사물인터넷 장치 통합 제어용 게이트웨이 인증 알고리즘 개선 연구 - A제품을 기반으로

정소영* 박준용** 오인수** 김찬민** 임강빈***

*순천향대학교(대학생), **순천향대학교(대학원생), ***순천향대학교(교수)

Study on the Improvement of Authentication Algorithm of Gateway for Integrated Control of IoT Devices-Based on Product A

Jung So Young* JunYoung Park** Insu Oh** Chanmin Kim** Kangbin Yim***

*Soonchunhyang University(Undergraduate student)

**Soonchunhyang University(Graduate student)

**Soonchunhyang University(Professor)

요 약

사물인터넷 장치는 경량화 및 소형화의 조건을 충족하면서도 적은 전력 소모와 원활한 무선 통신 성능이 보장함으로써 사용자에게 쾌적한 서비스 환경을 제공한다. 하지만 이러한 조건들을 충족하기 위해 설계와 개발 단계에서의 보안 요구사항에 대한 인지 결여가 시스템 내외부적으로 심각한 보안 취약점으로 이어진다. 본 논문에서는 시중에 판매 중인 사물인터넷 제품 중 게이트웨이 제품군 중 A 대상을 선정하여 이에 대해 발생할 수 있는 취약점을 분석하며 특히 인증 과정에서 취약성을 보완하고 암호화 기법 등을 적용하여 보안성을 개선한 알고리즘을 제안한다.

I. 서론

사물인터넷은 사물이라 불리는 다양한 형태의 사물 장치들이 상호 연결되어 인터넷 네트워크상에서 데이터 수집과 교환, 공유와 같은 기능을 적절히 활용할 수 있는 서비스 환경을 제공하여 사용자에게 편의를 제공하는 기술이다. 통신 네트워크 기술 발전에 따른 무선 네트워크 인프라의 확장과 생산 기술 고도화에 따른 센서 생산에 필요한 비용 절감 등 다양한 요인이 상호작용한다. 이에 따라 사용자가 사물인터넷 기술을 이용함에 받는 제약이 줄었으며 다른 산업 기술과 융합되어 일상에서 사용하는 가전 소품부터 산업 분야까지 기술에 대한 접근성 및 확장성이 좋아졌다[1]. 하지만 사물인터넷의 활용 범위가 확장됨에 따라 사물 간의 통신에 취급되는 사용자 정보와 사용 환경 정보의 양 또한 축적되므로 이를 목표로 한 사이버 공격과 위협이 지속해서 발생하는 추세이다[2].

임베디드 운영체제 기반의 사물인터넷은 경량화와 소형화의 조건을 충족하면서 일반 가전 장치보다 전력 소모량이 적고 무선 통신 기술 성능의 보장을 요구한다. 때문에 장치와 보드의 설계 및 개발 단계에서 보안 지식 부족으로 인해 보안 요구사항이 충족하지 못하는 경우가 발생할 수 있다. 이로 인해 시스템 내외부적으로 공격자에게 무방비하게 노출될 수 있다[3].

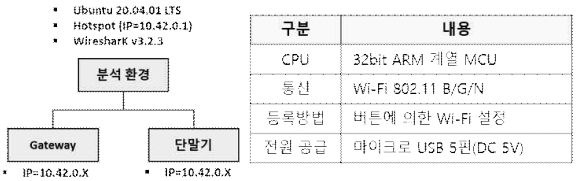
본 논문은 사물인터넷 장치 중 네트워크에 연결된 다수의 사물의 시스템 상태 정보 수집과 제어가 가능한 게이트웨이 제품군을 선정하여 분석한다. 사물인터넷 게이트웨이는 특히 사물 간의 모든 통신에 대한 네트워크 게이트웨이 역할을 수행하므로 이에 대한 공격 발생 시 정보 유출, 제어권 상실 등의 피해가 발생할 수 있다[4]. 따라서 본 논문에서는 사물인터넷 게이트웨이 A 제품을 선정하여 사용자의 인증 과정에 발생할 수 있는 취약점에 대해 분석하고 이에 대한 개선된 인증 알고리즘을 제안하고자 한다.

II. 사물인터넷 게이트웨이 인증 알고리즘 취약점 분석

2.1 분석 대상

사물인터넷 게이트웨이는 위한 사물과의 연결 수립 과정에서 무결성을 보장하는 인증 과정을 요구한다. 또한 연결 수립 이후 게이트웨이와 사물 간의 신뢰성 검증과 보장을 위한 암호화 과정 등이 게이트웨이의 보안 요구사항에 해당된다. 게이트웨이에서 보안 요구사항의 불충족으로 인한 취약점 노출은 사용자 정보와 사용 환경에 대한 정보 노출에서부터 사생활 침해, 제3자에 의한 제어권 상실 등의 피해가 발생한다. 실제 게이트웨이 장치 A를 선정하여 시중에 판매 중인 제

품에 대한 취약점 존재 여부에 대해 분석했다.

