홈 디바이스 기밀정보 은폐시스템 설계

김도우*·한종욱*

*한국전자통신연구원

Design of Hiding Secret Information System on Home Network Devices

Do-woo Kim*· Jong-wook Han*

*Electronics and Telecommunications Research Institute

E-mail : dwkim@etri.re.kr

요 약

홈 네트워크에서 요구되는 보안 서비스는 홈의 정의에 따라 달라질 수 있다. 그리고 댁내에 어떠한 홈 네트워크 기술들이 포함될 것인가에 따라 달라진다. 홈 네트워크에서는 다양한 디바이스들이 네트워크에 연결되어 있다. 이러한 홈 디바이스들은 외부의 공격으로부터 안전하지 않은 환경에 존재하게 된다. 따라서 홈 디바이스 내에 저장되어 있는 비밀정보를 보호하기 위한 요소들이 필요하다. 본 논문에서는 안전한 홈 네트워크 서비스를 제공하기 위해 필요한 홈 디바이스 내의 비밀정보를 보호하기 위한 시스템을 설계하고자 한다.

ABSTRACT

Security services required by a home network depend on the definition of a home. That depends on which of home network technologies is included. Various devices in home network environments connected with access network. These home devices can be attacked. So essential parts is needed to protect secret information stored in home network devices. In this paper we design the system that protects secret information in home network devices to offer secure home network services.

키워드

Home Network, Secret Information, Security

Ⅰ. 서 론

현재 홈 네트워크 기술은 홈네트워킹 기술과 미들웨어 기술 등 다양한 기술들이 활발히 연구 및 제안되고 있으며, 표준화 작업도 진행되고 있다.

홈 네트워크 기술이 보급되기 위해서는 최우선적으로 해결해야 할 기술 중의 하나가 보안기술이다. 홈 네트워크 보안기술은 악의적인 목적을 가진 공격자가 네트워크를 통하여 댁내에 침입하여 디바이스나 개인 프라이버시를 침해하는 것을 방지할 수 있다. 홈 네트워크 보안기술의 하나로

사용자가 홈 네트워크에 접속할 때에 사용자를 인증하고 인가하는 사용자 인증/인가 기술이 있다. 이는 홈 네트워크 서비스를 이용하고자 하는 사용자는 반드시 ID/PW 방식 또는 인증서 방식 등을 사용하여 인증/인가 과정을 수행한 후에, 그 결과에 의해 댁내·외에 존재하는 다양한 홈 네트워크 서비스를 이용하도록 한다[2-3].

홈 네트워크에서 인증 또는 인가를 위해서는 인증을 위한 증명데이터 또는 인가를 위한 ACL이 필수이며 이러한 데이터가 디바이스에 암호화 되어있지 않은 상태로 방치되어 있을 경우 공격자에 의해 쉽게 노출되어 다른 보안문제들을 야기 시킬 수 있다.

댁내의 네트워크가 외부 액세스 망과 연결되어 있지 않다고 가정하면, 안전한 홈 네트워크 환경을 제공하는 것은 쉽다. 그러나 댁내의 망이 인터넷과 같은 외부의 액세스 망과 연결되어 있다면, 안전한 네트워크 서비스를 제공하기 위해 필요한 인증 또는 인가를 위한 비밀정보의 보호는 아주 중요한 의미를 가진다. 따라서 홈 디바이스 내에 저장되어 있는 비밀정보를 보호하기 위한 요소들이 필요하다. 본 논문에서는 안전한 홈 네트워크 서비스를 제공하기 위해 필요한 홈 디바이스 내의 비밀정보를 보호하기 위한 시스템을 설계하고자 한다.

II. 관련연구

2.1 소프트웨어 보호기술

소프트웨어 불법복제, 임의적으로 소프트웨어를 수정하는 것과 같은 문제들을 해결하기 위한 기술들과 디지털 컨텐츠의 저작권 관련 당사자들의 이익과 권리를 보호해 주는 DRM(Digital Rights Management)은 소프트웨어나 서비스를 허용된 사용자만 접근할 수 있게 하는 기술이라는 점에서 비밀정보 은폐기술과 유사하다.

- 코드 혼잡화(code obfuscation)

코드 혼잡화(code obfuscation)는 코드 변형(code transformation)을 통해 기능적으로는 똑같지만 프로그램의 내부 구조를 다르게 하여 역 엔지니어링과 같은 분석을 가능한 복잡하게 하여 배포된 프로그램으로부터 소스 코드를 얻어내기 힘들게 하는 소프트웨어 보호기술이다. 코드 변형을 하면 프로그램의 구조, 실행 순서 등은 변화가 생기지만 실제 실행결과에는 영향을 주지 않는다. 공격자가 혼잡화 된 코드로부터 소스 코드를 얻어내기 위한 비용은 코드 변형의 수준, 공격자에게 주어진 시간, 자원과 변형된 코드를 원상복귀 시키기 위한 공격자의 역혼잡기의 성능에 따라 결정된다. 오브젝트 코드로부터 소스 코드를 분석하기 위한 공격자의 악의적인 역 엔지니어링 시도를 원천적으로 봉쇄할 수 없다면 코드 혼잡화를 오브젝트 코드에 적용하여 공격자의 역 엔지니어링을 최대한 어렵게 할 수 있다.

