홈 네트워크 환경에서 경량화된 디바이스 인증 방법

조강희*, 황재연*, 전문석*
*숭실대학교 컴퓨터학과
e-mail : goodguy82@nate.com

Light weighted Authentication of Device in Home Network

Kang-Hee Cho*, Jae-Yeon Hwang*, Moon-seog Jun*
*Dept. of Computing, Soong-Sil University

요 약

홈 네트워크 환경에서 각 디바이스와 사용자의 인증은 중요한 보안 문제로 남아있다. 이러한 보안 문제를 해결하기 위해 ITU-T 에서는 공개키를 기반으로 한 인증 방법을 추진하고 있다. 본 논문에서는 최근 추진되고 있는 공개키 방법의 인증에 대한 비용과 처리율에 관한 문제점을 보안하기 위해서 Challenge-Response 기반으로 각 홈 디바이스와 홈 서버의 사전 공유키를 이용하여 인증코드를 통한 디바이스 인증의 경량화된 인증방법을 제시한다.

1. 서론

최근 보다 편리한 삶을 추구하기 위해 사람들은 주거 환경에서도 유비쿼터스를 적용하게 되고 그러면서 홈 네트워크 기술이 발전하고 댁내 망 유선뿐만 아니라 무선 부분에서도 급속한 발전을 이루고 있다. 그러나 인터넷 환경에서의 해킹 기술도 급격히 증가하고 있어서 홈 네트워크에서의 사용자 인증이나 홈 서비스 등이 위협을 받고 있는 실정이다. 이러한 보안 위협으로부터 안전한 홈 네트워크를 구축하기 위해 인가, 인증 기술의 발달은 필수적이다.[3][4]

현재 ITU-T SG17 Question9 회의 내용에서 디바이스 인증은 X.509 기반의 인증서를 사용[2][5]하고 복잡한 암호 알고리즘을 사용하기 때문에 디바이스의 높은 처리능력을 요구한다. 그리고 앞으로 진보될 홈 네트워크 환경에서 많은 디바이스들에게 인증서를 부여한다는 것은 자원을 낭비하는 것이다[6]. 이러한 문제점을 해결하기 위하여 경량화 되고 자원 낭비를 줄이는 해쉬 알고리즘을 이용한 인증방법[1]을 사용하여 보다 효율적인 인증방법을 제시한다.

2. 경량화된 인증방법의 요구사항

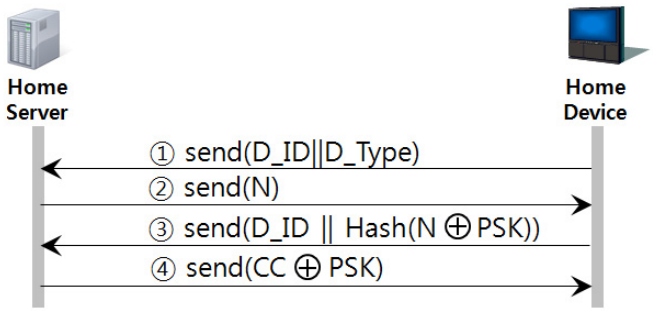
본 논문에서는 Challenge-Response 기반[1]을 통하여 복잡한 암호화 알고리즘을 사용하지 않고 해쉬 알고리즘을 이용하여 인증코드를 생성하여 효율적인 디바이스 등록, 인증, 제어 절차를 제안한다.

이와 같은 과정을 수행하기 위해서는 다음과 같은 두 가지 전제조건을 필요로 한다.

- 홈 서버에는 오프라인으로 미리 각 홈 디바이스 ID(디바이스 시리얼 번호)와 사전 공유키가 저장되어 있다.
- 각 디바이스 마다 사용자가 물리적으로 사전 공유키를 입력할 수 있다.

2.1 디바이스 등록

홈 네트워크 내에서 디바이스 등록은 인가코드를 발부하는 데에 목적이 있다. 사전에 물리적으로 서버에 등록이 되어있지만 통신하는데 있어서 해당 디바이스에 인가코드를 발부함으로써 제어부분에서 좀더 안전하게 통신할 수 있는 장점이 있다. 인가코드의 활용방안은 인증, 제어 절차에서 디바이스 키의 노출을 최대한 줄이기 위한 방법으로 본 논문에서 제안하는 시스템에서 중요한 역할을 한다.



D_ID	: 디바이스 ID	PSK	:사전 공유 키
D_Type	: 디바이스 Type	N	:비표 값
CC	: 인가코드		

(그림 1) 디바이스 등록

(그림 1)은 홈 디바이스가 홈 서버에 등록하여 인가코드를 발부 받는 과정이고 세부내용은 다음과 같다.

[1 단계] 디바이스가 홈 서버에게 등록하기 위해 자신의 ID 와 장비의 Type 을 연접하여 홈 서버에게

전송한다.

[2 단계] 디바이스로부터 받은 ID 와 Type 을 미리 작성된 디바이스 리스트에서 확인하여 새로운 등록이 필요한 디바이스일 경우 디바이스 사전 공유키 PSK 와 동일한 비트수의 비표 값 N 을 생성하여 디바이스에 전송한다. 이때 비표 값은 임시로 저장한다.

