신호 인증서버를 통한 허가되지 않은 WOL 보안※

이우기, 박순형[0], 임차성
인하대학교 산업공학과
trinity@inha.ac.kr, fgm0626@inhaian.net ,limcs79@inhaian.net

Protecting Unauthorized WOL by Signal Authentication Server

Wookey Lee, Soonhyoung Park[0], Chasung Lim
Dept. of Industrial Engineering, Inha University

1. 서 론

원격 컴퓨터 관리기능 중의 하나인 WOL(Wake On LAN) 은 특정신호(예: '매직패킷')를 받는 순간 메인보드와 연결되어 있는 네트워크 카드가 컴퓨터의 전원을 켜주는 역할을 할 수 있다[1]. 문제는 패킷의 특성 때문에 브로드캐스트 방식으로 진행되어 같은 네트워크망 안에 있는 모든 PC는 이 신호를 받게 된다. 따라서 허가된 사용자뿐만 아니라 동일 네트워크망 안에 있는 누구든 해당 컴퓨터의 몇 가지 정보를 아는 경우 해당 컴퓨터를 켤 수 있다. 만일 컴퓨터가 켜지게 되면 해당 컴퓨터는 해킹 등의 공격이 가능한 범위에 놓이게 때문에 정보유출의 가능성이 커지게 된다. 따라서 이러한 신호를 인증하는 서버를 둠으로써 들어오는 신호를 분석하고 허가 여부를 확인하여 해당 컴퓨터의 상태를 통제함으로써 그러한 위험에 대한 방어 방법을 제안한다.

2. 본 론

WOL기능은 회사에서 일이 끝나고 컴퓨터를 끈 상태로 모두 퇴근하였을 때 이를 이용하여 시스템 관리자들이 원격 조정하여 해당 기기에 소프트웨어 설치 및 설정 변경을 하는데 쓰기 위해 고안되었다. 만약 이러한 기능이 없었다면 직접 컴퓨터 앞에 가서 전원버튼을 하나하나 눌러 주어야 했을 것이다. WOL의 작동과정은 다음과 같다. 네트워크 카드에서 신호를 받던 중 매직패킷이라는 특정한 신호를 받으면, 네트워크 카드와 연결되어 있던 메인보드에서 컴퓨터를 켜게 된다.[2] 이러한 과정은 OSI 2계층(데이터링크)에서 일어나는 일이기 때문에 기본적으로 브로드 캐스트 되며, 이러한 이유로 해당 네트워크망 안에 있는 모든 기기들은 이러한 패킷을 받게 된다.

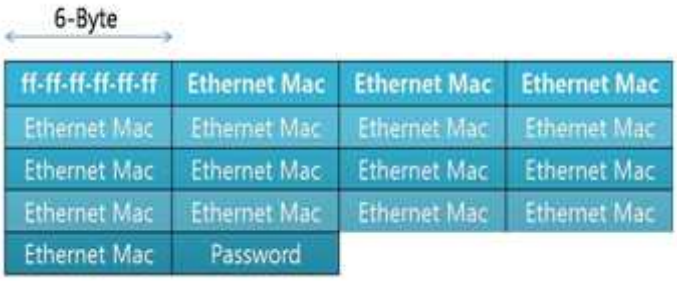
매직패킷은 Source IP와 PORT, Destinamtion IP와 PORT의 정보가 들어있는 UDP 헤더부분과 ff-ff-ff-ff-ff-ff와 해당 컴퓨터의 맥어드레스로 구성된 데이터로 나누어져 있다. 이를 보면 알 수 있듯이 내가 켜고자 하는 컴퓨터의 맥어드레스만 알고 있다면, 해당 네트워크망에 있는 누구나 다른 사람의 컴퓨터를 켤 수 있다. 어떤 회사나 조직에서 WOL을 쓸 수 있는 사람은 관리자와 회사원 본인이 허가해 준 IP에서만 쓸 수 있게 만드는 것이 가장 올바른 관리 방식이며, 또한 개인의 경우 자신이 허가해 준 IP에서만 쓸 수 있어야 하는 것이 올바른 보안관리 정책의 목표가 될 수 있다.

최근에 많이 등장하고 있는 IPv6라는 기술이 발전되어 모든 전자기기에 IP가 들어간다면 WOL은 모든 전자기기를 외부에서 켤 수 있는 기술이 될 수 있으며, 그 경우 이러한 문제는 더욱 심각해질 수도 있다[3]. WOL의 방식이 비교적 간단하기 때문에, 약간의 프로그램 과정에서의 오류라던가, 악의적인 사용자가 해당 기기에 접근하는 것이 매우 쉽다. 이러한 현상은 결국 IP를 가질 수 있는 대부분의 생활기기가 임의로 켜진다고 생각할 수 있다. 이러한 상황은 현재까지 보안이 이루어지지 않는 공백의 영역이며, 따라서 악의적 활용을 막는 조치를 취해야 한다는 점에서 본 연구는 매우 시의적이라 하겠다.

