Cyberphysical Security for the Masses: A Survey of the Internet Protocol Suite for Internet of Things Security

Narayanan Srinivasan, UWIN ID 105192312
Project Number 17, Email ID: srini11b@uwindsor.ca

I. ABSTRACT

In the recent years, the design and development of devices connected to the Internet (aka., Cloud) have increased exponentially. This is due to the device's ability operate connected to a network by collecting and exchanging data offering numerous real-world applications. In this survey we will discuss about the capabilities of such devices connected to physical entities and the security challenges posed by them. The devices which are connected to a network is commonly known as Internet of Things (IoT). The development of IoT are taking place at a fast pace, where the IoT devices are growing increasingly heterogeneous and innovative. Primarily, due the availability of open-source software, advancements in embedded IoT and creation open standards for IoT communication. Furthermore, the development of IoT has created numerous applications which led to the interaction of networked devices with the physical domain. This interaction of IoT with physical things are known in other terms as cyber-physical systems.

Keywords—Internet **of** Things **(**IoT), Cyber Physical Systems (CPS), IETF, Network security, Software security.

II. INTRODUCTION TO CYBERPHYSICAL SYSTEMS

The concept of cyber-physical systems arises from the architecture of Internet of Things where the various devices are networked to form interconnected systems. The unique feature of such interconnected systems is that they can monitor and manipulate real-life tangible systems and processes that have physical outcome. In a cyber-physical system (CPS), the integration between the two systems are performed corresponding to the applications, technologies, and standards Despite their inherent advantages the interconnected systems with physical capabilities have wider range of mission critical applications in real-life. Consequently, when these systems are compromised in the cyber sector then the physical systems can be manipulated corresponding to the attacker's objectives. This paper also surveys the vulnerabilities, threats, attacks on the cyber-physical systems that are connected via IoT while identifying the key issues, and challenges faced.

III. THREAT MODELING IN CPS

Threat modelling is performed to collect a list of assets that need protection in the system. After the threat modeling, threat analysis is carried out to analyze what kind of attacks can be performed on the listed assets. Considering the impact of the attack carried out on the asset the threat model is ranked accordingly to recognize the types of commonly occurring attacks and security problems. Generally, there is specific type of threat model used to rank and analyze the threat to the assets. However, it is a good practice to reconsider analyzing the commonly occurring security threats in terms of IoT security.

IV. CATEGORIES OF ATTACKS

In this survey, we mainly focus on the types of threats that are classified by Internet Engineering Task Force (IETF) which is based on an ensemble of standardization bodies, industry groups and professional organizations. We analyze the extent of the threat to the standards set by the IETF where it focuses on the network and cyber-based threats, vulnerabilities, attacks, and challenges. According to the standards, the attacks to the assets is classified based on the threat model as network or communication attacks, software attacks and hardware attacks.

1. Communication Attacks
2. Software Attacks
3. Hardware Attacks

V. SECURING IOT BY IETF AND ENISA SECURITY STANDARDS

Once the threats on CPS are collected and analyzed as per the security standards. By considering the threats, the decisions for securing the assets are carried out based on the security standards set by the Internet Engineering Task Force (IETF) and recommendations from E.U. Agency for Network and Information Security (ENISA).

A. Authentication and Communication Security

The authentication of signals and secure communication lines are primary security requirements to a secure CPS. There needs to be a high-level of signal integrity, confidentiality, and authentication to the interaction between multiple devices in the CPS so that the communication layer is secure from any threats. Here in this the communication security is carried out not only on the single point-to-point signal but on the overall communication link layers, application layer gateways and device ports. Thus, following the standards given above on the communication network is secured from multiple avenues of approach for attack.

1. End-to-End Security

The end-to-end security approach for securing a communication network is performed over a IoT device connected to the cloud or remote server via a transport layer in a network infrastructure. The end-to-end security can be improved by following the security best practices mentioned by the IETF and ENISA guidelines which protect the network and data transferred. The end-to-end security measures are used in the User Datagram Protocol (UDP), Transmission Control Protocol (TCP), Transport Layer Security (TLS) and Datagram TLS (DTLS).

