ISSN 2395-1621

IOT Transaction Security

[#1]Jogdand Gopal, [#2]Kadam Shubham, [#3]Patil Kiran, [#4]Mate Gaurav

[2]kadamshubham66@gmail.com

[#1234]Department of Computer

JSPM's Imperial College of Engineering and Research,
Wagholi, Pune University, Pune.

ABSTRACT

Vulnerability(s) and attack(s) can occur on the proxy or during translation protocol of secure transport protocols in Constrained Application Protocol (CoAP). Existing security countermeasure deploys Datagram Transport Security layer (DTLS) and Transport Security layer (TLS) between client and server as loT (Internet of Things) communicating entities. Proxy plays the role of interface between client and Server. It can also decrypt the received message and encrypt data according to the used security transport protocol of the other side. The vulnerability appears during this phase, especially, where the proxy is not confident or supervised by an illegitimate entity. Consequently, passing through the proxy communication node, security services like confidentiality and integrity can easily be compromised. Exploiting advantages of studied cryptographic algorithms, we focus on our customized security objectives regarding proxy element and DTLS-TLS translation. We detail, in this paper, the algorithm and the sequence diagram of secure communication of our proposal adapted for CoAP architecture. As an encryption strategy, we follow the cryptographic envelope principle based on ID-KEM and Three-pass Protocol. As a hypothesis, we assumed that the communication deploys our recent IDMS (Identity management System) contribution for loT, relying on the EAP _OAuth2.0 (Extensible Authentication Protocol and Open Authorization Protocol) protocols via DTLS, as the starting phase in order to keep authentication and authorization services. Finally, we describe the security validation, present our perspectives and conclude our work.

Keywords-CoAP, DTLS, TLS, vulnerabilities, security, proxy, IBE, loT, ID-KEM, Three Pass Shamir Protocol.

ARTICLE INFO

Article History

Received: 12th December 2017

Received in revised form :

12th December 2017

Accepted: 14th December 2017

Published online :

14th December 2017

I. INTRODUCTION

Secure communications via the Internet depends on different layers of OSI model. Encryption and decryption are techniques used to maintain confidentiality, authentication and integrity during session communication. Indeed, TLSl.O (Transport Layer Security), which provides such security services, has been considered as the most popular security protocol since 1996 [1]. It is based on TCP (Transport connection Protocol) or connected mode. Nowadays, the number of communication protocols and applications is increasing dramatically. Hence, the ubiquity of loT (Internet of Things) imposes the use of UDP (Unit Datagram Protocol). Time of UDP processing is faster than that of TCP processing due to the absence of acknowledgement packets and the lowest number of check processes for the provision of end-to-end transport. Consequently, the device energy will be maintained for a long period. By studying the CoAP protocol [2], a new vulnerability resides in the proxy. The aim of this work is to increase the level of security by introducing a modified identity based key encryption method (ID-KEM) protocol. The authors propose tailored security for CoAP communication. Taking into account that the communication takes place between three actors, we integrated three-pass protocol in order to exchange the data encryption secret between client and server via a malicious proxy. As soon as DTLS is established between client and proxy and TLS is established between proxy and server, the client and the server exchange an encryption secret using the ID-KEM protocol based on a three-pass protocol to ensure confidentiality and the integrity against the tilting of TLS -

DTLS translation at the level of the proxy. In section II, we compare TLS and DTLS[3]. Indeed, we explain the major drawbacks of TLS to be deployed in loT transactions, which makes difficult its application in loT. Unsuitable TLS characteristics with UDP have been resolved in DTLS [4]. Sections III shows the attacks on (D) TLS as well as weaknesses and motivation in loT. Section IV is reserved to the possible counter-measures deploying robust cryptography. After discussion, section VI details our proposal. Section VII represents the secure communication algorithm and describes the validation of the enhanced secured transaction. Finally, we present our perspectives and conclude our work.

II. RELATED WORK

Provide IOT transaction security

Studies affirmed that possible counter-measures are summarized in three possibilities: upgrading to the newest protocols versions, "the inclusion of a dummy zero-length message prior to each real TLS message", using RC4 (which is not supported by DTLS) instead of MAC-CBC-Encryption or deploying algorithm of authentication encryption [8][9]. Thomas Kothmayr and al. proposed a two-way authentication architecture for loT-based on DTLS to address the vulnerabilities [10]. Their approach does not take into account DTLS-TLS mapping used in default model for CoAP. Pascal Urien introduced an innovative DTLSffLS security modules embedded in SIM cards and integrated into the user's mobiles [11]. The features of such embedded module are to lock (using COAP-DTLSSIM) or to download an encryption key (using TLS-SIM API). In this case, the SIM soft element (embedded in user device) operates over UDP with a DTLS-CoAP server via Near Field Communication (NFC) and TLS-Server-Key of the user's home-domain. In our work, we implemented a different scenario. In fact, in the studied case, client and proxy are physically two different elements. Indeed, the proxy acts as NAC (Network Access Control) element of the visited domain. This proxy should interact via HTTP/TCP with the server (resource server like a sensor, resource application like e-health service). But, with the client, the proxy should communicate via CoAP/UDP. Recent works have aimed at maintaining security by using end-to-end security, deploying AAA services [8] [12]. Although, in these studies, all packets are decrypted and reencrypted by the proxy, vulnerabilities persist. Because no entity trusts others during the transaction, some works, in traditional internet ecosystem, deployed threshold cryptography as a strong algorithm type based on complicated mathematical functions to avoid eavesdropping and maintain data integrity of legal entities.

