홈 망의 인증 및 접근 제어에 대한 보안 분석+

*이광재 **김범한 ***이동훈

고려대학교 정보경영공학전문대학원

*mosd00@korea.ac.kr

A Security Analysis of Authentication and Access Control on Home Network

*Gwang-Jae Lee **Bum-Han Kim ***Dong-Hoon Lee

Graduate School of Information Management and Security, Korea University

요약

일상생활에서 사용되는 홈기기들을 원격조정 할 수 있는 것은 매우 흥미롭다. 하지만 우리 생활과 밀접한 기기이므로 더욱 더 안전성을 중요시해야 한다. 이 분야에 대한 연구가 활발히 되면서 점차 무선 통신을 이용하여 가정 내의 각종 기기들을 제어 및 모니터링 하고자 한다. 이는 생활의 편리성을 제공하는 반면에, 이기종망간의 연동 및 무선의 특성으로 인해 보안의 취약성이 노출되기 쉽고, 홈 망의 복잡성으로 인해 다양한 요구사항들이 필요하게 된다. 본 논문에서는 가정 내 다양한 기기들의 원격 제어 및 모니터링을 안전하게 서비스할 수 있는 메커니즘을 분석한다.

1. 서론

홈 망에서 가정 내의 다양한 기기들은 서로 유·무선으로 연결되어 하나의 망을 구성하는데, 이를 위해 다양한 유무선 통신 기술이 요구된다[1-3]. 무선으로 인한 가정 내의 이동성은 기기들 간 일일이 케이블로 연결하는 번거로움을 해소하여 생활의 편리성을 제공하고 가정 내의 공간을 최대한 효율적으로 활용할 수 있는 가능성을 증대시켜 준다. 특히, 이동 단말을 이용하여 HG를 통해 원격지에서도 가정 내의 각종 기기를 제어 및 모니터링 함으로써 보다 다양한 서비스를 제공받을 수 있고 생활의 편리성이 높아진다. 이러한 편리성 이면에는 이기종망간 연동 및 무선의 특성으로 인해 보안의 취약성이 노출되기 쉽고, 홈 망의 복잡성으로 인해 다양한 요구사항들이 필요하게 된다. 보안의 취약성이라 함은 공격자가 유무선 상의 메시지를 인터셉트하여 (eavesdrop) 정보를 변형 또는 유출하거나 합법적인 사용자로 가장해서 (masquerade) 홈 망에 침입하여 가정 내의 기기들을 불법적으로 제어하는 것을 의미한다.

기존 연구들에서는 개인 컴퓨터에서 웹을 이용하여 홈 게이트웨이를 인터넷을 통해 원격 제어하는 연구와 가정 내의 홈 게이트웨이와 기기들 간의 안전한 프로토콜과 서비스에 대한 연구가 진행되었다.

본 논문에서는 2장에서 유무선 통신 기술 요구 사항의 정의 하였고, 3장에서는 기존 프로토콜들을 보안 분석하였다. 그리고 4장에서는 결론을 내린다.

2. 프로토콜 분석

가. Krishnamurthy 프로토콜

보안 서비스와 기기들을 각각 6단계와 6 종류로 나누어 각 기기에 해당하는 적합한 인증 알고리즘을 적용하여 암호화된 통신을 제안하였고, 인증 정책에 따라 메시지 전송 가능 여부를 결정하였다. 예를 들면, 보안 서비스 단계가 낮은 장치들은 높은 장치들에게 메시지를 전송할 수 없으며, 단 특정 일정 시간 동안에만 통신이 가능하도록 하였다. 각 기기는 다른 기기와 통신하고자 할 경우 반드시 Access Point(AP)를 통하여 메시지를 송수신하기 때문에 AP에서 과부하 발생 시(i.e., 몇 개의 기기들이 동시에 미디어 정보를 전송하고자 할 경우) 병목 현상이 발생한다. 따라서 AP에 대한 Denial of Service (DoS) 공격을 극복할 수 없다.

