Study on IOT Architecture and Protocol for Wearable Devices

Anjana R
Department of CSE
Shiv Nadar University Chennai

1. Abstract

Wearable devices are parts of the essential cost of goods sold (COGS) in the wheel of the Internet of things (IoT), contributing to a potential impact in the finance and banking sectors. There is a need for lightweight cryptography mechanisms for IoT devices because these are resource constraints. —In this digital world Internet of Things plays major role in different fields. These IoT devices are extended from Wireless Sensor Network (WSN). s. The proposed protocol allows the customer to buy the goods using a wearable device and send the mobile application's confidential payment information. The application creates a secure session between the customer, banks and merchant. The static security analysis and informal security methods indicate that the proposed protocol is withstanding the various security vulnerabilities involved in mobile payments. For logical verification of the correctness of security properties using the formal way of "Burrows-AbadiNeedham (BAN)" logic confirms the proposed protocol's accuracy. The practical simulation and validation using the Scyther and Tamarin tool ensure that the absence of security attacks of our proposed framework. Wearable technology adds to mobile technology to offer higher efficiency and improve security in communication and payments. There is a demand for designing the secure protocol for wearable device environments. To answer this, we need an experience of digital payments through wearable devices; a secure end-to-end micro payment protocol for wearable devices is introduced. NFC for device pairing and a lightweight cryptography algorithm of ECC for achieving security features are used.

keywords: Internet of things· Wearable device· Mobile payments· ECIES · BAN logic· Scyther· Tamarin

2. Introduction

The rapid growth of the wearable device payment transaction from the last five years shows the massive impact on the wearable market, banks to provide more and more features and convenient services such as payments, notifications, purchase of stocks to the customers. Wearable technology is a part of an emerging trend that is the internet of things(IoT). As we know, IoT is about connecting devices that help to optimize operations,boost productivity, lower costs and improve lives. In current days, many applications such as healthcare, mobile banking, mobile payments, vehicle monitoring, home monitoring, etc., are implemented with the help of the Internet of Things (IoT). All these IoT applications are implemented with the support of different sensor devices. In addition to these sensors,security plays a crucial role in performing online transactions for financial sector applications security. These banking and financial sector applications use wearable sensor devices such as smart glasses, smart uniforms, smartwatches, smart jewellery etc. Wearable payments have made a tremendous impact on global payments. The wearable payments amount will increase from 3,1$billionin2015to501.1$ billion by 20201 and the tremendous growth of market value for wearable technologies globally from 2012 to 20182.

The wearable devices are used to offer various services, namely payments to the banking. The devices rely on a wide variety of wireless communication protocols supporting different communication ranges. Other wearable devices, namely wearable sensors, will transmit sensitive information to mobile user applications through establishing secure SSL/TLS communication.The SSL/TLS communica-

tion is essential for banking and financial transaction purposes,and it is achieved through mutual authentication and subsequent session key generations. Hence, SSL/TLS is a challenging task for application developers. Wearable communication is opened for several well-known attacks such as man-in-the-middle (MitM), replay, stolen mobile terminal or wearable device, device impersonation, eavesdropping, etc

3. System Models

This section deals with the two models one is the network model another one threat model, which are adopted in the proposed model

Network Model
The architecture for wearable devices is shown in Fig. 4. It consists of six types of entities, such as Issuer bank (IB), acquirer bank (AB), payment gateway (PG), a certification authority (CA), mobile terminal, and wearable sensing devices. The person using various wearable devices such as a smartwatch, smart wristband, smart glass, etc. In the architecture, a wearable device is connected to the mobile terminal through NFC. An app is running on a mobile device. Wearable devices are resource constraints because they have limited computing capabilities regarding battery, display, storage, and processing compared to a mobile terminal (smartphone). Hence, NFC is used to pair the wearable device and mobile terminal for transmitting public messages. Before conducting any transaction with the merchant, the customer and merchant should register their mobile numbers with the bank.

Threat Model
The threat model helps in understanding how an adversary can exploit various attacks in real-time traffic. The adversary's main objective is to violate the security properties such as Confidentiality, Authentication, Authorization.In a threat model, the attacker implements a "Man-in-the-Middle (MitM)".The attacker is actively present in the network and monitors the traffic between the end-user and server. The attacker always tries to establish the HTTP traffic instead of HTTPS between the Wi-Fi access point, user, and server. On the other hand, the attacker has a self-signed certificate, a fake or outdated certificate. Meanwhile, the attacker sends a fake certificate to the mobile application. In this way, the adversary exploits the MitM attack. This scenario is possible only when the mobile app receives a fake certificate or lack of certification pinning.

4. Proposed Architecture

The new protocol ensures the end-to-end security at the application layer for financial transactions. This payment model uses a digital signature mechanism based on ECC. The proposed protocol was analysed by static testing, formal and informal verification, and logically proved with BAN logic's help. Hence, the proposed payment protocols provide robust and without violation of security properties of authentication, data integrity, confidentiality, and non-repudiation. Finally, this mechanism supports payment secrecy, forward secrecy, order secrecy, preventing overspending, money laundering, and double-spending. In addition to this, the proposed payment protocol withstand replay, MitM, and impersonation attacks. The proposed protocol's security properties are successfully verified using BAN logic, Scyther, and Tamarin tools
The proposed framework is divided into three phases.

(i) Registration phase: In this phase, the customer, merchant and wearable device are acquiring the keys from their banks.

(ii) Authentication and Transaction initialization phase: Once keys are acquired from the banks, when the user needs to purchase the goods via a wearable device with a merchant, they should pair with the mobile device and a wearable device with a secure NFC connection. The wearable device is sent authentication information as well as payment order information to the mobile application. The mobile app connects to the customer's bank server, i.e. issuing bank (IB), once the IB validates the user's informa-

tion via a secure SSL/TLS network.

