안전한 Home Network 서비스를 위한 RMCS 설계 및 구현

선재훈* · 이동휘* · 김귀남*

요 약

최근 들어 Home 네트워크에 대한 관심이 높아지고 있다. 이러한 관심과 더불어 Home 네트워크 산업도 날로 발전하고 있다. Home 네트워크에 관한 관심과 보급이 날로 증가하고 있으며 Home 네트워크 환경에서 외부접근망(Access Network)과 댁내망(Home Network)의 중간에서 Home 네트워크 서비스를 원활하게 중계하고 댁내망안에서 홈기기(PC, 홈패드, DTV 등)들 사이의 중계 역할을 하는 Home 게이트웨이에 대한 중요성 역시 날로 높아지고 있다. 하지만, 아직까지 Home 게이트웨이에 대한 관련 기술의 표준화가 미비한 실정이며, 여러 가지 기술을 적용하여 Home 게이트웨이의 성능을 향상 시키고 표준을 마련하는 작업이 진행중에 있다. 현재 Home 네트워크 관리체계를 보면 대부분이 ID/PASSWORD 접근 방식을 그대로 사용하고 있는 추세이다. 이미 우리는 기존 네트워크 환경에서 '1.25 대란'과 같은 충분한 댓가를 치루며 보안에 대한 교훈을 얻었다. 본 논문에서는 Home 네트워크 환경의 보다 안전하고 효율적인 관리를 위한 방법으로 역할 기반의 다중인증 시스템 RMCS를 구현하여 시스템이 내·외부 모두로부터 안전한 보호를 제안하였다. 기존 ID/PASSWORD 방식을 전자서명을 이용하여 외부망으로부터의 접근에 대한 보안을 강화하였으며, 역할 기반의 MIB 구조를 이용하여 Home 네트워크 내부에서도 보다 안전한 권한 제어를 통한 Home 네트워크의 보안을 제안하였다.

RMCS Plan and the Embodiment for the Home Network Service which is Safeent

Jae Hoon Sun* · Dong Hwi Lee* · Kuinam J Kim*

ABSTRACT

As home network is increasing to use, home network industry is developing too. Also, it is to be a popular subject in the network's topics. In this reasons, home network become a important thing because home gateway function is working between access network and home network. In the home network, it relates on the personal computer, home pad, and digital television. But, home gateway is not prepared standard point about techniques. Therefore, many kind of technique want to try for developing of home gateway's functions. Usually, we use ID/PASSWORD method in network control system. But, we found a lot of problems about classical network system while we experienced Jan/25 big trouble. We are considering about that home network system are using same network net. Therefore, seriously we have to check about security and safety at the home network's environment. This report focus on the home network's environment to control for using and efficiency and then it wants to find ways to protect from the internal and external attacks. Existing ID/PASSWORD method it used a electronic signature and the security against the approach from of external watch, the MIB structure of role base and the security of the Home network which leads the authority control which is safe even from the Home network inside it strengthened it used compared to it proposed.

Key words : Home Network, RBAC, SNMP, Certificate, Security

* 경기대학교 정보보호학과

1. 서 론

최근에 각종 유무선 통신 기술이 급속히 성장하고 있다.

그에 따라 정보기기, 디지털 가전기기, Home 오토메이션 기기들을 하나의 네트워크 망으로 구성하여 시간이나 공간의 제약 없이 홈 기기들을 제어하고 관리하며 보다 안전한 Home Network 환경을 구축하기 위한 연구가 활발하게 진행되고 있다.

그 중에서도 외부망과 댁내망을 연결하고 있는 Home 게이트웨이의 안전성 확보에 대한 관심이 커지고 있다.

본 논문에서는 이러한 Home Network의 안전한 제어를 보장하여 안전한 Home 네트워크 환경을 만들기 위한 방법으로 Home 게이트웨이를 중심으로 한 역할 기반의 다중인증기법을 제안하였다.

댁내 환경에서 여러 가지 유·무선 Home 네트워크 기술들 중 하나 이상의 댁내망(LAN)기술에 액세스망(WAN) 기술을 상호 접속 및 중재하는 Home 게이트웨이를 매우 중요하게 보고 Home 게이트웨이의 안전성 확보를 위하여 Home 게이트웨이의 안전한 관리를 위한 제안을 하였다.