나. Hwang 프로토콜

다중 멀티 홈 도메인 상에서 기기 등록 및 인증 처리 절차를 제안하였다. 이 연구에서는 두 계층의 PKI(Public Key Infrastructure) 모델을 제시하였고 홈 게이트웨이 간 인증은 하나의 루트 CA(Certificate Authority)를 통한 기존의 PKI 모델을 사용하였고, 홈 도메인 내부의 인증은 홈 게이트웨이가 루트 CA 역할을 대신하는 지역적인 PKI 모델을 사용하였다.

Notion

+"본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음" (IITA-2008-(C1090-0801-0025))

$Gcert_X$ A X.509 certificate that the global CA issues to X.

$Ccert_{XY}$ A cross domain certificate that domain X issues to domain Y

$Lcert_{XY}$ A local device certificate that a home gateway X issues to Y

N_X A nonce that X creates to prevent a replay attack.

K_{XY} A symmetric key shared between X and Y

K_X A public key of X

M A device

D Manufacturer Server

H A home gateway

C A client device

S A service device

H_X a home gateway to which X belongs

표1. 디바이스 등록 프로토콜

1. $C \rightarrow S \quad N_c, Lcert_{H_cC}$

2. $S \rightarrow H_S \quad Lcert_{H_cC}, N_S$

3. $H_S \rightarrow S \quad Ccert_{H_cH_S}, (K_{H_C}, N_S)K_{H_S^{-1}}$

4. $S \rightarrow C \quad N_S^{'}, Lcert_{H_cS}, Ccert_{H_cH_S}$

5. $C \rightarrow S \quad (N_C, K_{CS})K_S, (S, C, N_S^{'}, N_C, K_{CS})K_{C^{-1}}$

1.클라이언트 디바이스는 N_c를 생성해서 지역 디바이스 인증서와 함께 서버 디바이스에게 보낸다.

2. 서비스 디바이스는 $Lcert_{H_cC}$ 에서 클라이언트 디아비스의 도메인 이름을 확인한다. 만약 도메인 이름이 일치 하지 않으면, 서비스 디바이스는 $Lcert_{H_cC}$와 N_S를 그것의 홈 게이트웨이 H_S에게 보낸다.

3. H_S는 자신과 H_C사이를 체크한다. 만약 두 도메인이 맞지 않으면 H_S는 크로스 도메인 인증서와 H_C의 공개키를 서비스 디바이스에게 보낸다.

4. 서비스 디바이스는 K_{H_C}를 이용하여 $Lcert_{H_cC}$를 검증한다. 만약 인증서가 유효하지 않으면 클라이언트 디바이스에게 크로스 도메인 인증서와 자신의 지역 디바이스 인증서를 보낸다.

5. 클라이언트 디바이스는 그것의 루트 공개키를 이용하여 크로스 도메인 인증서를 검증하고 $Ccert_{H_cH_S}$에서 H_C의 공개키를 이용하여 서비스 디바이스의 지역 디바이스 인증서를 검증한다. 만약 인증서가 유효하면 클라이언트 디바이스는 세션 키를 생성하고, 그것을 이용하여 서비스 디바이스의 공개키를 암호화 한 후, 그것의 서명 메시지와 함께 보낸다.

6. 서비스 디바이스는 클라이언트의 지역 디바이스 인증서와 서명, 그리고 이 때 받은 세션 키를 검증한다.

다. 새로운 플랫폼을 제시한 프로토콜

Nakakita 프로토콜

서버 기반의 안전한 무선 홈 망을 제안하였으며, 기기들은 통신하기 위해 필요한 공유키를 분배를 위해 마스터키를 저장한다. 이 공유키는 주기적으로 변경되며, 기기들 간 통신은 이 공유키로 메시지를 암호화하여 직접 송수신한다.

서버는 공유된 네트워크 키 $K_{0,}K_1, K_2, \cdots$를 배포한다. 그리고, 클라이언트들에게 각각 $M_{SA}, M_{SA}, M_{SA}, \cdots$ 를 배포한다.

이 때, 서버는 동시에 새로운 키를 보낼 수가 없다. 그리고 주어진 키를 다 소모하면 대규모 업데이트를 해야 한다.

