Home Network 게이트웨이에서 효율적인 MSAC 설계 및 구현

윤운관* · 최경호* · 김귀남*

요 약

홈 게이트웨이는 가정 내 홈네트워크를 구성하는 유비쿼터스 컴퓨팅(Ubiquitous Computing) 환경에서 통신과 제어 및 모니터링의 중심 역할과 더불어 외부 인터넷으로의 연결을 물리적으로 제공해 주는 장비이다. 홈게이트웨이를 통하여 홈네트워크 제어를 포함하는 다양한 서비스가 제공되고 있으며 홈 게이트웨이가 댁내망의 매체들간에 중재역할을 할 때 서비스 외부 공격 요인들로부터 데이터의 분석, 도청, 위/변조 등으로부터 대응할 수 있는 효율적인 보안기법을 채택하고, 홈 게이트웨이시스템을 최적의 상태를 유지함으로서 전송매체들간에 송/수신되는 데이터의 무결성을 보장하는 구조적인 보안시스템을 제시하고자 한다.

Design and Embodiment in Home Network at Gateway is Stabilization MSAC

Woon Kwan Yoon* · Kyong Ho Choi* · Kuinam J. Kim*

ABSTRACT

Home Gateway which composes Home network in Ubiquitous Computing environment is an equipment to provide the connection with the external Internet Physically, and it carry out the role which communication, control and monitor is important. But Home gateway has potential threats because it connected on external Internet as spillage user's information from outside wrongdoers. Consequently, Home gateway has to have security module and structure for the communication which is sate.

In this research paper, We designed Home gateway security structure for the communication which is protected when computer user use the computer from the outside to home to send information or important data.

Key words : Home Network, Home Gateway, Access Control

* 경기대학교 정보보호학과

1. 서 론

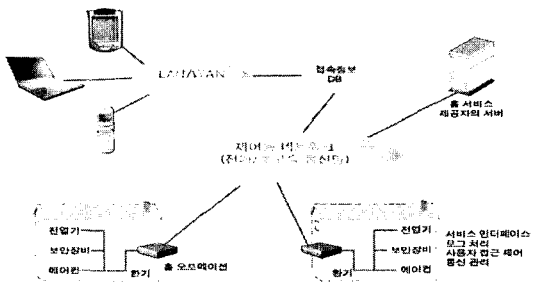
홈 네트워크는 콘텐츠 및 솔루션들을 외부서비스 네트워크환경, 즉 인터넷 망을 통해 연동하기 때문에 공중 네트워크에서 일어나는 해킹이나 바이러스 침입 등의 위험에 노출되어 있다. 이러한 잠재적 위험 요소를 고려하여 본 연구에서는 다가올 유비쿼터스 환경에서 보다 신뢰성을 갖춘 안전한 홈 네트워크 서비스 및 여건들을 제공하기 위하여 요구되는 홈 게이트웨이의 보안 요구 사항들을 각 홈 네트워크 구성 요소별로 살펴봄과 동시에 하나의 홈 게이트웨이에서 취약요소들로부터 감내하여 안전한 정보를 전송하기 위한 보안기술을 제시한다.

홈 게이트웨이의 보안을 말할 때 하드웨어적인 측면에서 홈 네트워크의 보안요소들은 기업과 비교하여 규모 면에서나 보안기술에 대한 고려 및 응용이 활발하지 않으며, 이론적 학문 고찰을 통한 보안응용기술들 중 정확한 분석이 안된 기술개발로부터의 오류(bug)로 인해 시스템의 안정적이지 못한 오류를 초래하며 이는 사용자 접근제어 수행시간을 지연시킬 뿐만 아니라 시스템에서의 큰 홀(hole)이 발생하여 외부 공격자나 취약요소로부터 충분한 공격의 요인이 된다. 따라서 본 논문에서는 위와 같은 이론적 학문 고찰에 의한 기술적인 문제점을 해결하고자 홈 게이트웨이에서의 접근제어 구조를 통한 효과적인 보안을 위해 새로운 기법 또는 메커니즘을 제안하였다.

