anything, anyone, any service."

II. THE IMPORTANCE OF SECURITY HARDWARE FOR IOT

Stuxnet, BlackEnergy, and several other recent attacks have shown that IoT systems cannot be adequately protected with software alone. Security software is simply bypassed by clever and smart attackers, who can then remotely control physical systems. The combination of software and hardware offers best possible balance between security and flexibility. Security chips provide protection even if software is compromise [1].

.

III. SECURITY CHALLENGES OF IoT

Here are main three key IoT security challenges:

A. A trillion points of vulnerability

Every single device and sensor in the IoT represent a potential risk. How poised can an organisation be that each of these devices havethe controls in place to preserve the secrecy of the data collected and the integrity of the data sent.

Researchers at the French technology institute Eurecom downloaded 32,000 firmware images from potential IoT device manufacturers and discovered 38 vulnerabilities across 123 productsincluding poor encryption and backdoors that could allow unconstitutional access. And one weak link could open up access to hundreds of thousands of devices on a network with potentially serious consequences.

B. Trust and data integrity

Corporate systems will be bombarded by data from all manner of linked sensors in the IoT. How confident can an organisation be that the data has not been compromised or interfered with?[2]

Take the example of utility companies automatically collecting readings from customer smart meters. Researchers have already demonstrated the smart meters broadly used in Spain, for example, can be hacked to under report energy uses. They were able to spoof messages being sent from the meter to the utility company

and send false data. In current years we have been able to go to a high street store and buy anti-virus protection on a disc or download it straight to our PC. But in the IoT (Internet of Things) that security capability doesn't exist in many of the devices that will rapidly become connected.

C Data collection, protection and privacy

The vision for the IoT is to make our everyday lives easier and enhance the efficiency and productivity of businesses and employees. The data collection will help us make smarter decisions. But this will also have an influence on privacy potential. If data collected by connected devices is compromised it will weakenthe trust in the IoT. We are already seeing the consumers place higher expectations on businesses and governments to safeguard their personal information.

And beyond that, what about the security that protect the critical national infrastructure (CNI), such as oil fields and air traffic control? With everything connected, the IoT smashes the division between the CNI and the consumer world.[1]Everyday house items could potentially be exploited by cybercriminals to achieve access to the CNI.

Businesses need start now to identify the risk level for their current disclosure to the IoT and where it is going in the future and also think about the privacy and security implications associated with the volume and type of data the IoT will generate.

It truly is a brave new world that promises many exciting opportunity. Trust is the foundation of the IoT and that needs to be underpinned by security and privacy. And it's a discussion we all need to start having now if we are to reap the benefits of the connected world.

IV. USER IDENTITY FOR IOT

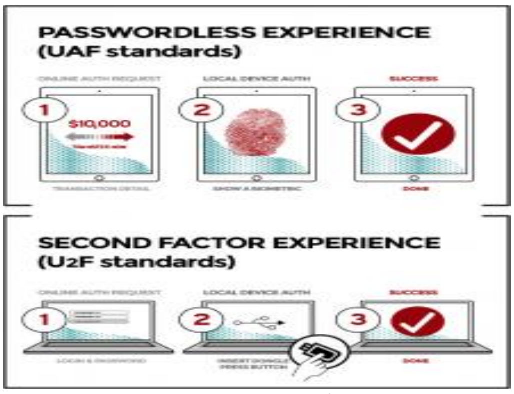

Figure 1: User identity for IoT

IoT users require remote access to their devices from anywhere and any location, but still need ease of use and strong security. Username and password confirmation fails to meet these requirements since passwords are painful to enter and easily stolen. Recently, the FIDO (Fast Identity Online)Alliance released standards for an open, scalable, interoperable set of multiple-factor authentication mechanism. IoT users benefit from FIDO (Fast Identity Online) in two ways. First, they get stronger security. Second, the complexity of control device credentials is hugely reduced. As illustrated in Figure 1, FIDO permits users to combine their online accounts with a local hardware security token. Then they can use this token to confirm and other systems, either with or without a PIN.

IV. DEVICE IDENTITY FOR IOT

With the rise of IoT, device security and specially identity is more important than ever. IoT devices control critical systems like cars, factory systems, door locks, and security cameras. Yet they are showing to a variety of network-based threats. To block unauthorized parties and provide security, IoT devices must be able to conduct mutual verification with users[1], other devices, and the cloud. Fortunately, device identity technology are well established and widely available.

Cryptographic validation is the best approach to IoT device identity. IoT devices are fully able of establishing, maintaining, and employing long cryptographic keys. And there is no reason to employ passwords for device identity. With security hardware, these cryptographic keys can be protected against leak.

Some security chips – such as the open standard Trusted Platform Module (TPM) – go further than establishing device identity by also performing encryption and detecting device negotiation. Monitoring system integrity is especially important for IoT because a rogue device with proper identification can cause real physical damage.

V. IDENTITY FOR THE INDUSTRIAL INTERNET

The industrializedinternet is the application of IoT concepts and technologies to industrial purposes. For example, next-generation manufacturing uses networking to integrate the entire supply chain from supplier and customer, enable suppliers to customize production to match demand. In such an environment, identity must be verified and communications must be protected end-to-end to make sure that customer demand is properly met. Therefore, all elements of the system from customer to supplier must be secured in all ways.

To improve system security and integrity, security controllers can be integrate in all parts of an Industrial Internet system from a tablet used by customers ordering products to the factory line where the products are manufactured and beyond into shipping, distribution, wholesale, and retail. These security chips can establish product, device, and user identity, perform encryption and authentication, and maintain device integrity. Furthermore, these security solution offer protection of sensitive IP and process knowhow.

VI. CONCLUSION

In the Internet of Things (IoT), strong identity for users and devices is required. Without a strong identity, attackers can cross the cyber boundary. Such attacks are taking place now. Because of the many applications of IoT technology, the impact of these attacks is not controlled to the smart home or connected cars, but extends to industrial automation, health care, and many other domains. Fortunately, standards and technologies for strong identity are available without sacrificing easiness of use. Hardware security is required to limit the impact of software vulnerabilities. When designing IoT systems and other systems that link cyberspace and the physical world, strong identity implement with secure hardware should be a requirement. Only in this manner it can be protectedsafety.

REFERENCES

[1] IoT: A new frontier for identity- Steve Hanna – 12 Jan 2015- http://www.secureidnews.com/news-item/iot-a-new-frontier-for-identity/

[2] Article - 3 key security challenges for the Internet of Things – Raj Samani - http://www.securingtomorrow.com/blog/ knowledge/3-key-security-challenges-internet-things/