홈네트워크용 방화벽 보안 필요 사항 연구

최 성*, 김승찬*, 선진국*, 조상일*, 차성훈*, 김 훈**
*남서울대학교 컴퓨터학과
**휴먼터치소프트기술연구소

A Study on the Necessary Home-Network Firewall Security

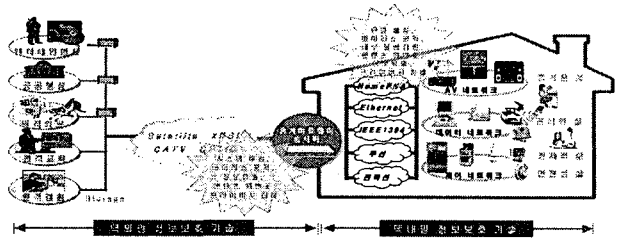
Sung Chol*, Seng-Chan Kim*, Jin-Kook Sun*, Sang-Il Cho*
,Sung-Hun Cha*, Hoon Kim**
*Computer Science, NamSeoul University
**Human Touch Soft Technology Center.

요 약

언제 어디서나 컴퓨팅이 가능한 유비쿼터스 컴퓨팅 사회에서는 개인의 컴퓨팅 환경 의존도가 증가함에 따라 사이버공격으로 인한 개인생활의 위협도 증가할 수 밖에 없다. 홈네트워크는 유비쿼터스 컴퓨팅 환경으로 가는 시작점이라고 할 수 있으므로 인터넷을 통한 사이버 공격의 증가는 눈앞에 현실로 다가오고 있는 홈네트워크의 활성화를 방해하는 장애물로 대두될 것이 틀림이 없으므로 이에 대한 대응책 마련이 시급하다. 본 연구에서는 안전한 홈네트워크 구축을 통하여 홈서비스가 활성화될 수 있도록 홈네트워크의 보안취약성 및 관련 보안기술 개발에 대한 연구와 홈네트워크에 필요한 보안사항을 연구하였다.

1. 홈네트워크 보안 기술

홈네트워크는 외부 인터넷과 연결을 위한 가입자망으로 xDSL, Cable, FTTH(Fiber To The Home) , PLC(Power Line Communication), 위성, IS-95, 3G, 4G, IEEE802.11 등의 다양한 유·무선망의 사용이 가능하다. 홈 네트워크는 그 적용 대상에 따라 여러 대의 PC 및 컴퓨터 관련 장비간의 통신을 위한 정보 네트워크, 가전장비 제어를 위한 자동화 네트워크, 음향 및 영상기기나 게임기 등의 오락 또는 문화생활을 위한 엔터테인먼트 네트워크 등 3가지 네트워크로 나눌 수 있다.



(그림 1) 홈네트워크의 보안취약점

홈네트워크에서는 다양한 유·무선 네트워크와 프로토콜 등의 혼재로 기존 인터넷 등에서 발생되던 보안취약성외에도 추가적으로 고려해야할 보안취약성이 존재하고 있다. 홈네트워크에는 Ethernet, HomePNA, PLC, IEEE 802.1x, Bluetooth, UWB(Ultra Wide Band) 등 다양한 홈네트워킹 기술이 사용 가능하나 홈네트워크 측면에서 매체의 보안취약성을 해결할 수 있는 대응기술을 갖고 있지 못하며, 미들웨어의 경우에도, 각 미들웨어들이 요구하는 보안기능을 모두 만족할 수 있고 개별 미들웨어를 통합한 통합미들웨어 환경에서도 유연하게 보안기능을 제공할 수 있는 보안인프라가 아직 개발되지 못하고 있다.

2. 홈네트워크 보안기술 개발

홈네트워크는 인터넷과의 연결로 인하여 인터넷에서 발생되고 있는 다양한 사이버공격에 그대로 노출되어 있어 해킹, 악성코드, 웜 및 바이러스, DoS(Denial of Service)공격, 통신망 도·감청 등에 보안취약성을 갖고 있다.

홈게이트웨이는 댁외의 공중망과 댁내의 홈네트워크를 연결하는 입구로서 외부의 불법 침입에 대해 일

차적인 대응 방안을 제공한다는 개념에서 최우선적으로 보안기능이 탑재되고 있다. 홈게이트웨이에 탑재된 대표적인 보안기능에는 Firewall, VPN (Virtual Provate Network) 등이 있다.

현재까지 개발 및 상용화된 보안기능이 제공되는 홈게이트 제품 현황은 표1과 같다. 국외 제품의 경우, 대부분이 미국제품으로 보안측면에서 제공되는 기능은 Firewall, VPN 등으로 대부분이 제한적인 유사한 보안기능만을 제공하고 있다. 아직 홈네트웍크용 전용 보안제품은 나오지를 않고 있다.