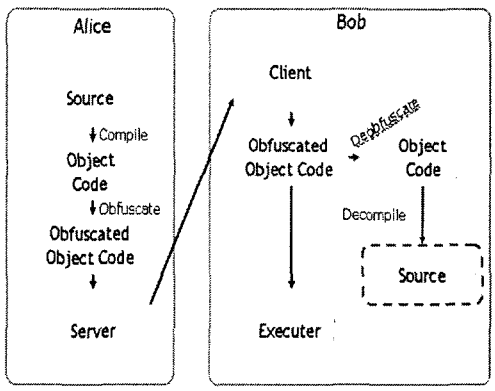

그림 1. 코드 혼잡화를 통한 소프트웨어 보호

그림 1에서처럼 프로그램 배포자인 Alice는 프로그램이 완성되면 컴파일 된 오브젝트 코드를 서버에 업로드 하기 전 혼잡화 과정을 통하여 사용자에게 혼잡화 된 오브젝트 코드를 다운받아가도록 한다. 다운로드 된 파일은 그대로 실행이 가능하지만 악의를 가진 Bob이 혼잡화 된 오브젝트 코드에 대해 역컴파일을 시도하여도 소스 코드를 알아낼 수 없으며 역혼잡화 작업을 따로 거쳐야 역컴파일 할 수 있는 오브젝트 코드를 얻을 수 있다.

- White-Box 암호학

전형적인 소프트웨어 환경에서 사용되는 암호 알고리즘은 공격자가 소프트웨어를 제어할 수 있는 환경에 있거나 악성 소프트웨어 또는 악성 코드가 공존할 경우 소프트웨어와 소프트웨어에 저장된 비밀정보는 안전하지 않다. *White-Box* 암

호학은 *encrypted−composed−function*을 이용하여 공격자가 모든 권한을 가질 수 있는 *White−Box* 환경에서의 공격에 대해 부분적인 보안을 제공한다. 이를 위해 키에 의존적인 테이블의 룩업(*lookup*)으로 구성된 *AES*를 보인다. *AES*의 여러 암호화 단계를 사용하는 대신 랜덤한 *bijection*을 통한 테이블의 조합으로 키를 숨기고 그것을 프로그램에 포함시켜 암호학적 범위(*Cryptographic Boundary*)를 확장한다[1].

III. 기밀정보 은폐 시스템

3.1 홈 디바이스 기밀정보 은폐 시스템 설계

홈 네트워크에서는 소프트웨어 보호 기법들의 가정과는 달리 디바이스들이 네트워크에 연결되어있다. 홈 디바이스 기밀정보 은폐 시스템은 홈게이트웨이나 홈서버가 홈 디바이스들에게 디바이스들이 안전한 환경에 있다는 것을 인지시켜주는 메시지를 주기적으로 전송하는 것으로 디바이스가 수신된 메시지의 값을 비교하여 자신이 안전하지 않은 환경에 있다고 판단되면 저장된 비밀정보를 곧바로 삭제한다. 공격자가 디바이스의 비밀정보를 얻어내기 위해서는 메시지가 주기적으로 뿌려지는 시간 안에 공격에 성공해야 하며 이로 인해 많은 공격을 봉쇄할 수 있다.

기본적으로 이 시스템은 홈 디바이스가 네트워킹 기능이 있다고 가정한다. 그리고 홈 네트워크에는 네트워크를 책임지는 홈게이트웨이나 홈서버가 존재한다고 가정한다. 홈게이트웨이나 홈서버는 보안성이 매우 높을 뿐만이 아니라 물리적인 공격으로부터 안전하다. 또한 홈 디바이스는 자신의 비밀 정보 이외에 홈게이트웨이나 홈서버의 공개키 PK_c를 가지고 있으며, RSA를 기반으로 홈게이트웨이나 홈서버의 메시지를 검증할 수 있는 능력이 존재한다. 비밀 정보는 휘발성 메모리 부분에 저장한다.

공격자는 홈 디바이스를 공격을 성공하기 위해서 일정한 시간 τ를 소요한다고 가정한다. 이 시간 동안에 공격당하는 홈 디바이스는 모든 기능을 정지당하여 전원이 나가거나, 켜져 있는 상태에서 공격자에 의해 홈 네트워크에서 이탈된다. 홈게이트웨이나 홈서버는 자신이 관리하는 홈 디바이스가 홈 네트워크 안에서 공격자에 의해 물리적으로 공격당하는 사실을 인지할 수 있다고 가정한다.