첫 번째, 기존의 ID/PASSWORD 인증 방식만으로는 보안의 취약성이 그대로 노출되므로 ID/PASSWORD 인증 방식에 전자서명을 이용한 초기 인증부분의 강화를 제안하였다.

두 번째로 역할 기반의 MIB 구조를 이용한 사용자 권한별 관리 제어로 Home 네트워크 망에서의 보안을 강화 할 수 있다.

이러한 ID/PASSWORD와 전자서명을 이용한 다중인증 방식과 역할 기반의 MIB구조를 이용한 역할기반의 다중인증 시스템 RMCS 를 제안하여 보안을 강화하고자 하였다.

2. 관련 연구

2.1 인증방식

Home 네트워크 환경에서 인증시스템을 위한 보안요소로써 현재 인증을 위해 사용하는 기법은 ID/PW(PASSWORD) 방식과 전자 서명 그리고 인증서를 이용한 방법이 있다.

2.1.1 ID/PW 방식

각각의 사용자가 지정한 ID와 PW를 이용하는 것으로 한사람의 ID, PW로도 다수가 이용가능하다는 것과 해킹에 많은 문제점이 발생

2.1.2 전자서명(Digital Signature)

공개키(Puublic Key)방식을 사용하여 사용자 인증과 메시지 불변성을 보장해 주는 기술로 전송하고자 하는 상대의 Public Key를 사용하여 암호화한 경우에 원하는 상대만이 자신의 Private Key를 사용하여 해독할 수 있으므로 메시지 내용의 기밀성이 유지시에 사용[1].

2.1.3 인증서(Digital Certificate)

주민등록증이 나의 신분을 보증해 주듯이 인증서는 전자서명에 사용되는 공개키를 공인인증기관이 인증해주는 문서[2].

현재의 Home 네트워크 환경에서는 인증을 위한 방법으로 ID/PW 방식을 그대로 사용하여 접근하는 방식을 대부분이 채택하고 있어 보안상 취약점이 그대로 노출되고 있는 이러한 보안상의 문제점을 보완하고자 초기 접속시에 전자서명을 이용하여 보안을 강화하고자 한다.

2.2 SNMPv3와 RBAC

2.2.1 SNMP

현재 관리자와 망관리 요소간의 프로토콜로

SNMP(Simple Network Management Protocol)는 보안이 강화된 SNMPv3가 개발되어 쓰이기 시작했으나, 몇가지 문제점들로 인하여 사용상 어려움이 나타나고 있는데 그 문제점들을 보면 아래와 같다[3].

- 관리대상시스템 MIB에 통신망 관리자 보안정보의 중복 저장
- 통신망 보안관리정보의 중앙집중방식의 관리기능 부족
- 통신망 관리자간, 관리자 그룹간 계층구조 미지원으로 인한 효과적 권한부여 관리의 어려움

2.2.2 RBAC

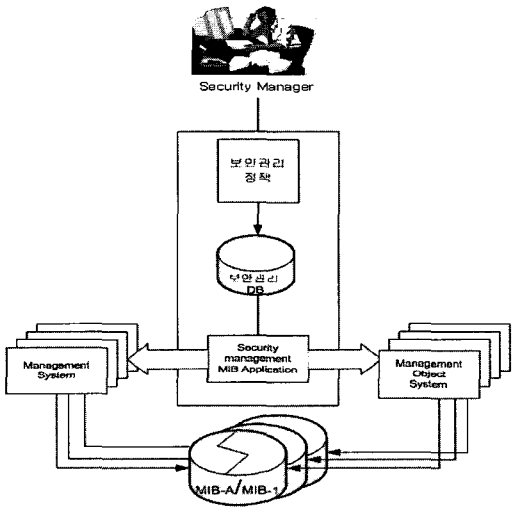
이와 같은 보안관리 문제점은 상업환경의 보안모델로서 최근 그 사용이 확대되고 있는 역할 기반 접근통제(RBAC : Role-Based Access Control) 모델이 제공하는 보안기능에 의해 해결 될 수 있다[4].