2. Home Gateway 보안구조 및 관리 시스템 연구

2.1 Home Gateway 환경분석

전송기술이나 프로토콜의 표준화가 진행하면서 홈 게이트웨이의 기능은 RG(Residential Gateway)라는 독립적인 하드웨어 형태로 흡수되어질 것이다. (그림 1)은 RG를 이용하여 가전장비 제어를 하는 경우의 시스템 구성을 예로 든 것이다. 그림에서 홈 서비스 제공자 또는 장비제조 업체에서 준비한 홈 서비스 서버는 장비에 관련된 상태정보 DB와 접속정보 DB 및 서비스 홈페이지 운영 기능을 담당하며, 가전장비의 원격지 관리기능도 수행한다.



(그림 1) 가전장비 제어를 위한 RG 시스템 구성도

홈 게이트웨이의 중요한 기능 가운데 하나가 브릿지 기능이다. 브릿지 기능은 상이한 네트워크 기술들 간의 연계를 위한 기능으로서 일반적으로 다양한 네트워크 프로토콜들을 수용할 수 있도록 하거나 공통의 표준 기술(Ethernet, HomePNA, HomeRF, HomePlug 등)로 변환해준다. 브릿지는 독립적인 장비로도 만들어질 수 있으나 일반적으로 홈 게이트웨이가 브릿지 기능을 통합해 가는 추세이다.

2.2 Home Gateway 기술 및 동향

홈 네트워크 기술의 발전과 함께 홈 게이트웨이는 최근에 새로 생겨난 장치의 한 형태로서 미래의 가정정보화 실현을 위한 통신 및 접속 구조에 큰 영향을 미칠 것이다. 홈 게이트웨이는 댁내환경에서 여러 가지 유무선 홈 네트워크 기술들 중 하나 이상의 댁내망(LAN) 기술과, xDSL, 케이블, 광 및 위성 등 하나 이상의 액세스망(WAN) 기술을 상호 접속 및 중재하고 그 상위 계층에 미

들웨어 기술을 부가하여 가정의 사용자에게 다양한 멀티미디어 서비스를 제공하기 위한 클라이언트 장치로 정의할 수 있다.

홈 게이트웨이는 다양한 홈 네트워크 기술과 초고속 액세스 망 기술을 연결시켜 주는 장치로서 전 세계적으로 표준화 활동이 활발하게 시작되고 있는 분야이다. 세계적으로 ISO/IEC JTC1 SC25 WG1, TIA/EIA TR-41.5, OSGi(Open Service Gateway initiative), VESA(Video Electronic Standard Association) 등의 표준단체들이 활동하고 있는데, ISO/IEC JTC1 SC25 WG1는 홈 게이트웨이의 스펙 및 요구 사항 등을 정의하고, TIA/EIA TR-41.5는 미국내의 건물 자동화와 관련되어 효율적으로 멀티미디어 서비스를 분배하기 위한 홈 게이트웨이 표준을 정의한다. 그리고, OSGi는 서비스 게이트웨이의 API를 정의하고 있으며, VESA는 IEEE1394 기술에 근간을 두고 AV 기기, 셋탑 박스 등으로 이루어진 홈 네트워크 기기를 활용한다.

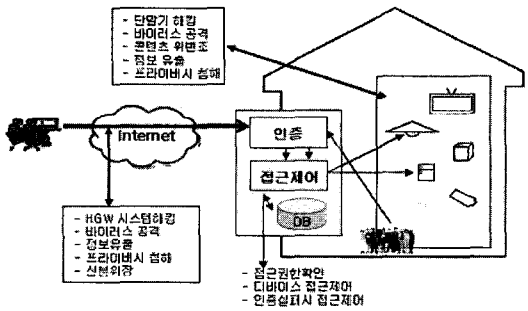
2.3 Home Gateway의 미들웨어 기술

하나의 가정 내에 여러 개의 기기가 존재하고, 각각의 기기가 같거나 다른 홈 네트워킹 미디어에 의해 연결되어 있을 때, 각각의 기기 간의 인터페이스 사이에 완충 역할을 해 줄 중간층이 없이는 이들 기기 간의 제어나 데이터의 전송은 불가능하다. 이러한 완충 역할을 해 주는 것이 홈 네크워킹 기기간 제어를 위한 미들웨어 기술이다. 미들웨어 기술을 이용하면 분산형 연산 환경과 서비스를 지원할 수 있으며, 데이터 네트워크와 제어 네트워크를 쉽게 통합할 수 있고, 여러 가지의 다양한 홈 네크워킹 기술을 이용한 기기 간의 데이터를 통합하기가 쉬우며, SNMP(Simple Network Management Protocol), DHCP(Dynamic Host ConfigurationProtocol), ARP(Address Resolution Protocol), IP over 1394, 그리고 Graphic User Interface (GUI) 등과 같은 높은 층의 응용을 구현하기가 쉽다.

