홈네트워크 인증을 위한 생체 정보가 저장된 스마트 카드 활용 방안

이준희*, 황은영*, 권성구*, 김주한*, 박세현*, 송오영*

*중앙대학교 전자전기공학부

An Architecture of smart card with bio-metric information for authentication in home network

Junehee Lee*, Eunyoung Hwang*, Sunggu Kwon*, Joohan Kim*, Se Hyun Park*, Oh Young Song*

*School of Electrical & Electronics Engineering, Chung Ang University.

요 약

유비쿼터스 시대의 도래와 유비쿼터스 환경이 가장 먼저 구축되고 있는 홈네트워크 환경에 대한 관심이 높아 지고 있다. 이종 네트워크와 디바이스들이 서로 연동을 이루어 사용자에게 서비스를 제공하고 있는 이러한 홈네트워크 환경 구축에 있어서 그 중요성에도 불구하고 보안적인 요소가 배제되어 있는 경우가 많다. 이에 따라 본 논문에서는 홈네트워크 환경에서 요구되는 보안사항을 분석하고 사용자 인증을 위해 생체 정보가 담긴 스마트 카드를 이용해 인증서 기반 EAP-TLS를 사용하는 구조를 제안한다.

I. 서론

유비쿼터스 홈네트워크 환경은 가정 내에 존재하는 정보기기 뿐 아니라 PDA, 휴대폰, 노트북과 같은 이동 단말들과 홈서버 또는 홈게이트웨이가 연동을 통해 사용자에게 서비스를 제공하는 환경이다.

이러한 홈네트워크는 유, 무선 네트워크가 공존하고 있으며 기존의 네트워크 인프라를 바탕으로 구축되는 홈네트워크 환경은 기존의 외부 보안 위협들을 그대로 반영하고 있다. 특히 홈네트워크는 개인적인 공간이라는 점에서 다양하고 많은 종류의 중요한 개인 정보를 내포하고 있는 환경이다. 따라서 보안 공격을 받아 개인정보의 유출시 개인 정보의 손실 뿐 아니라 중요한 정보 또는 경제활동에 필요 한 정보가 파괴 또는 손실, 유출에 따른 손실이 더욱 심각한 문제를 야기 할 수 있다.

하지만 아직까지 보안 요구 사항이 반영이 되고 있지 않아 많은 부분이 보안 공격에 노출되어 있는 실정이다. 현재로써 많이 사용되고 있는 패스워드 또는 PIN(personal Identification Number)만을 이용한 사용자 인증 방법으로는 개인의 중요 정보를 안전하게 보관할 수 없는 실정이다.

이러한 문제를 해결하기 위해 최근 들어 개인의 고유한 생체 정보인 신체적 또는 행동학적 특징에 따라 사람들의 신원을 확인하는 바이오 메트릭(biometric) 즉, 생체정보 인식 기술이 대두되고 있다.

생체정보는 개인의 고유 정보인 지문, 홍채, 음성, 얼굴 모양, 손의 형태, 서명, 손등의 정맥 분포 등 아주 다양하다. 이것은 신체의 일부이거나, 개개인의 행동 특성을 반영하여 잊어버리거나 타인에게 대여 또는 도난당하지 않기 때문에 정보보안을 위한 새로운 분야로 활성화되고 있다.

본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT 연구센터(중앙대학교 홈네트워크 연구센터) 지원 사업의 연구결과로 수행되었음

따라서 본 논문에서는 홈네트워크 환경으로 접근하는 사용자의 신원 확인을 위해 생체 정보를 활용하는 방안을 알아본다.

II. 본론

본 연구에서는 홈네트워크 환경에서의 보안 요구사항을 알아보고 홈네트워크 환경에서 개인 정보 보호 및 보안을 위해 생체 정보를 활용한 보안 시스템의 구현 방안을 제시한다.