(iii) Notification phase: In this phase, the banks sent successful/unsuccessful information as SMS to the customer and merchant

5. Protocols

The IoT data protocols are mainly used connect with low power IoT devices. These protocols are providing point-to-point communication to the physical hardware at the user end. IoT devices transfer data from sensors over the Internet. In direct to perform the IoT communication with high level quality in a large-scale network for real-time data collections; protocols should need on appropriate features such as low packet loss, high packet creation time and low packet response time etc.

A) MQTT Protocol

MQTT (Message Queuing Telemetry Transport) is a lightweight messaging protocol it's provides constrained network clients with a simple way to distribute telemetry. MQTT is a TCP-based publish-subscribe protocol invented by IBM and then open-source for simple messaging communication applications. In working technique of publish-subscribe format of an asynchronous communication procedure in which message or data are exchanged between applications without knowing the sender and receiver identity, clients can either "publish" data on a specific topic to the server or "subscribe" to a topic where the server automatically will send new data on the topic to the subscriber registered. MQTT capabilities of one-to-one, one-to-many and many-to-many publish subscribe format with TCP based communication.

B) CoAP

An IoT supports Constrained Application Protocol (CoAP), and it is defined in RFC 7252. The functionality of CoAP is similar way to Hyper Text Transmission Protocol (HTTP) it is specifically designed for constrained based devices. The nodes constrained devices to communicate with the wider Internet using UDP protocols in addition, the communication between Server and Client is peer-to-peer and Server or Client can response unicast and multicast requests[12]. Constrained Application Protocol (CoAP) is used as a web transfer protocol. Constrained 8-bit microcontroller nodes with small random access memory (RAM) and read only memory (ROM) whereas constrained network results are having high packet error rate commonly used for machine-to-machine (M2M) applications.

C) AMQP

The Advanced Message Queuing Protocol (AMQP) is open-source applications are free protocol in IoT with binary data designed to professionally support a wide variety of messaging in application layer protocol previous to AMQP, developers are used different message brokering and transferring applications their own, on this case they more difficulty work with another. AMQP have the functionality in networking takes place and the same message broker applications work of two processes. This protocol supports different transport protocols for transmitting large amount of data it an underlying reliable transport protocol such as TCP. AMQP takes responsibilities of asynchronous publish/subscribe communication in data transfer. The main advantage of AMQP is store-and-forward feature that ensures reliability after network interrupt. It gives ensured message-delivery guarantees with at-most -once: the sent once whether message delivered or not, at-least-once: one time definitely the message will be delivered or possibly more. Exactly once: only one time the message will be delivered. Security issues are handled by TLS/SSL protocols over TCP.

D) BLE Protocol

Bluetooth Low Energy (BLE) has become the primary transmission media due to its extremely low energy consumption, good network scope, and data transfer speed for the Internet of Things (IoT) and smart wearable devices. With the exponential boom of the Internet of Things (IoT) and the Bluetooth Low Energy (BLE) connection protocol, a requirement to discover defensive techniques to protect it with practical security analysis. Unfortunately, IoT-BLE is at risk of spoofing assaults where an attacker can pose as a gadget and provide its users a harmful information. Furthermore, due to the simplified strategy of this protocol, there were many security and privacy vulnerabilities. Justifying this quantitative security analysis with STRIDE Methodology change to create a framework to deal with protection issues for the IoT-BLE sensors. Therefore, providing probable attack scenarios for various exposures in this analysis, and offer mitigating strategies. In light of this authors performed STRIDE threat modeling to understand the attack surface for smart wearable devices supporting BLE. The study evaluates different exploitation scenarios Denial of Service (DoS), Elevation of privilege, Information disclosure, spoofing, Tampering, and repudiation on MI Band, One plus Band, Boat Storm smartwatch, and Fire Bolt Invincible

D) Lightweight Protocol

It comprises protocols for lightweight encryption, authentication as well as key management. The key management protocol is the application of our early work on information theoretically secure key management to IoT; it is computationally efficient and information-theoretically secure, and enables that every data item (file) is encrypted with its own random key. The security and computational efficiency of the proposed protocols are compared with those of IPsec, which is the most commonly used suite of network-layer security protocols in Internet based applications but not desirable, due to its computationally-intensive procedures, to IoT applications and cyber-physical systems (CPS) with resource and computation-capability constraints. The proposed security protocols can be employed in IoT and CPS applications, replacing the IPsec core algorithms or the whole IPsec suite, to achieve a higher level of security with a very low resource consumption that helps to maintain the system sustainability.

6. Conclusion

An IoT is not a single component which includes concepts of network, power, data transmission, delay time, bandwidth and etc... Which generate an enormous amount of data, and among the devices they are shared the data. Various types of fields seamlessly need these IoT devices for forthcoming automation process with low power consumption. Also processed information is used for critical and non-critical decision-making so it will leads to new Internet world. Which generate an enormous amount of data, and among the devices they are shared the data. Wearable technology adds to mobile technology to ofer higher efciency and improve security in communication and payments. There is a demand for designing the secure protocol for wearable device environments. To answer this, we need an experience of digital payments through wearable devices; a secure end-to-end micropayment protocol for wearable devices is introduced. NFC for device pairing and a lightweight cryptography algorithm of ECC for achieving security features are used. The proposed protocol is executed mutual authentication between various entities involved in the protocol using the BAN logic. In addition to this, for security analysis, advanced simulation tools, namely Scyther and Tamarin, are used. The proposed work is implemented and compared with existing communication cost, computational cost, security features, phases, entities, application and cryptography algorithm. Implementation results show that the proposed protocol is suitable for real-time payments with banks and IoT environments. To make the proposed protocols more secure can add biometric-based authentication can be added.