2.4 Home 게이트웨이 위협요소 분석

홈 네트워크에서 공격자 유형은 크게 수동적 공격자, 능동적 공격자로 나누어 볼 수 있다.

수동적 공격자는 송/수신되는 데이터를 관찰하고 데이터를 분석함으로써 통신하는 주체의 키를 획득하기 위해 노력한다. 이렇게 해서 획득한 키를 통해 수동적 공격자는 통신을 하는 사용자가 어떤 메시지를 주고받는지 알 수 있다.



(그림 2) Home 게이트웨이 보안구조

2.4.1 Home 서버 및 게이트웨이 보안 취약점

소비자가 정보가전 제품과 같은 가정내의 모든 정보 단말기를 인터넷이나 휴대정보 단말기로 연결하여 언제 어디서나 손쉽게 제어할 수 있는 홈 서비스 환경에서 다양한 가정정보 서비스를 안전하게 제공받기 위해서는 외부 망(인터넷)과의 연결은 필수적이다.

2.4.2 정보가전기기의 보안 취약점

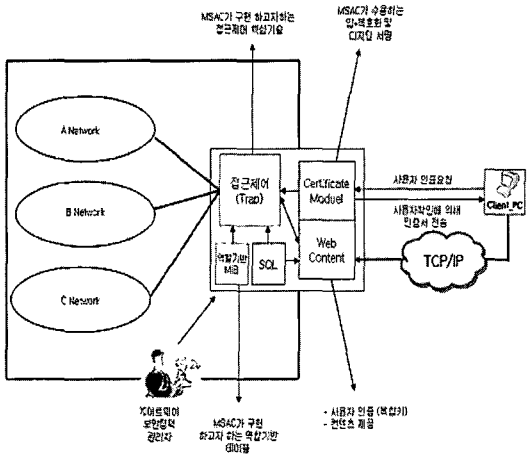
유비쿼터스 홈 네트워크에서 다양한 가전기기들-TV, 팩스, 프린터, PC 등-을 구성하는 댁내망의 보안 취약점들은 외부(인터넷)의 바이러스나 웜에 의한 노출 위협, 데이터의 유출, 변형에 따른 위험이 존재하게 된다.

2.4.3 Home 게이트웨이 취약점 유형

무선으로 구성된 경우 그 특성상 전파가 외부로 노출될 수 있고 홈 외부에서 무선 데이터 분석을 통해 댁내에서 어떤 일을 수행하는지 알 수 있다. 또한 통신 데이터를 변조하여 정당한 서비스를 받지 못하게 하거나, 데이터를 위조하여 전송해서 서비스 사용자가 예기치 않은 결과를 초래할 수 있는 송수신이 가능하다.

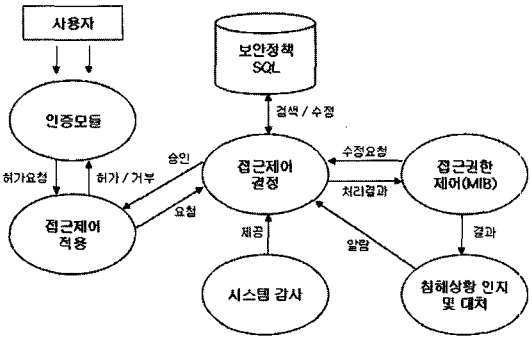
3. Home Gateway MSAC(Management System of Access Control) 구조설계

홈 게이트웨이로 오는 모든 트래픽을 의심스럽게 봐야 한다는 개념에서 사용자가 TCP/IP환경을 통해 댁내 망의 각각의 네트워크제어를 하고자 할 때 홈 게이트웨이 구성에서 사용자인증을 통한 접근권한과 MSAC(Management System of Access Control) 제어구조를 통해 바이러스, 오류, 외부공격으로부터의 기존 관리시스템보다 좀더 향상된 효율적인 데이터처리를 하기 위한 구조를 나타내고 있다.