2.1 홈네트워크 보안 환경 분석

홈네트워크에는 홈서버, 홈게이트웨이 등 많은 수의 기기들이 존배하는데 그중에서 현재 상용화되고 있는 것이 홈게이트웨이 분야이다. 현재 홈게이트웨이는 2001년 12월에 정보통신 표준협회를 통해 표준을 재정했다. 하지만 최근에 이더넷(Ethernet), PLC, IEEE1394 등의 많은 프로토콜과 서비스등이 탑재되고 있어 향상된 성능 및 사용자 인증과 접근제어와 같은 보안 기술도 요구되고 있다. 외부 네트워크망과 댁내 네트워크망의 연결점인 홈게이트웨이에서는 네트워크 패킷 수집을 통해 댁내의 금융정보 및 사용자 ID등이 유출 될 수 있다. 아래 그림은 접근망을 통하여 홈게이트웨이로 접속되는 사용자 정보를 수집하여 위협이 될 수 있는 부분을 나타낸다.

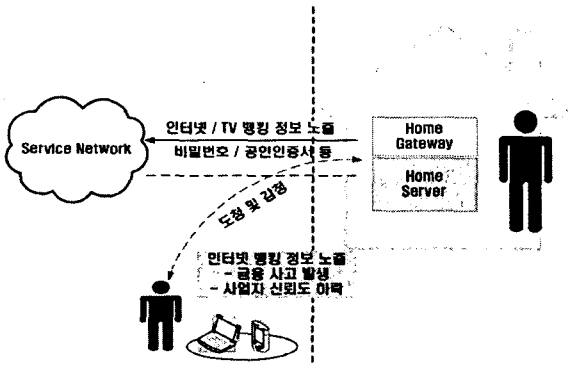

그림 1 도청에 따른 위험

이렇듯 도청을 통해 유출된 사용자 정보를 이용한 보안 위협 요소들을 분류하면 다음과 같다.

홈게이트웨이 취약성	● 현재 대부분의 관리 프로그램들이 웹기반이어서 웹서버 및 하위의 CGI 취약점을 이용한 관리자 권한 획득 가능성 존재 ● 홈게이트웨이의 침해는 곧바로 홈네트워크 전반에 걸쳐 위협으로 발전
	● 사용자가 홈게이트웨이를 관리하는 관리프로그램 설치 ● 관리프로그램 상의 취약점을 이용하여 네트워크 패킷을 수집 ● 사용자의 정보를 몰래 취득하여 홈기기로의 접속 시도 ● 사용자 프라이버시 및 중요정보 취득
유선 프로토콜 취약성	● Ethernet(802.3), PLC, IEEE1394 등 인터넷을 위한 접속망과 유선의 댁내망은 현재 인터넷에서의 취약점(해킹, 바이러스/웜 등)을 그대로 내포 ● 타 프로토콜로의 확산을 막기 위해서는 신속한 보안 댕응이 필요 ● 불법적인 접근자의 제거 가능성이 존재하며 물리적 장애 및 오작동, 홈 내부의 통신 장애를 일으킬 가능성 존재
	● 악의적인 의도를 가진 공격자가 서비스 제공 서버로 QoS 공격 시도 ● 홈 내부 사용자의 서비스 제공 서버로의 접속 불가 ● 사용자의 정보를 습득하여 원래의 서비스 제공 서버로 위장 ● 사용자의 개인 접속 정도 등을 몰래 취득
무선 프로토콜 취약성	● 무선랜, HomeRF, Bluetooth, UWB, ZigBee 등 ● 근본적으로 도청과 감청이 가능하므로 송신자와 수신자 간 보안설정이 중요 ● 댁내 기기에 대한 제어 신호는 암호화를 통한 신호 전송이 필요 ● 주기적인 무선 접속요청을 통한

	DoS 공격에 의해 홈 내부통신 장애 발생 가능
	● 악의적인 의도를 가진 공격자가 홈 내부의 AP에 계속적인 접속 요청 ● 홈 내부 무선 통신 제어 신호 장애 및 교란 발생

