

추계학술 발표대회

2019.11.1(금)~2(토)

부경대학교 대연캠퍼스

주최 사단법인 한국인터넷정보학회

주관 부경대학교

후원 (주)카카오, (주)아이티센, LGCNS(주), (주)한스컴정보통신

www.ksii.or.kr



KOREAN SOCIETY FOR INTERNET INFORMATION

사단법인 한국인터넷정보학회

법인등록번호 101-86-33111



논문발표

11월 2일(토) 09:30~11:30(향파관 3층 309호)

세션 B. 인터넷보안

좌장 : 배인한 교수(대구가톨릭대)

- B-1 DLOTAv2 기반의 안전한 펌웨어 업데이트 방안
이민경, 최슬기, 광진(아주대)
- B-2 DCV 기반 공격기법 분석 및 대응방안
정해선, 광진(아주대)
- B-3 유전 알고리즘을 이용한 컴파일러 분류
황철훈, 신건윤, 한명목(가천대)
- ☆ B-4 은닉형 안티포렌식 APK 분류기법에 관한 연구
김대규, 김창수(부경대)
- B-5 악성코드 프로파일 기반 유사 악성코드 검색 연구
강홍구, 최보민, 김경한, 박순태(KISA)
- B-6 완전동형암호를 이용한 Metropolis Hastings 샘플링 알고리즘에 관한 연구
유준수, 윤지원(고려대)
- B-7 완전 동형암호를 이용한 베이지안 선형 회귀분석
홍미연, 윤지원(고려대)
- B-8 안드로이드 취약점 기반 변종 랜섬웨어 동향 분석
박소희, 광진(아주대)
- B-9 암호화된 데이터상에서 영상처리를 위한 Gaussian 필터 구현
송백경, 윤지원(고려대)

11월 2일(토) 09:30~11:30(향파관 3층 304호)

세션 C. 인터넷통신

좌장: 김석훈 교수(순천향대)

- ☆ C-1 실시간 얼굴인식을 위한 분산 시스템
장종권, 범정현, 추현승(성균관대)
- C-2 Wi-Fi 기반 그룹 관리 MAC 프로토콜 구현
한명승, 장윤경, 유인태(경희대)
- C-3 무선 센서 네트워크에서 시간 효율적인 지연 제한 데이터 집계를 위한 제한 기법
Vo Van Vi, Dung T. Nguyen(성균관대), 김문성(서울신학대), 추현승(성균관대)
- C-4 듀티 사이클 센서 네트워크에서 구조 기반 데이터 집산 알고리즘에 대한 성능 평가
Dung T. Nguyen(성균관대), 김문성(서울신학대), 추현승(성균관대)
- C-5 WIT-tree 기반의 가중치 빈발패턴 마이닝 기법의 분석
임현근, 윤은일, 남효주, 백윤지, 김종성, 김현호(세종대)
- C-6 STPA 기반 무인기 조작 규정 안전 검증 새로운 방법
Xiaorui Shao, 김창수(부경대), 라일군(Univ. of Colorado Denver)
- C-7 STPA 기반 무인기 시스템상의 컴포넌트 오류 및 불안정한 상호작용에 관한 연구
Palash Sontakke, 김창수(부경대), 라일군(Univ. of Colorado Denver)
- C-8 복수의 SFC 환경에서 모니터링 에이전트 배치 최소화를 통한 시그널링 비용 감소 방안
이도경, 김문성, 사이드무함마드라자, 추현승(성균관대)