Saito 프로토콜

홈 게이트웨이에 자바를 이용한 웹 서버를 기반으로 하는 홈 게이트웨이를 이용하여 인터넷을 통한 외부 원격 제어를 위한 웹 기반 API를 제공하였다. 홈 게이트웨이는 인터넷망과 홈 망을 상호 연결하는 기능을 제공한다.

Bae 프로토콜

홈 망과 인터넷 망을 연결해 주어 홈 디지털 서비스를 제공해 주는 새로운 홈 서버 플랫폼을 제안하였다. 서비스 제공자는 무선 네트워크에서 받은 메시지를 홈 서버와 공개된 인터넷 TCP/IP 통신을 통하여 메시지를 전달한다. 이 플랫폼은 OSGi(Open Service Gateway initiative) 프레임워크 기반으로 유무선 홈 망 기기들 간 인터페이스를 제공하여 디지털 TV 서비스, 원격 멀티미디어 서비스, 인스턴트 메시지 서비스 등과 같은 다양한 서비스를 제공한다.

3. 결론 및 향후 연구 방향

지금 까지 연구 되어진 부분은 모두 인터넷을 통한 외부 원격으로 홈 기기들을 제어하거나 홈 디지털 서비스들을 제공한다. 그렇기 때문에 인터넷이 가지고 있는 특성상 보안의 취약성에 노출되기 쉽다. 따라서 가정 내 다양한 기기들의 원격 제어 및 모니터링을 안전하게 서비스할 수 있는 새로운 메커니즘이 필요하다. 사용자가 홈 망을 원거리에서 쉽고 편리하게 제어할 수 있으며, 기존의 이동망의 인증 처리 절차가 이기종망간 전통적인 PKI(Public Key Infrastructure)인증 방식을 처리 절차를 제공하고, 정교한 접근 제어 규칙을 사용하여 안전성과 효율성을 최대한 보장해야 한다.

5. 참고문헌

[1] Prashant Krishnamurthy, Joseph Kabara, and Tanapat Anusas-amornkul, "Security in wireless residential networks," IEEE Transactions on Comsumer Electronics, Volume 48,Issue 1, pp. 157-166, February 2002.

[2] H. Nakakita, K. Yamaguchi, M. Hashimoto, T. Saito, and M. Sakurai, "A study on secure wireless networks consisting of home appliances," IEEE Transactions on Comsumer Electronics,

Volume 49,Issue 2, pp. 375 - 381 May 2003.
[3]Jin-Bum Hwang, Do-Woo Kim, Yun-Kyung Lee, and Jong-Wook Han, "Two Layered PKI Model for Device Authentication in Multi-Domain Home Networks," In Proc. 10th IEEE Int'l. Symposium on Consumer Electronics, Russia, June 2006.
[4] Takeshi Saito, Ichiro Tomoda, Yochiaki Takabatake, Junko Ami and Keiichi Teramoto, "Home gateway architecture and its implementation," IEEE Transactions on Comsumer Electronics, Volume 46,Issue 4, pp. 1161-1166, November 2000.
[5] Changseok Bae, Jinho Yoo, Kyuchang Kang, Yoonsik Choe, and Jeunwoo Lee, "Home server for home digital service environments," IEEE Transactions on Comsumer Electronics, Volume 49,4,pp. 1129-1135, November 2003.
[6] 3GPP2 X.S0006, "MAP Support of Authentication and Key Agreement (AKA)," v1.0, October 2005.
[7] Snyder, Randall A., "Wireless Telecommunications Networking with ANSI-41," McGraw-Hill, 2/E, January 2001.
[8] C.-C. Lee, M.-S. Hwang, and W.-P Yang, "Extension of authentication protocol for GSM," In Proc. IEE Communications, Volume 150,Issue 2,pp. 91-95, April 2003.
[9] 3GPP TS 33.102, "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects;3G Security; Security architecture(Release 6)," V6.3.0, Dec 2004.
[10] 3GPP2 X.S0013, "All-IP Core Network Multimedia Domain," July, 2005.