① RBAC 모델의 특징

- 권한을 부여하는 단위가 사용자가 아닌 사용자가 수행하는 역할[5, 6]
- 사용자 접근권한은 해당 접근권한이 배정된 역할의 구성원이 되어야 가능
- 권한부여 및 관리 단위가 역할이므로 다수의 사용자의 시스템의 효율적 관리 가능
- 역할간 계층구조로 하위 역할에 배정된 권한이 상위 역할에 의해 사용될 수 있는 권한 상속(Permission inheritance) 특징을 제공
- 보안 관리자가 관리기능을 통해 모델 구성요소의 구성정보를 변경함으로써 다양한 보안특성 모델링이 가능, 구성요소 관리를 통한 보안특성의 통제가 가능

② 역할기반 보안관리 모델

역할기반 보안관리 모델은 다수의 통신망 관리자들의 관리연산 수행에 의해 관리정보의 일관성과 일치성이 침해될 수 있는 SNMPv3 보안서비스를 보완하는 기능을 수행한다. 또한, 다수의 통신망 관리자에 의해 통신망이 운용, 관리되는 환경에서 통신망 전반에 적용되는 일관된 보안정책의 수립과 실행을 가능하게 하는 기능을 제공한다[7, 8].



(그림 1) 역할 기반 보안 모델 구성요소

2.2.3 동작절차

① 보안관리자는 SNMPv3에 의해 관리되는 통신망의 관리시스템, 관리대상시스템, 통신망 관리자, 통신망 관리자에 부여된 관리권한을 분석한 후 통신망 관리자 역할과 역할간 계층구조, 역할에 부여될 관리권한, 역할이 수행될 시스템을 결정하여 보안관리정책을 기술
(통신망 관리자 역할에 부여되는 관리권한을 통신망 구성요소의 중요도, 통신망 구성요소의 기능적 특징 및 관리부서 등에 의해 배정함으로써 통신망 관리권한의 통제와 관리부하를 경감)

② 기술된 보안관리정책은 변환기에 의해 보안관리 MIB 테이블로 변환

③ 변환된 보안관리 MIB 테이블들은 보안관리 MIB 전송 프로그램에 의해 관리시스템과 관리대상시스템으로 전송(보안관리 MIB 테이블의 생성과 전송은 통신망 관리시스템의 초기화나 보안관리정책의 변경때 수행)

이와 같이 역할기반 보안관리모델은 보안관리자가 통신망 전반에 대한 효과적인 보안관리정책의 기술하고 보안관리정책을 반영한 보안관리 MIB 테이블을 관리시스템과 관리대상시스템에 적용함으로써, 일관된 보안정책의 실행과 중앙집중방식의 보안관리기능을 제공한다.

3. RMCS(Role-base Multiplex Certification System) 설계

역할 기반의 MIB 구현으로 중앙집중방식의 보안관리 기능과 다중인증 시스템을 이용하여 보다 안전한 RMCS System을 제안하고자 한다.

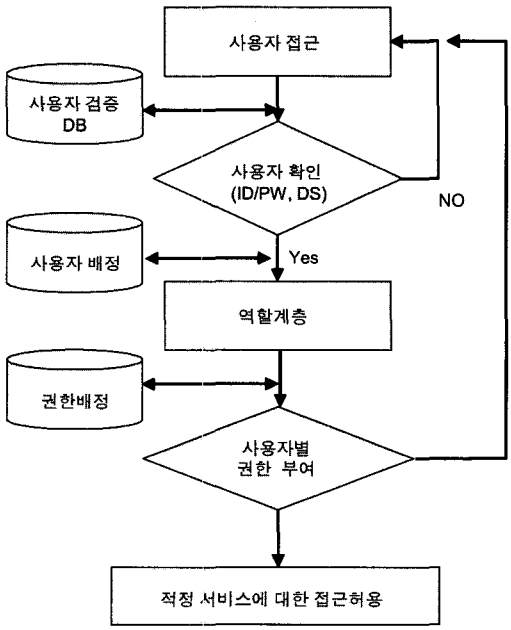
3.1 RMCS 시스템 구성

사용자가 ID/PW, 전자서명을 가지고 로그인을 하게 될 때 ID/PW만으로 로그인하는 제한된 권한을 가진 일반 user 접속과 ID/PW와 전자서명 모두를 포함한 로그인으로 Admin 권한을 가지는 접속으로 나뉘게 된다.

ID/PW 또는 ID/PW와 전자서명 모두가 올바른 사용자라면 시스템으로부터 Home 네트워크 원격 서비스를 이용할 수 있는 권한을 부여받게 된다.