(그림 3) MSAC 전체 흐름구조

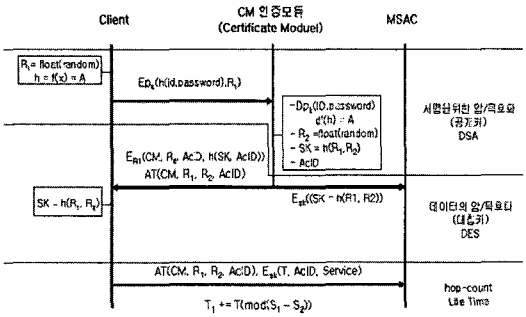
MSAC 시스템에서는 핵심구현기술부분을 크게 집행(Enforcement)과 정책(Policy) 구조를 갖는다. 이것을 구성하는 세부적인 동작절차에 필요한 역할별 요소들의 객체는 다음과 같다.



(그림 4) MSAC 정합블럭도

사용자 요청메시지는 인증모듈과 접근제어적용을 통해 서명이 이뤄지며 이를 통해 들어온 데이터는 접근제어 적용 블록으로부터 메시지 큐 선입선출(FIFO : First in First out) 대기열에 정합되어져서 순차적으로 놓여지게 된다. 이때 접근제어 결정 블럭은 유입되는 데이터에 대해 권한제어에 필요한 정책을 데이터베이스와 MIB 테이블로부터 정보를 수집한다. 따라서 사용자데이터에 대하여 역할에 기반한 정책권한을 부여하고 각각의 컨트롤 박스로 전송하여 송·수신되는 데이터에 대한 결정 블럭을 침해상황인지 모듈에서 알람 발생 정보와 스케쥴링에 의한 시스템감사를 통한 프로세서의 상태 및 데이터(패킷)의 유입량, 포트 이상유·무의 정보를 취합하여 필터링 하는 기법이다.

본 MSAC의 사용자인증 프로토콜 구조는 기존 공개 키나 대칭 키 암호화 방식에서처럼 암호화된 사용자정보 및 데이터에 대해 복호화 적용 시 하나의 메커니즘에 의한 동시에 서명에 대한 해쉬와 복호화가 이루어지는 방식이 아닌, 사용자 확인절차(서명) 및 데이터 복호화 처리과정을 분리시킨 구조이다.



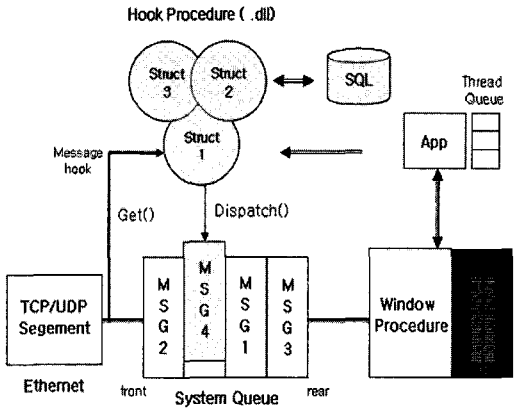
(그림 5) MSAC 사용자 인증 프로토콜

〈표 1〉 사용된 약어 및 기호

기 호	설 명
R1	Client가 생성한 대칭 키 랜덤넘버
RF	R1의 최초 생성 값
R2	CM가 생성한 대칭 키 랜덤넘버
Epk(·)	공개 키를 위한 암호화
SK	대칭 키공유 세션키
Dpk(·)	복호화를 위한 개인키
h(·)	일방향 해쉬함수
AcID	접근제어권한 넘버
AT	인증티켓
Ek(·)	대칭 키를 위한 암/복호화
f(·)	생성함수
X	서명 key
A	서명원문
df(·)	서명 복호화

사용자와 CM(Certificate Module)간에는 공개키 암호화 방식에 의한 인가된 사용자에 대한 서명과정으로 이루어 지고 사용자에 대한 인가절차가 이루어진 후에 대칭 키 암호화 방식에 의한 사용자(Client)와 MSAC(Management System of Control) 접근제어가 이루어지게 된다.