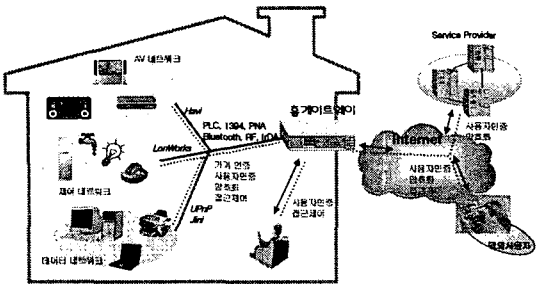
3. 보안사항

3.1 홈네트워크 보안프레임워크

미들웨어	제공 보안기능 현황
UPnP	• Ver 1.0에서는 보안기능이 정의되어 있지 않음 • Ver 2.0에서 보안기능이 추가될 예정임 - 제품 인증기능 제공 - 기기간 인증기능 제공 - 접근제어를 위한 Device가 자체적인 ACL 제공 - 기밀성 제공
Jini	• Ver 1.0의 보안기능은 Java Security에 의존 - 사용자 인증 기능 제공 - 기기간 인증 기능 제공 - 메시지 무결성 및 기밀성 제공 - 접근제어 기능 제공 • Ver 2.0에서 추가적으로 상호인증, 인가기능, 코드 무결성 등에 대한 기능이 강화됨
Havi	• Havi 인증서를 이용한 인증기능 제공 • 접근제어 기능 제공
LoneWorks	• 기기간 인증기능 제공
HNCP	• 보안기능 정의 안되어 있음 (Ver 1.0)

홈네트워크에서는 이종의 유무선 네트워크와 다양한 프로토콜 등의 혼재로 기존 인터넷 등에서 발생되던 보안취약성 외에도 추가적으로 고려해야할 보안취약성이 많이 존재한다. 홈네트워크의 다양한 정보가전 기기들은 인터넷과의 연결로 사이버공격의 대상이 될 수 있으며, 더욱이 홈네트워크 내의 정보기기의 다양성과 기기간 자원의 공유 등으로 보안측면에서 고려해야할 보안요구사항은 더욱 복잡해지고 다양화되고 있다. 또한, Ethernet, HomePNA, IEEE1394, PLC, IEEE 802.1x, Bluetooth, UWB 등 다양한 홈네트워킹 기술이 활용될 것으로 예상되고 있으나 대부분은 보안취약성에 대한 대응기술이 아직 개발되지 못하고 있다.

홈네트워크를 구성하는 다양한 통신매체나 프로토콜 등과 관계없이 요구되는 보안기능을 만족할 수 있는 보안프레임워크가 정립되어야 하며, 홈네트워크의 발전전망을 고려하여 현재 추진 중인 시범서비스에서 연동될 수 있는 수준의 보안기술과 향후 유비쿼터스 컴퓨팅 환경에 근접한 홈네트워크 모델에서 활용될 수 있는 보안기술로 나누어 실질적인 기술개발을 추진하는게 효율적이다.



(그림 2) 홈네트워크 보안취약성 대응을 위한 보안기능

3.2 디바이스 인증

불법 디바이스의 사용을 방지하지 위해서는 홈네트워크의 구성요소인 디바이스 자체에 대한 인증과정이 필요하다. 현재까지 디바이스 인증은 미들웨어 레벨에서 제공되고 있다. UPnP의 경우, 디바이스 마다 부여된 Security ID로 디바이스의 홈네트워크 등록과정에서 디바이스 인증이 이루어지고 있으며, Havi의 경우에는 디바이스마다 고유한 인증서를 발행하여 디바이스 인증 수행 시 사용하고 있다.

디바이스 유효성 확인을 위한 시리얼 넘버나 인증서 등은 개별 제조업체 등에서 자체적으로 발행하고 있어 향후 디바이스에 대한 다양한 사후 서비스 제공이나 유비쿼터스 컴퓨팅 환경에서 디바이스 및 사용자 인증 기능과 결합한 새로운 서비스의 제공을 위해서는 디바이스 인증정보에 대한 통일된 발급체계 및 관리체계에 대한 기술적, 정책적인 연구가 필요하다.

3.3 사용자 인증

홈네트워크에서는 디바이스 인증 외에 디바이스를 사용하는 사람의 신원확인을 위한 사용자 인증기능도 반드시 필요하다. 홈네트워크에는 생체인식, 패스워드, 인증서, 스마트카드 등 다양한 사용자 인증기술의 활용이 가능하겠지만, 유비쿼터스 컴퓨팅 환경으로의 진화를 고려할 때 정보단말기기의 낮은 성능을 고려한 사용자 인증기술의 활용의 적용성이 검토되어야 한다. 기존의 다양한 사용자 인증기술을 수용할 수 있는 종합적인 사용자 인증 인프라기술 개념으로 개발되어야 한다.