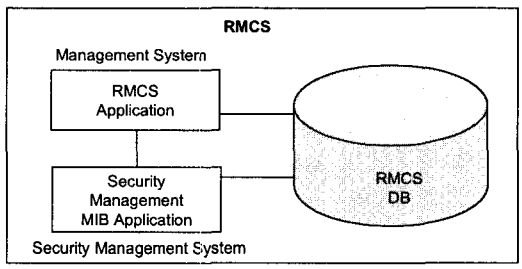
그러한 다중인증에 의한 로그인은 접속 역할기반의 접근통제 구조를 이용하여 각각의 접속자가 지정된 권한 레벨에 따라 서비스 이용에 제약을 두어 보안을 강화한다.

아래 (그림 2)은 RMCS의 인증에 따른 사용자의 권한이 역할기반으로 전환되는 모듈이다.



(그림 2) RMCS 모듈 진행 구성도

3.2 RMCS 시스템 구성요소 역할



(그림 3) RMCS 구조도

3.2.1 구성요소

① RMCS Management System

유·무선망을 이용하여 들어온 ID/PW, 전자서명을 이용한 접속 요청을 받아들이며 ID/PW와 전자서명의 진위여부를 DB로부터 파악하여 정당한 사용자의 접속요청에 대한 승인처리를 한다.

② RMCS Application

접속요청에 대한 인터페이스를 제공하며 ID/PW, 전자서명을 요구하여 정당한 사용자의 접속 요청에 대해서만 응답한다.

③ Security Management System

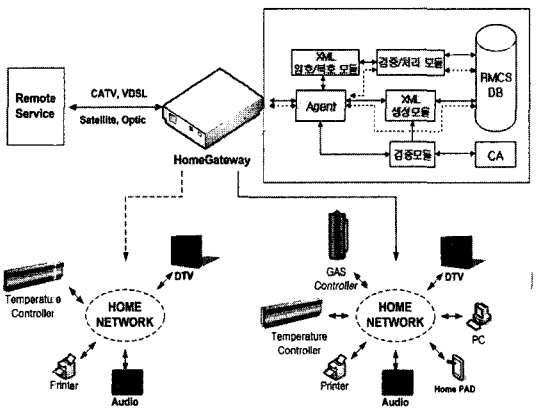
ID/PW, 전자서명등으로 정상적인 사용자로 확인되었다면, RMCS 서버의 MIB로부터 접속된 사용자에 대한 정보와 접속된 사용자별 권한정보를 조회한 후 사용자별 권한 레벨을 설정하고 그에 따른 권한부여를 실행한다.

④ Security Management MIB Application

권한부여의 처리 결과로 접속된 사용자의 사용권한 레벨에 따라 사용 가능한 서비스내역에 대한 인터페이스를 제공하며 권한별 각기 다른 관리제어 인터페이스를 보여준다.

3.3 RMCS 시스템의 실제 적용 모델

역할 기반의 MIB 구현으로 중앙집중방식의 보안관리 기능과 다중인증 시스템을 적용하여 보다 안전한 Home 네트워크 구축을 가능하게 하는 RMCS(Role-base Multiplex Certification System)의 모델을 아래의 (그림 4)와 같이 제안하였다.



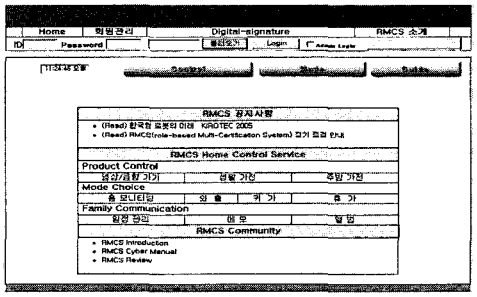
(그림 4) 제안된 RMCS 시스템 모델

4. RMCS의 WEB 모델 구현과 공격시나리오를 이용한 Test

RMCS 시스템은 웹상에서 회원가입을 통하여 서비스를 받는 형식을 갖추고 있으며 공격 시나리오를 통한 검증으로 안전성을 확인해 본다.