정합 블럭에 의한 집행과정이 사용자 인증과 홉 카운트 연산을 통해 외부 침입자로부터 차단하는 보안구조라면, 정합 블럭에서 정책적용 접근제어 구조로서, 홈 게이트웨이 내부취약요소인 특정 포트를 이용한 웜 바이러스 혹은 서비스거부 공격(Dos)등에 의한 접근 제어 단에서 어플리케이션 감사정책을 통한 안정적인 시스템운영을 하기 위한 보안 기법이다.



(그림 6) MSAC 훅 프로시저

(그림 6)에서의 시스템 구조에서는 사용자 데이터가 이더넷을 통해 유입될 때 관리자 어플리케이션에 의해 시스템 리소스 사용률과 TCP/UDP 세그먼트에서의 감사를 통해 악성 패킷에 대한 정보를 파악하여 훅 프로시저를 호출하게 되고 이렇게 호출된 훅 프로시저는 보안정책에 의하여 관련 없는 메시지데이터를 시스템 큐(Queue)로부터 비교·분석하여 처리(Dispatch)하게 된다.

훅 프로시저에 의한 처리구조는 3개의 구조체 원형을 갖게 되며, 첫 번째 처리구조는 감사정책에 의한 이더넷으로 부터 유입되는 메시지에 대한 감시를 하여 비정상 메시지가 시스템 큐(Queue)에서 대기하게 될 주소 포인터를 리턴 받아서 해당 주소에 대한 메시지를 처리하게 되며, 두 번째 구조체에서는 첫 번째 구조체가 가져온 데이터를 비교 분석하여 조작/변경/삭제하는 역할을 처리하게 된다. 마지막 세 번째 구조체는 데이터의 전달(pass) 및 시스템 큐의 메모리 공간에 대해 반환 여부를 처리하게 된다.

4. 결 론

홈 게이트웨이는 하나 이상의 홈 네트워크와 하나 이상의 액세스망(Home Access Network)을 상호 접속, 중재하여 인터넷 서비스 등 다양한 멀티미디어 서비스를 제공하기 위한 장치로 정의할 수 있으며, 기본적으로 LAN과 WAN을 연결할 수 있는 지능적인 인터페이스를 제공해야 한다.

따라서 본 논문에서는 홈 게이트웨이 시스템으로 서비스 제어를 위해 외부 망으로부터 제어를 위한 메시지 데이터가 유입될 때 위협요소들에 의한 악성 메시지 데이터로 인해 시스템의 오류 및 서비스를 방해하는 요소들로부터 훅(Hook) 기법을 이용한 접근제어구조를 통해 비정상적인 메시지 데이터를 추출함에 따라 시스템의 안전성을 보장하며 원활한 서비스를 제공할 수 있는 시스템 구조설계를 제시하였다. 이렇듯 내-외부망의 중재 역할을 하는 홈 게이트웨이에서도 다양한 이기종간의 전송 프로토콜에 대한 호환 인터페이스 제공과 구조적인 측면에서의 통합적인 관리형태의 보안구조에 대한 연구가 지속적으로 이루어져야 된다고 판단된다.

참 고 문 헌

[1] HomeGateway, http://cnscenter.future.co.kr
[2] HomePlug, http://www.homeplug.com/about/
[3] IEEE1394, http://www.ieee1394.org
[4] Steve G. Ungar, "Home Network Security", IEEE Fourth International Workshop on Network Appliance(IANA-4).
[5] B. Clifford Neuman and Stuart G. Stubblebie, "A Note on the Use of Timestamps as Nonces Operating Systems Review", 1993.
[6] H. Orman, "The OAKLEY Key Determination Protocol", IETF RFC 2412, Nov. 1998.
[7] 국내외 홈 네트워킹 기술 표준화 동향 및 발전 전망, 전자부품연구원, 최광순, 정광모, 2003.

윤 운 관

2003년 호원대학교 컴퓨터과학부(이학사)
2004년~현재 경기대학교 정보보호학과 석사과정

최 경 호

2003년 경기대학교 경제학과 (경제학 학사)
2005년 경기대학교 경제학과 (경제학 석사)
2005년~현재 경기대학교 정보보호학과 박사과정

김 귀 남

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