III. PRESENT SYSTEM AND CHANGES

Attacks on (D)TLS In this section, we enumerate the different attacks on (D)TLS [5] [6] [7]. These attacks can be grouped based on three hacked channels:

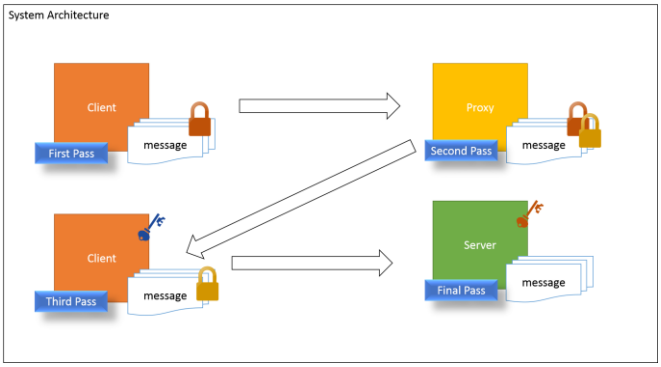
• The implementation (weakness of the checking process): Random Number Prediction, Wildcard Certificate Validation, Vulnerable Certificate Validation Libs, Weak Random Numbers, Null Prefix Attacks Against Certificates, ECC-Based Timing Attacks, Certificate Validation Issues, "Heartbleed" and "FREAK".

• The protocol or the used cryptographic algorithm and design: MAC does not Cover Padding Length, Cipher Suite Rollback, ChangeCipherSpec Message Drop, Bleichenbachers Million Questions, Weaknesses Through CBC Usage, Colliding Certificates, Renegotiation Flaw, Message Distinguishing, Key Exchange Confusion, BEAST, CRIME, Lucky Thirteen, RC4 Biases, BREACH, POODLE, Logjam.

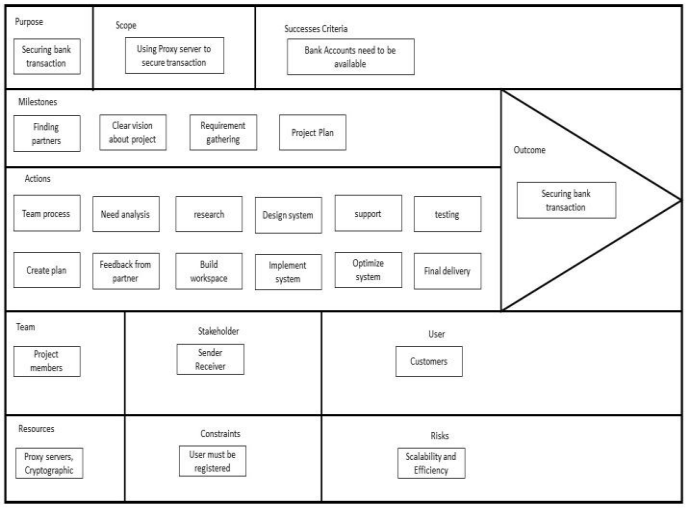
• The end-user: refers to any communication part like client or server: SSL strip, Conquest of Comodo CA, Conquest of DigiNotar CA, Accidentally Issuing of Certificates by TURKTRUST, Weak Certificates by DigiCert Malaysia CA, Risks Caused by Unqualified Domain Names and usability. All these attacks are cryptographic and need man in the middle (MITM) hacker to be achieved. B. Weaknesses and Motivations in loT With loT applications, deployment of (D) TLS becomes increasingly widespread. In loT communication stack, many challenges must be taken into the account. Constrained Application (CoAP) is the used protocol in loT devices. CoAP was invented to respond to requested challenges of smart objects instead of HTTP. These challenges reduce IP impact, code size (by compression), energy consumption, interoperability and auto-configuration. They also minimize the checking processes guarding to low capacities (memory and processor). Communication steps of loT constrained communication take place using two transport protocols. In other words and as depicted by next picture, UDP and TCP must be deployed in the same transaction. Hence, such applications are sensitive to:

• TCP and UDP,
• TLS and DTLS weaknesses and attacks,
• Transparent layer DTLS-TLS mapping using a dedicated proxy,

• Proxy security policy and vulnerabilities of TLS-DTLS and DTLS-TLS translations. As depicted in figure. 1 , Decryption and re-encryption, in the proxy, have an impact on all traffic flowing between client and server. Consequently, there is a risk of confidentiality and integrity violation. In our proposal, we assume that each entity does not trust the other party.