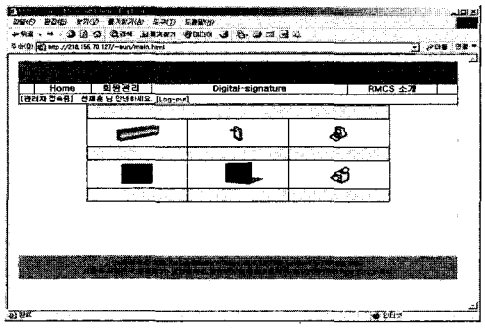
4.1 RMCS Web 모델의 구현

RMCS는 아래의 (그림 5)과 같이 웹상에서 ID/Password와 인증서 이용 유무를 이용하여 접속 할 수 있다.

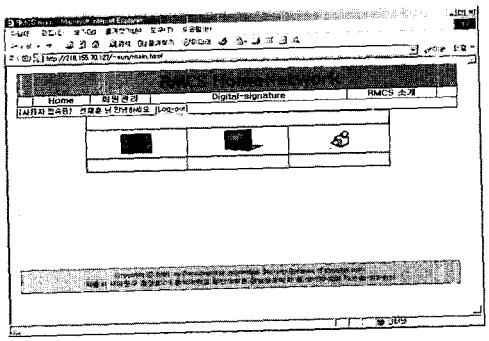


(그림 5) RMCS Web 모델 구현

이러한 ID/Password 및 인증서를 이용한 접속 시에 (그림 6), (그림 7)과 같은 권한에 따른 다른 접속 화면을 볼 수 있으며 각기 다른 권한을 가짐을 알 수 있다.



(그림 6) RMCS Web 관리자 접속 화면



(그림 7) RMCS Web 일반 접속 화면

4.2 테스트 환경

테스트에서 Home 네트워크 환경에 대해 침입을 가정한 공격을 가하여 기존 ID/PW 접근 방식과 ID/PW및 전자서명을 이용한 RMCS Web에 대해 아래 <표 1>과 같은 3가지의 대표적인 공격 방법을 이용한 가상의 공격을 차단하여 안전한 Home 네트워크 환경의 유지가 가능한지 실험을 하였다.

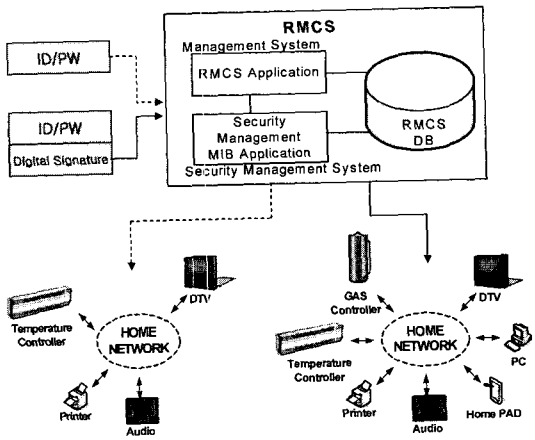
〈표 1〉 Home 네트워크 환경에 대한 가상 공격 방법

공격 방법	사용 공격 툴
Eavesdropping Attack	Sniffer
Dictionary Attack	Klepto
Backdoor Attack	Keylogger

공격에 이용된 3가지 방법으로는 첫 번째로, 통신장비간의 패킷 흐름에서 사용자의 패스워드를 알아내는 Sniffer 툴을 이용하는 것이고, 두 번째로는 사전 공격(Dictionary Attack) 방식의 Klepto 툴을 이용한 공격 방법이다,

마지막 세 번째로는 백도어 공격(Backdoor Attack) 방식의 Keylogger 툴을 이용하여 테스트를 실행하였다.

본 논문에서는 (그림 8)과 같은 다중인증에 의해 사용자의 접근에 대한 보안을 강화하며 내부에서 허가되지 않은 항목에 대한 접근을 역할기반의 관리구조로 제어하여 중요한 정보의 포함 또는 우선순위에 따라 지정된 항목을 제어 할 수 있는 권한을 사용자에 따라 다르게 부여하여 Home 네트워크 환경의 보안 고려사항에 대처한다.

