한국컴퓨터정보학회 하계학술대회 논문집 제23권 제2호 (2015. 7)

SSL/TLS 기반의 IoT에서 cipher suite rollback 공격 탐지를 위한 선택된 알고리즘 검증 방법

정진희°, 조대호*
*°성균관대학교 전자전기컴퓨터공학과
e-mail : jinhee91@skku.edu°, thcho@skku.edu*

Selected Algorithm Authentication Method for Detection of Cipher Suite Rollback Attack in SSL/TLS of IoT

Jin-Hee Chung°, Tae-Ho Cho*
*°Dept. of Information and Communication Engineering, SungKyunKwan University

● Abstract ●

본 논문에서는 SSL/TLS에서 발생할 수 있는 cipher suite rollback 공격 탐지를 위해 선택된 알고리즘을 리스트로 검증하는 방법을 제안한다. 제안 기법은 SSL/TLS의 핸드셰이크 단계에서 이루어진다. 클라이언트 기기가 암호화 알고리즘의 순위를 리스트로 만들고 핸드셰이크가 끝난 후에 선택된 알고리즘의 순위를 비교해서 해당 기기에 대한 공격을 의심하도록 한다. 그러므로 우리의 제안 기법은 cipher suite rollback 공격 탐지를 향상시키고 안전한 메시지 통신을 한다.

키워드: IoT security, MQTT, SSL/TLS, Cipher suite rollback attack

I. Introduction

사물 인터넷(Internet of things; IoT)은 언제, 어디서나, 어떤 것이든 연결시켜주는 기술이다. IoT의 발전은 놀라운 속도로 가속화되고, 스마트 기기 의존도도 증가되고 있다. 그러나 IoT는 통신, OS, API, 접근 제어 등 여러 기술이 통합, 연동되므로 보안의 취약성이 발생될 가능성이 매우 커서 보안의 문제가 크게 부각된다[1]. IoT에서 메시지 큐 텔레메트리(Message Queue Telemetry Transport; MQTT)의 암호화 통신을 위해 적용되는 SSL/TLS는 스마트 기기 사이에서 사용된다. 이러한 암호화 통신을 위해 두 기기는 암호화 알고리즘을 선택하는데 이 과정에서 사이퍼 수트 롤백(Cipher suite rollback) 공격이 흔히 발생할 수 있다. 이 공격의 탐지를 향상시키기 위해, SSL/TLS 핸드셰이크 동안 클라이언트 쪽에서 암호화 알고리즘의 보안 강도로 순위 리스트를 만들어서 해당 공격을 의심하도록 하는 방법을 제안한다. 2장에서 용어 설명을 하고, 3장에서 공격을 탐지하는 기법을 제안한다. 마지막으로, 4장에서 결론을 맺는다.

II. Background

1. MQTT

MQTT는 IoT에서 TCP/IP 기반으로 동작하는 경량의 메시지 전달 프로토콜이다. 이 프로토콜을 사용할 때는 스마트 기기를 중개자(Broker), 발행자(Publisher), 구독자(Subscriber)로 구별한다. 중개자를 중심으로 기기들의 정보교환이 이뤄지는데 발행자가 중개자에게 토픽(topic)과 데이터를 전송하고 중개자가 해당 토픽을 구독한 구독자에게 데이터를 전송한다. 평문 전송이기 때문에 SSL/TLS를 사용해서 보안을 강화한다[2].

2. SSL/TLS

SSL/TLS은 전송계층과 응용계층의 암호화 통신을 위해 사용되는데 핸드셰이크의 암호화 알고리즘을 선택하는 과정에서 스마트 기기 간에 다음과 같은 취약점이 있다[3].

- Hello 메시지가 평문이다.
- 암호화 알고리즘을 선택하는 메시지 중에 암호화 방식 변경(Change cipher spec) 메시지가 여전히 변경될 가능성이 있다[4].