표 1 구성 요소별 보안 취약점

2.2 생체 정보 인식 기술

생체정보 인식 기술은 개인정보를 이용해 신분을 확인하는 기술로서, 인간의 고유한 신체적 특징이나 성분 등을 자료로 사용하기 때문에 국가나 기업차원은 물론, 개인에게도 생체측정 기술 개발의 연구가치 이면에 정보보호 필요성이 상존하게 된다. 특히 ATM, 휴대폰, 스마트카드, 데스크톱 PC, 워크스테이션 및 정보통신망의 불법 사용이나 불법 접속을 방지하기 위해 지문, 홍채, 망막 스캐닝, 음성, 얼굴 및 손모양, 혈관, 땀구멍 분석, DNA패턴, 귀, 얼굴체온, 냄새 탐지 등 다양한 형태의 생체측정 시스템을 실시간 인식에 사용하고 있다. 지금까지 이러한 생체인식 시스템들은 주로 물리적 출입통제의 수단으로 사용해 왔으나, 최근컴퓨터 시스템 및 네트워크 보안의중요한 수단으로 등장해 전자상거래를 운영하는 사이버 몰이나 금융기관 등 인증 시스템을 구축하면서 생체인식 보안 시스템을 적극 활용 하고 있다.

생체인식보안 시스템은기존의 방식인 이용자 ID와 패스워드입력 및 PKI (공개키 기반의 전자서명 인증서 보증방식) 등에서 발전해, 생체인식기술을 이용한 통합보안 시스템을 구성하기에 이르렀다. 이는 기존의 방식에다 지문인증, 홍채인증, 정맥인증, 얼굴인증, 음성인증, 서명 인증 등을 결합하고, 거기에 스마트카드와 USB Key 등 하드웨어 보안 시스템까지 통합한 형태로 발전하고 있다.

2.3 스마트카드와 EAP-TLS

스마트카드는 외부에 정보를 노출시키지 않고 안전하게 정보를 처리할 수 있는 장소다. 스마트카드는 전자적이나 기계적 또는 화학적 간섭을 막아주고 카드에 저장된 데이터를 암호화하며 PIN에 의한 이중 인증 등을 통해 정보의 안전성을 확보해 준다. 신용카드, 현금차감 카드, 고객우대 카드 등 각종 카드가 널리 사용되고 있어 스마트카드도 매우 눈에 익은 형태의 카드가 돼 사용자들이 쉽게 수용할 수 있다.

EAP-TLS는 초안으로 IETF에 제안된, 공용키 인증서에 기반한 엄격한 인증 방법이다. EAP-TLS를 사용하는 경우, 클라이언트는 사용자 인증서를 전화 접속 서버에 제공하며 서버는 서버 인증서를 클라이언트에 제공한다. 사용자 인증서는 서버에 확실한 사용자 인증을 제공하며 서버 인증서는 사용자가 원하는 서버에 연결된 것을 확인할 수 있게 한다. 인증서의 검증은 신뢰할 만한 인증기관의 도움을 받는다.

사용자 인증서는 전화 접속 클라이언트 컴퓨터에 저장되거나 외부 스마트카드에 저장될 수 있다. 두 경우 모두, 사용자와 클라이언트 컴퓨터 사이에서 사용자 확인 절차(PIN 번호 또는 이름, 암호 교환)를 거치지 않고는 인증서에 액세스할 수 없다.

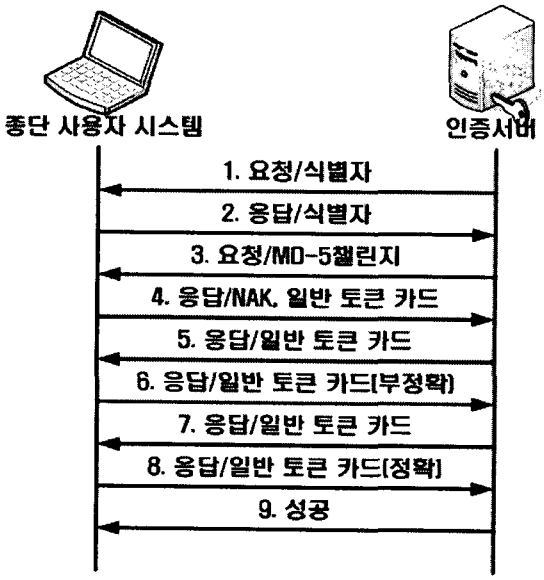

그림 2 EAP 인증 프로시저

2.4 생체 정보 인식 기술을 이용한 인증

방안

기술한 보안 위협 요소들을 보면 홈게이트웨이를 통한 사용자인증은 그 중요성을 알 수 있으며 홈네트워크 보안의 시작점이라고 할 수 있다. 따라서 본 논문에서는 스마트카드에 인증서 뿐 아니라 생체 정보를 함께 저장하고 인증 단말에 생체 정보 인식시킴으로써 사용자 인증을 하는 방안을 제시한다.