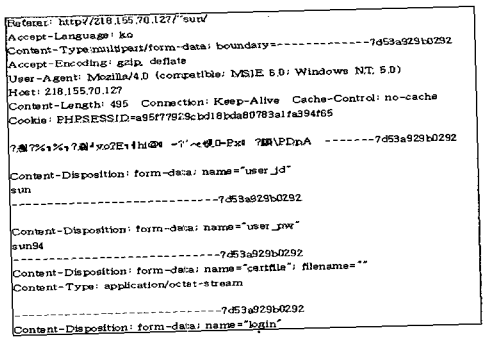


(그림 8) RMCS 적용 Home 네트워크 평가 환경

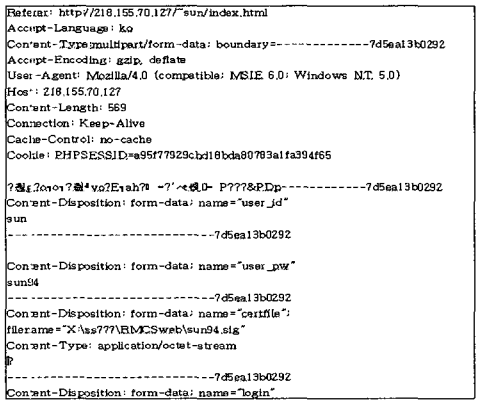
4.3 공격 시나리오

방법 1~3까지를 이용하여 기존 ID/PW 접근 방식과 ID/PW와 인증서를 이용한 RMCS Web에 대한 안전성을 검증해 본다.

방법 1 : 네트워크 패킷을 Eavesdropping Attack에 대한 비교

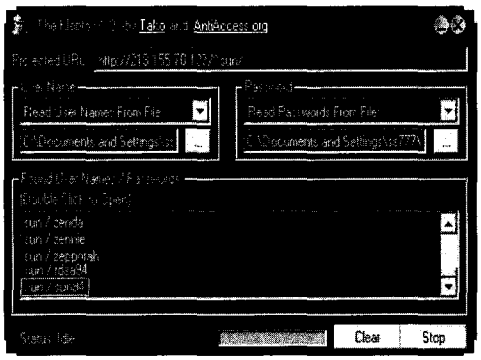


(그림 9) 기존 ID/PW 접근방식에 대한 TEST

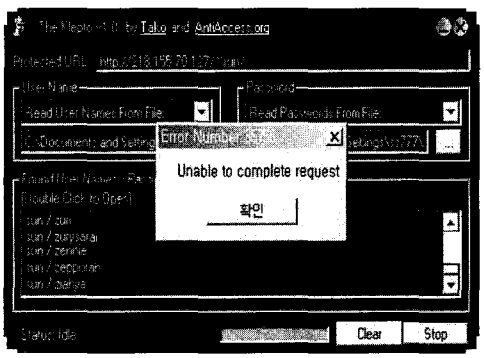


(그림 10) 제안된 RMCS 접근방식에 대한 TEST

방법 2 : Dictionary Attack에 대한 비교

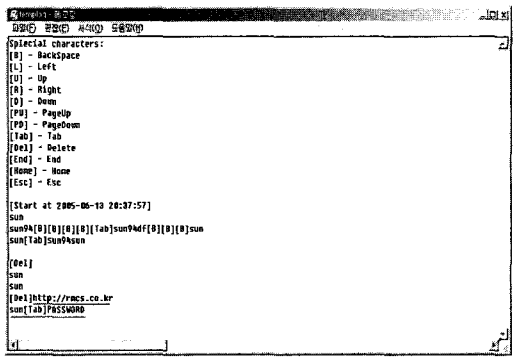


(그림 11) 기존 ID/PW 접근방식에 대한 TEST

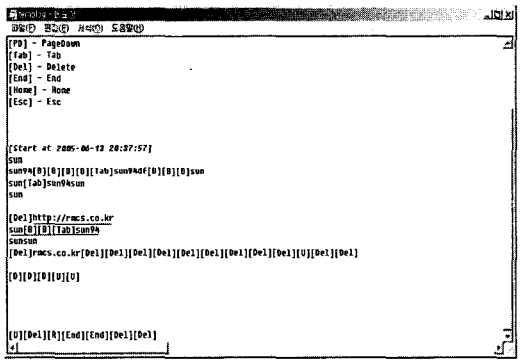


(그림 12) 제안된 RMCS 접근방식에 대한 TEST

방법 3 : Backdoor Attack에 대한 비교



(그림 13) 기존 ID/PW 접근방식에 대한 TEST



(그림 14) 제안된 RMCS 접근방식에 대한 TEST

4.4 테스트 성능 결과

Home 네트워크환경에 대한 침입에 따른 테스트 환경에서 실험의 결과는 <표 1>과 같다.