3. Cipher Suite Rollback Attack

사이퍼 수트 공격은 IoT에서 SSL/TLS의 취약성을 통해 흔히 일어나는 공격 중 하나이다. 공격자는 평문의 Hello 메시지를 가로채서 정상적인 암호화 알고리즘이 아닌 공격자에게 유리한 암호화 알고리즘으로 바꾼다. 결국 키를 알아 낸 공격자는 암호화된 데이터에 접근할 수 있다. 두 번째 방법으로, 공격자는 암호화 방식 변경 메시지를 가로채고 암호화 알고리즘을 바꿔서 키와 데이터에 접근할 수 있다. 이 공격은 SSL 2.0에서는 심각한 결점이 되는 공격이었지만, 3.0에서 모든 메시지를 MAC으로 인증하면서 보완되었다. 그러나 여전히 암호화 방식 변경 메시지는 MAC으로 인증되지 않는 취약점이 있다[4].

III. The Proposed Scheme

1. Assumption

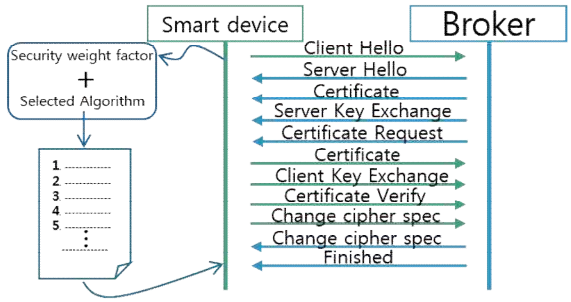
제안 기법에서는 아래와 같은 가정이 있다.

- 스마트 기기는 이전에 한 번 이상의 연결이 있다.
- 과거 선택했던 암호화 알고리즘을 저장한다.

2. Motivation

SSL/TLS의 취약성을 통해 사이퍼 수트 롤백 공격이 발생하는데, 본 논문에서 제안하는 기법은 해당 공격에 대해서 탐지를 향상시키고 기기 간의 안전한 메시지 통신을 돕는다.

3. The Proposed Scheme



Selected algorithm list authentication method

Fig 1은 본 논문에서 제안하는 사이퍼 수트 롤백 공격 탐지를 위한 선택된 알고리즘 리스트 검증 방법이다. Fig 1에서와 같이 스마트 디바이스는 데이터를 발행 또는 구독하는 기기이고 중개자는 스마트 기기 간의 메시지를 관리하는 역할을 한다. 핸드셰이크가 시작되면, 클라이언트는 지원하는 암호화 알고리즘에 우선순위를 매겨서 리스트로 만든다. 우선순위로는 알고리즘의 보안 강도와 이전 연결 시에 선택된 알고리즘이 높은 순위로 반영된다. 핸드셰이크가 끝나고 앞으로 사용 될 암호화 알고리즘이 결정 되면 클라이언트가 가진 리스트와 선택된 알고리즘을 비교하여 위치한 순위가 낮으면 해당 기기에 대한 사이퍼 수트 롤백 공격 여부를 의심한다.

IV. Conclusions

MQTT로 메시지를 전송하는 IoT기기는 암호화 메시지 전송을 위해서 SSL/TLS를 사용하는데, 이 암호화 프로토콜은 여전히 여러 공격으로부터 취약점이 존재한다. 본 논문에서는 사이퍼 수트 롤백 공격의 탐지를 높이고 안전한 데이터 전송을 돕기 위해 새로운 기법을 제안하였고, 향후 제안 기법을 증명하기 위한 실험을 할 것이다.

Acknowledgement

이 논문은 2013년도 정부 (교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임 (No. NRF-2013 R1A2A2A01013971).

References

[1] K. Zhao and L. Ge, "A survey on the internet of things security," in *Computational Intelligence and Security (CI S), 2013 9th International Conference on,* 2013, pp. 663-667.

[2] MQTT, *http://mqtt.org.*

[3] H. lei Zhang, "Three attacks in SSL protocol and their sol utions," .

[4] D. Wagner and B. Schneier, "Analysis of the SSL 3.0 pro tocol," in *The Second USENIX Workshop on Electronic C ommerce Proceedings,* 1996, pp. 29-40.