DLOTA_v2 기반의 안전한 펌웨어 업데이트 방안

이민경*, 최슬기**, 박진***

*,***아주대학교 사이버보안학과

**아주대학교 컴퓨터공학과 정보보호응용및보증연구실

e-mail : *leemkl@ajou.ac.kr, **skchoi.isaa@gmail.com, ***security@ajou.ac.kr

Secure Firmware Update Method based on DLOTA_v2

Minkyung Lee*, Seul-Ki Choi**, Jin Kwak***

*,***Department of Cyber Security, Ajou University

**ISAA Lab., Department of Computer Engineering, Ajou University

요 약

시장조사기관 가트너에 따르면, 2020년에는 전자제품의 95%가 사물인터넷(IoT)기술이 탑재된다고 한다. 이렇듯 IoT 기기는 지속적으로 증가하고 있는 추세이다. 지속적으로 증가하는 IoT 기기들을 효율적으로 관리하고 편리성을 향상시키기 위해 원격으로 펌웨어를 업데이트하기 위한 OTA(Over the Air)방식이 사용되고 있다. 그러나, 이러한 OTA 방식에 대한 결함이 발생한다면 이전 버전의 취약한 펌웨어 혹은 악성 펌웨어를 업로드하는 등의 보안위협이 발생할 수 있다. 따라서, 상호인증, 기밀성, 무결성등을 보장하는 펌웨어 업데이트 방안에 관한 연구가 주목을 받고 있다.

본 논문에서는 현재 펌웨어 업데이트 방식인 OMA에서 제시한 OTA 기반 DLOTA_v2를 분석하고 DLOTA_v2 기반의 안전한 펌웨어 업데이트를 위해 상호인증, 기밀성과 무결성을 보장하는 검증 방안을 제시한다.

1. 서 론

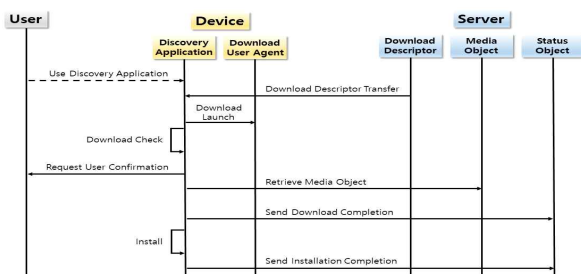
IoT 기기들은 다양해지고 있으며 지속적으로 증가하고 있다. 가트너에 따르면, 2020년에는 IoT기술이 전자제품의 95%에 탑재될 것으로 예측했다[1]. 하지만 수많은 IoT 기기들을 관리하기 위한 OTA 기반의 펌웨어 업데이트 방식에 취약점이 존재한다면, 이는 다양한 보안위협이 발생할 것으로 예상된다. 실제로 최근 원격으로 DSLR 카메라 펌웨어 업데이트 취약점을 이용한 랜섬웨어 공격 방법이 발표되기도 하였다[2].

따라서 본 논문에서는 펌웨어(Firmware) 업데이트 방안을 보완하고자 OMA에서 제시한 DLOTA_v2 기반의 안전한 펌웨어 업데이트 방안을 제안하고자 한다.

2. 관련 연구

2.1 DLOTA_v2

DLOTA_v2는 Download Over The Air의 약자로 다음 그림 1은 OMA(Open Mobile Alliance)에서 제시한 OTA 기반의 표준 데이터 다운로드 방식이다[3].