3.4 기기간 인증

원할한 홈서비스 제공을 위해서는 기본적으로 홈네트워크 구성요소 간의 자원공유를 위한 신뢰가 확보되어야 한다. 이를 위해서는 구성요소 간의 기기간 상호인증이 필요하다. 사용자 인증 기능, 접근제어 기능 등을 위해서는 기본적으로 기기 간 인증기능이 우선되어야 하므로 다른 보안기능과의 연동성이 고려되어야 한다. 또한, 현재 개발 중인 통합미들웨어 상에서도 유연성있는 기기 간 인증기능이 제공되어야 하므로 통합미들웨어 환경에서의 인증 기능에 대한 연구도 필요하다.

3.5 접근제어

홈서비스에 따라 홈네트워크 자원에 대한 접근권한 제어 기능이 요구된다. 홈구성원별로 제공받을 수 있는 홈서비스의 종류가 다르고 홈네트워크 구성요소에 대한 제어 범위도 다르므로 이에 대한 접근제어 기능이 필요하다. 유비쿼터스 컴퓨팅 환경을 고려할 때 접근제어를 위한 ACL(Access Control List)은 단말기기가 내장하고 있는 것이 효율적이라고 할 수 있지만 안전성 측면이나 사용자 편리성 측면에서 일관된 보안정책따라 접근권한이 제어되어야 하므로 홈게이트웨이에서 종합적으로 관리하는 방안에 대해서도 검토가 필요하겠다. 또한, 인증 정보 유출로 인한 불법적인 접근시도가 발생한 경우, 보안정책을 능동적으로 변경하여 공격에 대응하는 보안기능에 대해서도 연구가 있어야 한다.

3.6 미들웨어 보안기능

홈네트워크를 구성하는 경우에도 여러 가지의 다양한 미들웨어가 사용되고 미들웨어별로 제공되는 보안기능도 다르고 구현방법도 상이하므로 보안측면에서 고려해야할 부분이 많다. 미들웨어상에서 보안기능의 통합화에 대한 연구도 필요하겠다. 또한, 홈네트워크 보안프레임워크 연구과정에서 미들웨어의 보안기능 외에 추가적인 새로운 보안기능의 개발 필요성에 대해서도 검토가 필요하므로 이를 위한 미들웨어 보안기능에 대한 안전성 분석이 필요하겠다.

기타 그밖에 홈게이트웨이에서의 침입에 대한 대응기능 및 VPN서비스의 고도화도 필요하며, End-to-End 보안서비스를 위해 정보가전기기에서의 기밀성 제공 기능도 개발이 필요하겠다. 외부 스팸메일이나 불법적인 컨텐츠로부터 홈구성원 특히, 아이들을 보호할 수 있는 보안기능의 개발도 필요하다.

4. 결 론

유비쿼터스 컴퓨팅 환경 구현을 통해 창출될 시장규모가 580조원을 상회할 것이라는 연구보고서만 보아도 유비쿼터스 컴퓨팅 환경의 시작점으로 인식되고 있는 홈네트워크 시장 육성의지와 맞물려 관련 업체들이 적극적으로 시장에 참여하고 있다. 10대 신성장 동력으로서 홈네트워크 산업은 연구가 활발해질 것이며, 산업체의 적극적인 시장참여로 홈네트워크 분야 활성화를 통한 경제적, 사회적 기대가 높아만 가고 있지만, 안전성이 확보되지 않는 홈서비스는 사용자로부터 외면을 받을 수 밖에 없다. 더욱이 홈서비스에 따라 개인의 경제손실뿐 아니라 생명까지도 위협받을 수도 있으므로 홈서비스 활성화에 있어 보안기술이 차지하는 매우 중요하다고 볼 수 있다. 이 연구에서는 홈네트워크 보안프레임워크부터 세부 보안기능 등에 대한 요구사항 등을 모두 반영한 홈네트워크 기술을 개발한다면 홈네트워크 분야를 통해 예상되고 있는 시장 선점을 통한 미래 지향의 가정환경 구현이 가능해질 것이다.

참고문헌

[1] 박광로, 송영준, "홈네트워킹", TTA저널, 제78호, pp.101-109, 2001.

[2] 전호인, "디지털홈기술 및 표준화동향", TTA저널, 제88호, pp.59-73, 2003.

[3] 이윤철, "최근의 홈네트워크 기술동향 및 시장전망", 주간기술동향, 제1098호, pp.22-33, 2003.

[4] Carl M.Ellison, "Interoperable Home Infrastructure Home Network Security." Intel Technology Journal, Vol 6., pp.37-48, 2002.

[5] "Home Network Control Protocol(HNCP) Prespec. Ver. 1.5", PLC 포럼 디지털 가전위원회, 2003.