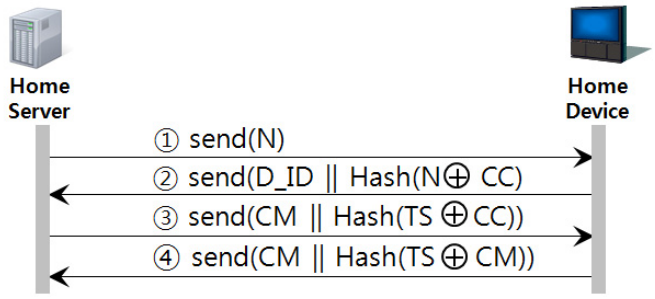
[3 단계] 홈 서버로부터 수신한 비표 값과 디바이스가 사용자에게 디바이스 사전 공유키를 입력 받아 XOR 연산하여 해쉬함수를 적용한다. 이 과정은 디바이스 사전 공유키의 노출을 막기위해 수행된다. 디바이스 ID 와 키-해쉬함수를 이용해서 변경된 값을 연접하여 생성된 값 D_ID||Hash(N ⊕ PSK)를 홈 서버에 전송한다. 디바이스에게 수신된 값을 디바이스 리스트에서 검색 후 임시 저장한 비표 값과 해당 디바이스의 사전 공유키를 XOR 연산하여 해쉬함수를 적용한 값을 수신된 값과 비교하여 디바이스에 대한 인증을 수행한다.

[4 단계] 등록을 완료하면 해당 디바이스의 아이디와 디바이스 사전 공유키를 XOR 연산하여 해쉬함수를 적용한 값 Hash(D_ID ⊕ PSK)를 디바이스의 인가코드로 저장한다. 인가코드를 디바이스에게 안전한 전달을 위해 디바이스 사전 공유키와 XOR 한 값 CC ⊕ PSK 을 디바이스에 전송한다. 디바이스는 수신된 값을 디바이스 비밀키로 XOR 연산하여 인가코드를 추출하고, 디바이스에 저장한다.

3 단계 과정에서 사전 공유키 확인을 통하여 홈서버는 디바이스에 대한 인증을 수행하여 디바이스를 등록하고, 4 단계 과정에서 디바이스 인증 및 제어에 사용될 인가코드를 발부함으로써 사전 공유 키 사용을 최소화 한다.

2.2 디바이스 인증, 제어

디바이스 제어를 위해 먼저 해당 디바이스가 정상적인 디바이스인지 인증해야 한다. 또한 디바이스도 정상적인 서버임을 인증해야 하는 상호 인증 과정이 필요하다. 인증과정이 완료된 후에는 타임 스탬프를 이용하여 제어 메시지를 전송하여 악의적인 공격자의 중간자 공격(Man-in-the middle Attack)을 예방한다.



D_ID	: 디바이스 ID	CM	: 제어 메시지
TS	: 타임 스탬프	N	: 비표 값
CC	: 인가코드		

(그림 2) 디바이스 인증, 제어

(그림 2)는 홈 서버가 홈 디바이스를 제어하기 위한 인증, 제어 과정이고 세부내용은 다음과 같다.

[1 단계] 홈 서버는 디바이스를 인증하기 위해 인가코드와 동일한 비트수의 비표 값을 생성하여 디바이스에 전송한다. 이때 비표 값은 임시로 저장한다.

[2 단계] 디바이스는 등록과정에서 받은 인가코드를 사용하여 수신된 비표 값과 XOR 연산하여 해쉬함수를 적용한 값 Hash(CC ⊕ N)을 홈 서버에게 자신의 ID 와 연접하여 전송한다. 홈 서버는 수신된 디바이스 ID 를 리스트에서 확인 후 등록과정에서 생성했던 해당 디바이스의 인가코드와 임시로 저장했던 비표 값을 XOR 연산한 값을 해쉬함수 적용 후 수신된 값과 비교하여 디바이스에 대한 인증을 수행한다.

[3 단계] 홈 서버는 디바이스를 제어하기 위한 메시지를 평문으로도 보내고 인가코드와 타임스탬프를 XOR 연산하여 키-해쉬함수를 이용해서 변경된 값으로 연접하여 전송한다. 디바이스가 메시지를 수신하면 평문 제어메시지를 취하고, 여기에 키-해쉬함수를 적용한다. 그 다음에 자신이 수신한 값과 계산된 값을 비교하여 정상적인 서버의 메시지임을 확인한다.

[4 단계] 메시지의 무결성을 확인하기 위해 디바이스는 메시지를 타임스탬프와 XOR 연산하고 키-해쉬함수를 이용해서 변경된 값을 평문 메시지와 함께 서버에 전송한다. 홈 서버는 디바이스에게 수신된 값과 계산된 값을 비교한 후 디바이스가 올바르게 작동되었는지 확인한다.

2-3 단계 과정에서 각각 인가코드를 사용하여 상호 인증을 수행하고, 3-4 단계 과정을 통해 미리 동기화된 타임스탬프를 사용하여 재생 공격(Replay Attack)에 대한 저항성을 지닐 수 있다.

3. 결론

본 논문에서 제안하는 방법은 홈 네트워크의 서버와 기기들을 댁내 망이라는 이점을 최대한 활용하여 Challenge-Response 기반으로 가벼운 처리율과 속도로 사용자들에게 편리함을 제공한다.

참고문헌

[1]Behrouz A. Forouzan, “암호학과 네트워크 보안” McGraw-Hill

[2]ITU-T, http://www.itu.int/ITU-T

[3]김도우, 한종욱, 정교일, “홈 디바이스 인증/인가 기술동향” 정보통신연구진흥원, 주간기술동향 제 1329 호 2008, pp.1-11

[4]김정태, 박혜경, 백의현, “홈 네트워크 서버(HS/HG) 기술 동향” ETRI, 20 권 제 6 호

[5]이덕규, 김도우, 한종욱, “홈 네트워크 보안 기술 및 표준화 동향” ETRI, 23 권 제 4 호, pp.89

[6]정은희, 이병관, “홈 네트워크 환경에서 OTA 키를 이용한 DA_UDC 모듈 설계”, 한국통신학회논문지 ’09-04 Vol. 34 No.4