이와 연관된 기술로 최근에 나와 있는 것은 Secure-On이다. 아래의 **[그림 1]**이 Secure on기능에서 작동하는 매

※ 본 연구는 지식경제부 및 정보통신산업진흥원의 대학 IT연구센터 육성·지원사업(NIPA-2010-C1090-1031-0002)의 연구결과로 수행되었음.

직패킷의 구조 이다. 이 기술은 일반적인 신호 뒤에 6BYTE의 암호를 추가하여 신호가 전송되어 올 때 뒤에 암호가 있는 것만을 인식하고 작동한다. 하지만 이 방식은 각각의 기기마다 다른 암호가 설정되기 때문에 관리적인 측면에서 비현실적이다. 이 경우 TLS암호화 방식을 사용하여 WOL을 통한 위험을 막을 수도 있는데 이 방식은 128비트의 암호와 2048비트 길이의 RSA 키 모듈을 사용한다. 하지만 이러한 시스템은 AMT기반의 컴퓨터에만 제공된다는 한계가 있다[3].



[그림 1]Secure on기능에서 작동하는 매직패킷

이러한 문제를 해결하기 위해 본 논문에서는 일반적으로 적용될 수 있는 신호 인증서버라는 시스템을 도입하고자 한다. 해당 네트워크망 안에 이러한 인증서버를 둠으로써 받게 되는 신호를 분석하고, 그러한 정보 중 Source IP가 허가된 사용자인지 확인함으로써, 의도하지 않은 WOL을 효과적으로 차단하는 것이다. 이와 같은 시스템의 장점은 하나의 서버로 다수의 컴퓨터를 관리할 수 있다는 장점이 있다.

3. 결 론

WOL은 시스템 관리자들에게 있어 편의성을 제공하고, 유무선통신망의 발전에 따라 원격접속을 활용하고자 하는 사용자 편의성 증대에 따라 네트워크에 연결되는 기기의 숫자가 급격히 확대되는 추세와 맞물려 최근 급속히 확산되고 있는 기술이다. 뿐만 아니라 이 기술이 최근에는 많이 알려지면서, 휴대용 기기에 까지 다양하게 도입되고 있다. 하지만 이러한 기술의 편리한 적용의 이면에는 그 보안성의 취약성이 적용되지 않았고, 현재로서는 이 기능의 보안절차가 마련되어있지 않다.

본 논문에서는 WOL을 위한 신호 인증서버를 도입함으로써, 허가된 IP와 되지 않은 IP를 구분하고 허가되지 않은 IP라면 종료 코드를 보내어 끄는 시스템을 제안하였다. 또한 분석은 컴퓨터가 꺼져있을 때만 함으로써, 인증서버의 과부하를 막고, 헤더 파일이 변조될 경우에 대해서도 막을 수 있는 시스템을 구현하였다.

후속 연구에서는 그리고 본 연구에서 적용한 단순한 헤더파일 변조방식을 보완하는 다양한 보안정책이 적용될 수 있다. 또한 Secure-On방식의 취약점과 WOL에 쓰이는 신호를 전달하는 것이 브로드캐스트가 아닌 단일캐스트가 가능한지 검증할 필요가 있다. 그리고 근본적으로 본 기술을 확장하여 서버 혹은 서버팜(Server Farm) 등의 에너지 절감방식에 적용할 수 있다. 즉, 모든 서버를 켜두지 않고, 사용자 접근빈도 혹은 활용 정도에 따라 필요한 서버만의 전원을 수시로 스케쥴링 하는 에너지 절감방식[4][5]에 있어서 본 연구에서 제안하는 보안절차를 적용하는 연구가 가능하다.

4. 참고문헌

[1]Nilesh, M., Kameswari, C., Bhaskaran R., Abhinav P., "Wake-on-WLAN", International World Wide Web Conference, pp761-769, 2006

[2]Charles E., David B., "Mobility support in IPv6", International Conference on Mobile Computing and Networking, pp27-37, 1996

[3]Wikipedia : Wake-on-Lan, http://en.wikipedia.org/wiki/Wake-on-LAN

[4]M. Romain, M. Jean-Frederiv, "A Mobility management Mechanism for Broadcasting in Unknown Mobile Ad hoc Networks", International Workshop on Modeling Analysis and Simulation of Wireless and Mobile Systems, pp242-245, 2005

[5]Jardosh, A. P. et al., "Green WLANs: On-Demand WLAN Infrastructures," Mobile Networks and Applications, Vol. 14, No. 6, pp.798-814, 2009.