(그림 1) DLOTA_v2 과정

Step 1. 서버(Server)는 Download Descriptor를 디바이스(Device)에 전송

Step 2. 다운로드 시작

Step 3. 다운로드에 필요한 용량 확인

Step 4. 유저의 확인

Step 5. Media Object 검색 결과 상태보고서 전송

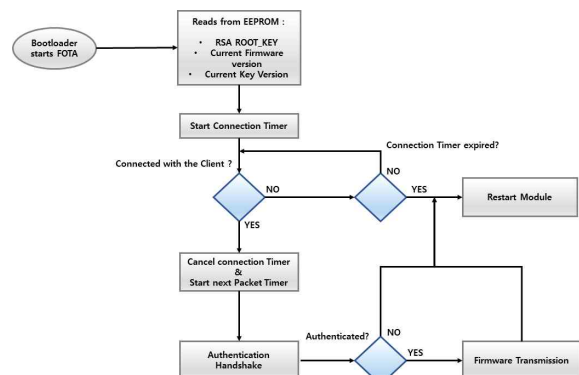
Step 6. 다운로드 완료 메시지 전송

Step 7. 설치

Step 8. 설치 완료 메시지 전송

2.2 Anton 등의 펌웨어 업데이트 방안

Anton Martinsen와 Alexander Nässlander은 안전한 펌웨어 무선 업데이트 방안을 제안하였다[4]. 이는 Bluetooth를 이용한 펌웨어 무선 업데이트 방안으로써, 128kB의 크기 제한 내에서 서버 인증 및 데이터 무결성 검증을 포함하였다. 다음 그림 2는 Anton 등이 제안한 Flow chart diagram이다.



(그림 2) A Flow chart diagram of FOTA

이 논문은 2019년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. NRF-2017R1E1A1A01075110).

Step 1. Bootloader에 의해 FOTA 시행

Step 2. EEPROM으로부터 필요한 정보 읽음

Step 3. 연결 타이머 시작

Step 4. Client와의 연결이 실패 시, 타이머에 따라 다시 연결을 시도 또는 모듈 재시작

Step 5. Client와의 연결이 성공 시, 연결 타이머를 취소 및 패킷 타이머 시작

Step 6. 인증 Handshake 시행

Step 7. 인증 실패 시, 모듈 재시작

Step 8. 인증 성공 시 펌웨어 유효화 확인

Step 9. 유효하지 않은 펌웨어일 경우 모듈 재시작

Step 10. 유효한 펌웨어일 경우 펌웨어 수신 준비 완료

□ Anton 등의 펌웨어 업데이트 방안 분석**• 효율성 분석**

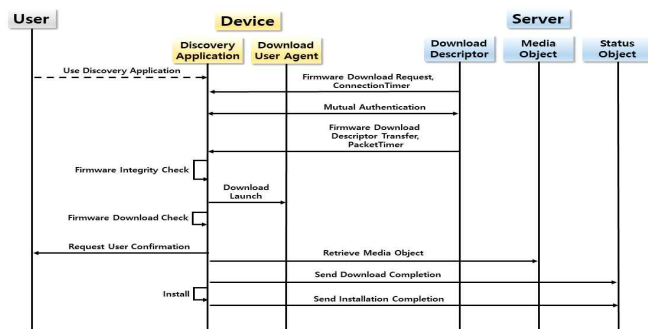
Anton Martinsen와 Alexander Nässlander이 제안한 펌웨어 업데이트 방안에서 서버의 인증은 RSA 알고리즘을 이용하여 인증하며, 펌웨어 암호화 및 데이터 암호화는 비대칭키인 세션키(Session Key)를 이용한 RSA 알고리즘을 적용한다. 이는, CPU의 과도한 연산을 필요로 한다.

• 안전성 분석

해당 펌웨어 업데이트 방안의 펌웨어 무결성 검증은 SHA-1 해시 알고리즘을 이용한 Message Digest에 RSA 알고리즘을 적용하여 무결성 검증을 시행한다[4]. 하지만 최근 SHA-1 해시 알고리즘에 충돌현상이 발생할 수 있음을 입증하는 연구가 발표되었다[5]. 이는 펌웨어 무결성 검증이 제대로 이루어지지 않을 경우, 악의적인 공격자에 의해 펌웨어에 대한 변조가 발생할 수 있음을 의미한다.

3. DLOTA v2 기반의 안전한 펌웨어 업데이트 방안

위에서 분석한 취약점에 대한 개선 방안은 다음 그림 3과 같다. 펌웨어를 다운로드 하기 전에 상호인증을 수행한 후 서버로부터 오는 Firmware Download Descriptor의 무결성 검증을 수행한다.