2. Object Security

In object security the primary data transferred in the communication such as files, sensor data or audio etc., are encoded into objects for the purpose of transferring them to different applications. These objects are data encoded in a specific format which are passed to the other applications via the network. Some of the types of objects used for data transfer are Concise Binary Object Representation (CBOR), JavaScript Object Notation (JSON), Concise Object Signing and Encryption (COSE), Constrained Application Protocol (CoAP).

B. Authorization and Access Control

Numerous IoT devices are designed for integration with the smart home application such as thermostats, door locks etc. When multiple devices are placed in a specific environment, their interaction with each other, and the user raises numerous issues. Here the security standards are mentioned by the IETF Authentication and Authorization for Constrained Environments (ACE). In such ecosystem, the security of IoT devices is vulnerable as the chances of inadvertent access are higher. Furthermore, the management of access control policies are sone by JSON Web Token (JWT), scalability, and implementation of strong authentication mechanism such as ACE-OAuth for securing the IoT assets are used.

C. Key Management

The IoT devices requires keys for enabling remote management of functions and services. The creation of IP for Smart Objects alliance on credential management for IoT devices lay down a common security layout of credential and key management in IoT devices. The importance of key management lies in the fact that in allows use to prevent unauthorized access to the IoT assets via untrusted connection or malicious code. The process of key management is offering a provision for implementing long-term credential which is then used to provision further keys. Such process is called bootstrapping. Many organizations have designed key management protocols to offer bootstrapping functionality.

D. State-of-the-Art Cryptography

Cryptography is the used of mathematical algorithms to encrypt data. It is relatively slowly, taking years in developing tools and the methods used take long time to develop, test, publish and standardize. Even though the use of cryptography is widespread it is expensive to develop new function for every application. Hence, many IETF groups are relying on the recommendations of Internet Research Task Force. In terms of IoT devices, the current cryptographic standards offered are insufficient, or not suited for IoT applications. The cryptographic standards in IoT are classified into symmetric key cryptography which uses a set of symmetric encryption algorithms and asymmetric key cryptography which is used is limited functionality due to IoT hardware constraints.

E. Firmware and Software Updates

Offering consistent updates to the IoT device firmware and software is an excellent strategy for securing the IoT assets from threats that are detected and rectified in the system. While it may seem obvious, updating the IoT devices over the network offers ability to improve the overall architecture, enhance security and creating additional functionalities. software the IETF SUIT is working for developing standards for updating the firmware and software on IoT devices via network.

F. Restricting Communication

IoT devices works to offer applications via numerous communication protocols. But this functionality must be restricted as the attacker can compromise the IoT device, systems and network via the communication or the network layer. The assessment of communication protection was carried out by the IETF Network Endpoint Assessment (NEA). The IoT devices faces challenges when deciding which communication endpoints must be secured and which must be restricted to access by creating policies that manage them.

VI. SECURITY CHALLENGES FOR IOT PRODUCT DEVELOPMENT

Developing IoT products is aligned with the specific use case and environment creates numerous challenges in the security aspects. The IoT Security Standards are designed by IETF for the above mentioned six avenues of IoT environment. Beyond these, there are some issues outside the scope of IETF affecting the security aspects of IoT ecosystem as mentioned below.

1. Integration with other Systems
2. Gaps in Implementation
3. Open Standards vs Proprietary Solutions
4. Advanced Cryptographic Solutions for IoT
5. Selecting a Key-Management Solution
6. Choosing a Communication Security Paradigm

VII. CONCLUSION

Designing a IoT product or application offering complete capability and overall security is a matter of delivering a clever balance between contrasting values that are critical to the IoT user and application. In this article, we focus on the possibility of developing a reasonably secure IoT system where the predesigned standards by IETF are used to design a secure IoT system instead of relying on a homegrown solution. To allow development of secure IoT systems the IETF has created the security standards with large, in-depth, and elaborate scope of work. Furthermore, such IETF standards to IoT ecosystem offers scope for optimization, configuration potential within the framework of IETF-developed IoT security standards to design advanced IoT system.

VIII. REFERENCES

[1] Hannes Tschofenig and Emmanuel Baccelli, “Cyber-physical Security for Masses A Survey of the Internet Protocol Suite for Internet of Things Security” IEEE Security & Privacy, Volume:7, Issue:5, Sept-Oct. 2019. https://ieeexplore.ieee.org/document/8764344.