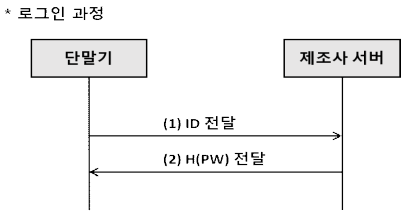


구분	내용
CPU	32bit ARM 계열 MCU
통신	Wi-Fi 802.11 B/G/N
등록방법	버튼에 의한 Wi-Fi 설정
전원 공급	마이크로 USB 5핀(DC 5V)

[그림 1] 분석 대상 정보 및 분석 환경

위 [그림 1]은 분석 대상의 성능과 분석 환경의 도식화이다. 게이트웨이 제어를 위해 제조사에서 제공하는 어플리케이션과 게이트웨이 장치 사이에 발생하는 네트워크 통신 패킷을 수집하여 발생 가능한 취약점을 분석했다.

2.2 로그인 과정 분석



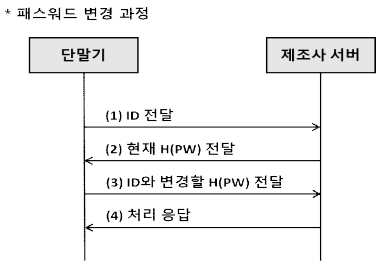
[그림 2] 알고리즘 - 로그인

게이트웨이 제어는 제조사의 모바일 어플리케이션으로 수행하며 위 [그림 2]과 같다. (1) 서버로 사용자의 ID를 전달하고 PW는 해시 연산을 위해 임시 저장한다. (2) ID의 해시 값인 H(PW)를 어플리케이션으로 전달한다. H(PW)는 어플리케이션 내부에서 PW 평문과 검증 알고리즘 연산을 통해 일치 여부를 판단한다.

[그림 3] 로그인 패킷

위 [그림 3]는 로그인 과정에서 수집한 (1)과 (2)의 패킷이다. 로그인 과정에서 서버의 통신 시 UDP 페이로드 내 사용자의 ID와 H(PW)가 평문으로 노출되는 취약한 구조임을 알 수 있다.

2.3 패스워드 변경 과정 분석



[그림 4] 알고리즘 - 패스워드 변경

위 [그림 4]는 어플리케이션 내 패스워드 변경 과정의 도식화이다. (1) 서버로 ID를 전달한다. (2) ID의 H(PW)를 전달한다. (3) 패스워드 검증 연산 후 변경할 PW를 해시 연산하여 ID와 전달한다. (4) 패스워드 변경 처리에 대해 응답한다.

[그림 5] 패스워드 변경 패킷 - 과정 (2)

[그림 6] 패스워드 변경 패킷 - 과정 (3)

위 [그림 5, 6]에서 패스워드 해시 값과 변경할 패스워드 해시 값 또한 노출됨을 확인했다. 해당 취약점에 대해 패스워드 임의 변조 실험을 수행했다. [그림 6]은 변경할 H(PW)를 전달하는 패킷이며 해당 H(PW)의 내용 변조 후 재전송하여 수행했다. 기존 패스워드 [12345678]의 해시 값을 [bbbbbbbb]의 해시 값으로 대체했다.

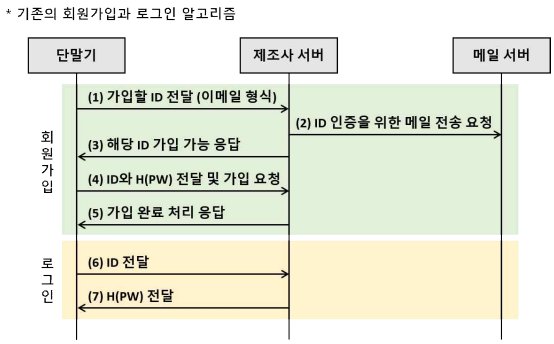
[그림 7] 패스워드 변조 실험

위 [그림 7]은 패스워드 [bbbbbbbb]로 로그인이 성립했으며 본 실험을 통해 사용자 인증 과정이 취약함을 보여준다.

III. 사물인터넷 게이트웨이 인증 알고리즘 개선 방안 제안

3.1 기존 인증 알고리즘의 문제점

게이트웨이 A는 어플리케이션을 통해 제어하며 해당 어플리케이션은 사용자의 인증을 과정에 사용되는 해시 연산에 대하여 Bcrypt 알고리즘을 사용한다[5].