ARCHITECTURE OF IOT TRANSACTION



IDEA CANVAS

IV. METHODOLOGY

The **three-pass protocol** is a cryptographic protocol that allows two people to communicate privately without having to exchange keys in advance. It is based on commutative encryption, i.e. an encryption method *E*, and its corresponding decryption method *D*, which allow a message encrypted with two different keys to be decrypted using those keys in either order.

The protocol gets its name from the fact that transmitting a secret message *M* from John to Tom requires the exchange of three messages:

John→Tom:$CA=E(KA,M)$

Tom→John:$CAB=E(KB,CA)$

John→Tom:$CB=D(KA,CAB)$

Tom then calculates

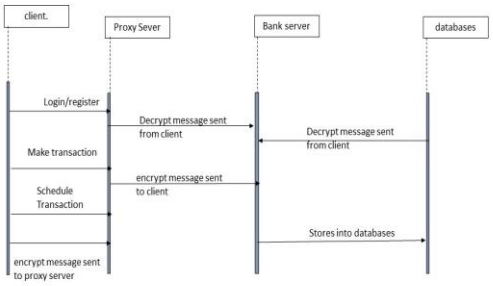
$M=D(KB,CB)=D(KB,D(KA,E(KB,E(KA,M))))$.

Because (E,D) is a commutative encryption method, the decryption succeeds even though it's done in the "wrong order".

For the three-pass protocol to be secure, an attacker observing the encrypted messages *CA*, *CAB* and *CB* must not be able to determine the secret message *M*. A trivial implementation of the three-pass protocol using a synchronous stream cipher $E(K,M)=D(K,M)=S(K)\oplus M$ is *not* secure, since an attacker can calculate

$CA\oplus CAB\oplus CB=(SA\oplus M)\oplus(SB\oplus SA\oplus M)\oplus(SB\oplus M)=M$,

where $SA=S(KA)$ and $SB=S(KB)$ are the keystreams used by John and Tom.



Flow Diagram

V. CONCLUSION

This paper addresses the vulnerabilities of TLS/DTLS translation via proxy in CoAP communication. As a countermeasure, we proposed an adopted secure architecture deploying cryptographic envelop. Three- pass protocol is already demonstrated as secure. The unique weakness of three-pass protocol is that it do not preserve/assure authentication. But, in our work, we assume an IDMS is implemented, using EAP _OAuth2.0 protocols, in order to maintain authentication and authorization as the first phase of the secure transaction. Hence, authentication, authorization, confidentiality and integrity are preserved thanks to EAP _OAuth2.0, as a first step, and the modified ID_KEM based on the "Three-Pass Protocol of Shamir" as the second step. Our future work will focus on deploying this proposal in a real application.

REFERENCES

[I] [TLS]: T. Dierks. E. Rescorla. "The Transport Layer Security (TLS) Protocol". rfc5246. August 2008.

[2] [CoAP]: Z. Shelby. K. Hartke, C. Bormann. "The Constrained Application Protocol (CoAP)". rfc7252, June 2014.

[3] [DTLS]: E. Rescorla, N. Modadugu. "Datagram Transport Layer Security Version 1.2". rfc6347,January 2012.

[4] H. Tschofenig, Ed, T. Fossati. " Transport Layer Security (TLS) IDatagram Transport Layer Security (DTLS) Profiles for the Internet of Things". rfc7925, July 2016.

[5] Henry Corrigan-Gibbs and Suman Jana. "Recommendations for Randomness in the Operating System or, How to Keep Evil Children out of Your Pool and Other Random Facts. 15th workshop on Hot Topics Operating Systems, May 2015.

[6] [Attacks]: Attacking SSL when using RC4. Hacker Intelligence Initiative, Imperva, Inc. March 2015. Web link: https:llwww.imperva.com/docs/hu_attacking_ssLwhen_usingJc4.pdf

[7] Y. Sheffer, R. Holz, P. Saint-Andre. "Summarizing Known Attacks on Transport Layer Security (TLS)and Datagram TLS (DTLS)".rfc7457, February 2015.

[8] Constantinos Kolias, Angelos Stavrou et ai, "Learning Internet-of-Things Security 'Hands-On'", Journal: IEEE Security and Privacy, Volume: 14.

[9] Y. Sheffer, R. Holz, P. Saint-Andre, "Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)". rfc7525, May 2015

[10] C. Schmitt, B. Stiller, T. Kothmayr, TU Muenchen, W. Hu. "DTLS-based Security with two-way Authentication for IoT".lnternetDraft,July 4 2013. Web Link: https:lltools.ietf.orglhtmlldraft-schmitt-\ \two-way authentication-for-iot-OO