〈표 2〉 테스트 결과

		방법 1	방법 2	방법 3
침입시도	기존 방법 (ID/PW)	True	True	True
	제안 방법 (ID/PW+DS)	False	False	False

침입에 대한 가상공격으로 선정한 방법 1~3

까지의 시나리오대로 Home 네트워크에 가해지는 침해 사고에 대하여 기존 ID/PW 접근방식의 보안과 제안된 RMCS에 의해 ID/PW에 전자서명을 이용한 접근 방식의 보안을 비교 해보았으며 결과로 기존 ID/PW 방식에 의한 보안은 방법 1~3의 공격으로 보안에 심각한 위험이 생겼으나, 제안된 역할 기반의 다중인증 기법에 의한 접근방식은 ID/PW의 노출시에도 보안상의 문제가 발생하지 않았음을 알 수 있다.

5. 결론 및 향후 과제

본 논문은 사용자와 Home 네트워크 환경이 정보를 공유하며 위협으로부터 안전하게 서비스를 받을 수 있는 보안이 필요하다는 전제하에 기존의 댁내에 위치한 Home 게이트웨이 중심의 Home 네트워크 관리의 어려움을 해결하기 위한 해결책으로 RMCS를 제안하여 Home 네트워크환경을 위한 보안을 강화하고자 하였다.

또한 본 논문의 연구 결과에 따르면 RMCS는 기존 ID/PW 접속방식에 전자서명을 도입한 다중인증방식으로 Home 네트워크환경에서 보안을 보다 강화할 수 있음을 알 수 있고, 역할기반 MIB 모델을 이용하여 Home 네트워크 환경내에서 작업 및 정보취득의 권한을 제한하여 보다 안전한 Home 네트워크 환경 관리를 이룰 수 있다.

향후 과제로 Home 네트워크 환경 전반에 걸친 표준화가 이루어지지 않고 있으므로 전반적인 표준화 연구뿐만이 아닌 각 기술들의 특성에 따른 세분화된 응용 분야에 대한 기술적 요소의 연구와 보안 위협 요소들에 대한 연구와 체계적이고 효율적인 대규모 그룹관리와 이종기기간의 관리 방안에 대한 연구가 필요하겠다.

마지막으로 이번 논문에서 모듈 구현에 그친 내용에 대한 전체 시스템에 대한 직접적인 응용과 다양한 경로를 이용한 보안성 검증에 관한 실험 및 보완이 이루어져야 하겠다.

참 고 문 헌

[1] 김세영, 원덕재, 신동일, "XML 전자서명 시스템의 설계 및 구현", 한국정보처리학회, 제8권, 제2호, 2001.

[2] 이계상, 김한철, "전자서명 인증 기술동향", 정보통신연구지, 제3집, pp. 45-52, 2002.

[3] William Stallings, SNMP, SNMPv2, SNMPv3 and RMON1 and 2, 3rd Ed., Addison-Wesley, 1999.

[4] RFC 1157, Simple Network Management Protocol(SNMP), May 1990.

[5] Ravi S. Sanhdu, Pierangela Samarati, "Access Control : Principle and Practice", IEEE Computer, pp. 40-48, September 1994.

[6] David F. Ferraiolo, Janet A. Cugini, D.Richard Kuhn, "Role-Based Access Control(RBAC) : Features and Motivations", Proceedings of the 11th Annual Computer Security Applications Conferences, pp. 241-248, December 1995.

[7] 박명호, "RBAC 정책기반의 Rule-DB를 이용한 네트워크 침입차단 시스템 설계 및 구현", 한국정보과학회 논문집(1), pp. 745-747, 2003.

[8] "Role Based Access Control", BSR INCTS359, American National Standard for Information Technology, 2003.

선 재 훈

2000 경기대학교 토목공학 공학학사

2005 경기대학교 정보보호학과 공학석사

이 동 휘

2000년 경기대학교
전자계산학과(이학사)
2003년 경기대학교
정보보호기술공학과
(공학석사)
2004년 경기대학교 정보보호학과 박사과정

김 귀 남

미국 캔자스대학 수학과
(응용수학사)
미국 콜로라도주립대학
통계학과(통계학석사)
미국 콜로라도주립대학 기계
산업공학과(기계·산업공학박사)
현재 경기대학교 정보보호학과 주임교수