(그림 3) DLOTA v2 기반의 안전한 펌웨어 업데이트 과정

Step 1. 서버는 디바이스에 Firmware Download Request 전송 및 연결 타이머 동작

Step 2. 디바이스와의 연결 실패 시, 타이머에 따라 다시 연결 시도 또는 모듈 재시작

Step 3. 디바이스와의 연결 성공 시, 상호인증 수행

Step 4. 인증 실패 시, 모듈 재시작 및 종료

Step 5. 인증 성공 시, 패킷타이머 시작

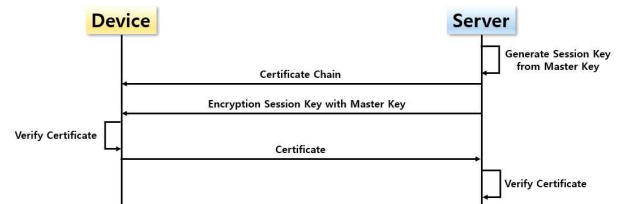
Step 6. Firmware Download Descriptor 전송

Step 7. 펌웨어 무결성 검증 수행

Step 8~14. DLOTA v2의 Step 2~8과 동일

3.1 효율성 및 안정성 분석**□ Symmetric Key Algorithm & Mutual Authentication**

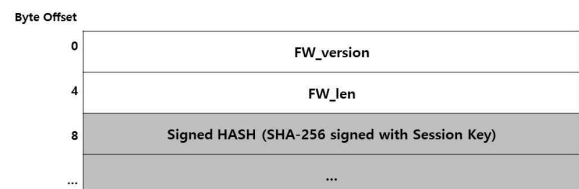
인증되지 않은 서버와의 펌웨어 업데이트 수행을 방지하기 위해 서버와 디바이스간의 상호인증 방안 제시한다. 서버는 공개키 암호 방식을 사용하여 마스터키(Master Key)를 생성한다. 그 후, 마스터키로부터 세션키를 생성한 후 디바이스와 안전하게 공유한다. 이때 세션키는 CPU의 과도한 연산을 줄이기 위해 대칭키 암호 알고리즘을 사용한다. 서버의 인증은 CA가 발급한 인증서로부터 디바이스는 서버의 인증을 수행하고, 디바이스는 디바이스의 인증서를 Server에 보내 인증을 수행한다.



(그림 4) Example of Mutual Authentication

□ Firmware Integrity Check

중간자 공격 등을 방지하기 위해 펌웨어 변경에 대한 Firmware Integrity Check를 필요로 한다. 따라서 Firmware Integrity Check 방안을 제시한다. 펌웨어 데이터를 SHA-256 등 안전한 해시 알고리즘을 이용하여 Message Digest를 생성한 후 세션키로 암호화를 수행한다. 그 후, 디바이스는 펌웨어가 변경되었는지 해당 Message Digest를 비교하여 검증을 수행한다. 다음 그림 5는 펌웨어 패킷 구조의 예시이다.



(그림 5) Example of Firmware Packet Structure

4. 결론

펌웨어 업데이트 과정에 취약점이 발생한다면, 다양한 보안 위협이 발생할 수 있다. 이에 따라, 안전한 펌웨어 업데이트 방안에 관한 연구가 필요하다.

따라서 본 논문에서는 안전한 펌웨어 업데이트를 위해 DLOTA v2기반의 안전한 펌웨어 업데이트 방안을 제시하였다.

참고 문헌

- [1] Gartner, "Gartner Top Strategic Predictions for 2018 and Beyond", Oct 2017.
- [2] ESTsecurity, "캐논 DSLR 카메라, 원격으로 랜섬웨어에 감염될 수 있어", 알약, Aug 2019.
- [3] Open Mobile Alliance, "Download Over the Air Specification Approved Version 2.0", Mar 2011.
- [4] Anton Martinsen, Alexander Nässlander, "Firmware update in a resource constrained environment", Lund university, 2015.
- [5] Google, "Announcing the first SHA1 collision", Google Security Blog, Feb 2017.