[그림 8] 기존 인증 알고리즘

위 [그림 8]은 어플리케이션 상에서 회원가입과 로그인을 처리하는 알고리즘을 정리한 과정의 도식화이다. (4)(6)(7)의 과정에서 회원가입과 로그인 시 평문으로 사용자의 ID와 H(PW)이 노출되며 이를 이용한 패스워드 임의 변조의 가능성을 앞의 2장에서 확인했다. 따라서 패킷을 암호화하여 보안성이 개선된 인증 알고리즘을 제안한다.

3.2 보안성이 개선된 인증 알고리즘 제안

[표 2] 알고리즘 내 수식 정리

n	범위 내 가장 큰 두 정수의 곱
e	$\gcd(e,\phi(n))=1$가 1인인 공개키
d	$d \bullet e = 1 \bmod \phi(n)$인 개인키
K	대칭키 AES 알고리즘의 비밀키
$H(PW)$	Bcrypt 알고리즘으로 연산된 패스워드 해시 값
T	타임스탬프

[그림 9] 알고리즘 제안

위 [그림 9]는 보안성을 개선한 인증 알고리즘을 도식화한 그림이다. 인증 알고리즘의 기밀성과 사용자 인증을 보장을 위해 AES[6]과 RSA[7]으로 암호화하고 타임스탬프로 메시지 무결성을 보장한다.

(1) 사용자가 가입할 아이디를 서버로 전달한다. (2) 서버는 이메일 형식으로 전달받은 아이디의 중복 여부와 유효 메일 확인을 위해 메일 서버에 인증을 요청한다. (3) 아이디의 가입 가능 여부 응답과 공개키 RSA 연산의에 이용할 공개키 e와 두 소수의 곱 n을 전달한다.

$$C = (E(H(PW),K))^{e} \bmod n$$

[수식 1] 암호문 구조

(4) 사용자의 아이디와 패스워드를 입력받은 어플리케이션은 아이디와 위 [수식 1]에 해당하는 암호문 그리고 무결성 인증 목적의 타임스탬프를 서버로 전달한다. (5) 서버는 개인키 d로 암호문을 복호화하여 사용자의 패스워드 해시 값을 서버 내 데이터베이스에 저장하며 응답 처리와 함께 한 단계 증가한 타임스탬프를 전달한다. (6) 평문 노출의 문제가 있었던 로그인 과정에서도 역시 패스워드 해시 값을 위 [수식 1]과 같이 전달한다.

위와 같은 기밀성과 송수신자 인증, 메시지 무결성이 보장되는 알고리즘을 제안함으로써 사물인터넷과 어플리케이션 사이 통신 속도 측면에서의 성능 저하가 예상된다. 하지만 기존의 인증 알고리즘과 비교 시 암호화와 타임스탬프를 적용함으로써 메시지 변조와 재전송의 방지가 가능하여 사용자 안전성이 보장된다.

IV. 결론

본 논문은 사물인터넷 제품 중 게이트웨이 제품군 A를 선정하여 취약점을 분석했다. 로그인 과정과 패스워드를 변경하는 과정 각 과정에서 패스워드 해시 연산 알고리즘 파악이 가능했고 평문 문자열의 노출됨을 확인했다. 또한 패스워드 변경 과정에서 발생한 패킷의 변조 및 재전송 결과로 패스워드 변조 성립을 확인했다.

인증 구조상의 취약점으로 판단하여 인증 알고리즘을 분석하고 보안성이 추가된 알고리즘을 제안한다. 이 외에도 암호화되지 않은 통신에 대한 다양한 패킷 변조 및 재전송 공격이 가능함으로 보이며 앞으로 사물인터넷 장치를 보다 안전하게 이용하기 위한 보안 알고리즘 및 사물인터넷에 적합한 경량 암호화 기술에 대한 연구가 지속될 것으로 예상한다.

[참고문헌]

[1] 황원식, “산업 패러다임에 따른 미래 제조업의 발전전략 (2) 사물인터넷(IoT)이 가져올 미래의 산업변화 전망”, KIET 산업경제 2016년 3월, pp. 15-22, 2016.

[2] “IoT 취약점 5년새 54배 늘었다.” 아이뉴스24, http://www.inews24.com/view/1185014.

[3] “IoT 보안 취약 신고, 5년간 1400여건”. 이뉴스투데이, http://www.enewstoday.co.kr/news/articleView.html?idxno=1343147.

[4] 신승혁. “빅 데이터 처리를 위한 개방형 플랫폼 기반 IoT 센서 미들웨어의 설계.” 박사학위, 금오공과대학교 대학원, 2015.

[5] Bcrypt, https://www.npmjs.com/package/bcrypt

[6] Simon Heron, “Advanced Encryption Standard (AES)”, Network Security, Volume 2009, Issue 12, 2009, Pages 8-12, https://doi.org/10.1016/S1353-4858(10)70006-4.

[7] R. Rivest, A. Shamir, L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems ", Communications of the ACM, Vol. 21 (2), 1978, pages 120 - 126.