홈 디바이스 기밀정보 은폐 시스템은 홈게이트웨이나 홈서버에 내장될 기밀정보 은폐 서버 모듈과 각 홈 디바이스에 내장될 기밀정보 은폐 클라이언트 모듈로 구성된다. 서버 모듈은 난수 생성, 난수 서명, 멤버 관리를 위한 기능을 수행하고, 클라이언트 모듈은 서명 검증, 침입에 대한 대응, 도메인을 이동하거나 홈게이트웨이나 홈서버로부터 메시지를 받을 수 없는 경우에 대한 도메인 이동 관리 기능을 수행한다.

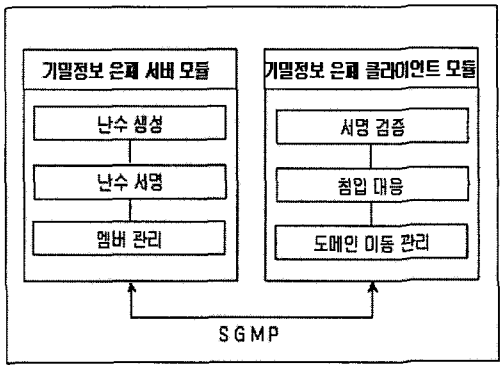

그림 2. 시스템의 구성도

홈게이트웨이나 홈서버는 다음과 같은 순서로 홈 디바이스의 안전성을 확인할 수 있다.

step 1. 홈게이트웨이나 홈서버는 이전에 전송했던 난수 R_1을 서명한 값 $R_1^{SK_c}$과 새롭게 뽑은 난수 R_2을 함께 모든 디바이스에게 보낸다. 최초의 R_1값의 교환은 안전한 상황에서 교환되었다고 가정한다. 이때, R_2는 범위 안에서 유니폼하게 선택해야 하며 되도록 과거에 사용하였던 수를 재사용해서는 안 된다.

step 2. 이를 수신한 모든 디바이스는 $R_1 = R_1^{SK_c PK_c}$로 복원하여 자신의 가지고 있던 Q_R의 값이 R_1과 같은지 확인하고 같다면 아직 자신이 안전함을 인지하고 Q_R에는 새롭게 R_2을 대입한다.

step 3. 만약 다르다면 R_1과 Q_R의 값이 서로 다르다면 홈 디바이스는 이를 무시한다.

step 4. 만약 일정한 시간 안에 유효한 SGM이 도착하지 않으면 디바이스는 자신의 휘발성 메모리 영역에 저장되어 있는 비밀 정보를 삭제한다.

IV. 결론

홈 네트워크 환경의 발전과 더불어 홈 네트워크에서 정보보호의 중요성이 증대되고 있다. 홈 네트워크에서 안전한 홈서비스를 제공하기 위해 필요한 인증 정보 및 ACL 정보가 디바이스에 암호화 되어있지 않은 상태로 방치되어 있을 경우 공격자에 의해 쉽게 노출되어 다른 보안문제들을 야기 시킬 수 있다. 본 논문에서는 안전한 홈 네트워크 서비스를 제공하기 위해 필요한 홈 디바이스 내의 비밀정보를 보호하기 위한 시스템을 설계하였다.

참고문헌

[1] S. Chow, P. Eisen, H. Johnson, P.C. van Oorschot: "White-Box Cryptography and an AES Implementation", LNCS 2595, pp 250 - 270

[2] Carl M. Ellison, *Home Network Security*, Intel Technology Journal, 2002.

[3] Guoyou He, *Requirements for Security in Home Environments*, Residential and Virtual Home Environments Seminar on Internetworking, Spring 2002.

[4] David F. Ferraiolo, R.S. Sandhu, Serban Gavrila, D.Richard Kuhn and Ramaswamy Chandramouli, *Proposed NIST Standard for Role-Based Access Control*", ACM Transactions on Information and Systems Security (TISSEC), Volume 4, Number 3, August 2001.

[5] S. Sandhu, E.J. Coyne, H.L. Feinstein, C.E. Youman, *Role based access control model*", IEEE Computer, 29 February 1996.

[6] David Ferraiolo and Richard Kuhn. *Role-based access control*", In 15th NIST-NCSC National Computer Security Conference, pages 554-563, Baltimore, MD, October 13-16 1992.

[7] Kim Thomas, *Building a Secure Home Network*, SANS Institute, 2001

[8] Blakey,G,R, Safeguarding cryptographic keys. Proc. AFIPS 1979 NCC, Vol.48, Arlington, Va., June 1979, pp. 313-317