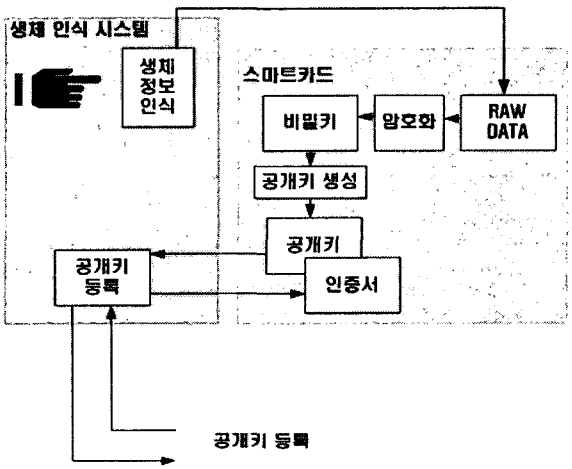

그림 3 생체 정보를 이용한 인증서 등록

사용자는 우선 자신의 생체 정보를 스마트카드에 저장을 한다. 그리고 저장된 생체 정보를 갖고 비밀키를 생성한다. 그리고 이렇게 만들어진 비밀키와 기존의 전통적인 방식으로 생성된 비밀키를 갖고 공개키를 생성한다. 이렇게 생성된 공개키를 사용해서 인증기관으로부터 인증서를 받아 그 인증서를 스마트카드에 저장하는 과정을 거쳐 자신의 생체 정보를 인증에 사용할 준비를 한다.

사용자가 홈네트워크에 접근하기 위해 인증을 원하는 경우 사용자는 생체 정보 인식 센서에 자신의 생체 정보를 입력함과 동시에 스마트카드를 사용해야 한다. 여기서 사용자는 자신의 생체 정보를 기존의 PIN 대신에 사용한다고 할 수 있다. 사용자가 생체 정보를 입력하면 스마트카드에 저장되어 있는 생체 정보와 동일한지를 확인하고 동일함이 확인이 된 후에야 스마트카드에 저장되어 있는 인증서를 사용하여 인증을 할 수 있게 된다.

이러한 방식은 스마트카드 자체적으로도 높은 보안성을 제공하고 있는데다 EAP또한 그 구조와 프로세스의 안정성을 인정받고 있기 때문에 홈네트워크 시스템으로의 인증과정에서도 높은 보안성을 제공한다고 할 수 있다.

III. 결론

본 논문에서는 유비쿼터스 홈네트워크 환경에서 발생 가능한 보안 공격에 대해서 알아보고 사용자의 개인 정보 보호를 위해 사용자 인증 방법으로 생체 정보를 활용하는 방안을 제시 하였다. 제안된 방식은 구현이 용이하면서도 기존의 패스워드, 아이디 방식에 비해 더욱 강력한 보안을 제공할 수 있을 것으로 예상된다. 하지만 PKI가 높은 보안성을 제공하기는 하지만 그 크기가 너무 크기 때문에 시스템에 무리를 줄 수 있다. 또한 생체 정보는 사용자의 의도와 상관없이 한번 유출이 되어 복제가 되면 교체 할 수 없다. 이러한 점으로 미루어 볼 때 홈네트워크 환경에서 사용 할 수 있도록 SPKI와 같이 경량화 된 PKI 모델이 필요하며, 생체 정보 위, 변조 방지 기술을 도입할 필요가 있을 것으로 예상된다.

[참고문헌]

[1] 강명희, 유황빈 "유비쿼터스 컴퓨팅 환경을 위한 익명성을 보장하는 사용자 인증 및 접근제어 모델", 전자공학회 논문지 제 42권 CI 제 4호

[2] 유동영, 김영태, 노병규 "유비쿼터스 홈네트워크 환경에서의 침해 위협 및 대응 방안", 한국정보과학회 논문집 vol.31, No2.

[3] Paul Reid, "Biometric for Network Security", prentice Hall PTR

[4] Smart Card Alliance, "Smart Cards And Biometrics In Privacy-Sensitive Secure Personal Identification Systems", A Smart Card Alliance White Paper