능동형 인터넷 주소 자가변이와 OTP 를 활용한 서버 보안 시스템

고혁준*, 한성수**, 정창성***
*고려대학교 영상정보처리협동과정
**강원대학교 자유전공학부
***고려대학교 전기전자공학부
e-mail : doltwo@hanmail.net*, sshan1@kangwon.ac.kr**, csjeong@korea.ac.kr***

Server security system using active Internet address self-mutation and OTP

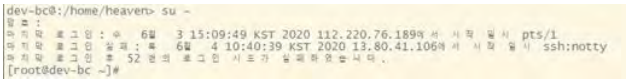
Hyug-Jun Ko*, Seong-Soo Han**, Chang-Sung Jeong***
*Dept. of Visual Information Processing, Korea University
**Division of Liberal Studies, Kangwon National University
***Dept. of Electrical Engineering, Korea University

요 약

4 차 산업혁명의 시대를 맞아 사물인터넷 및 5G 를 활용한 수많은 사물들이 인터넷을 기반으로 연결되고 있다. 또한 이러한 사물들을 관제 및 유지 보수하기 위해서 장비들에 보안 관제 시스템을 구축하고 모니터링을 하기 위한 많은 비용과 관리의 어려움을 겪고 있다. 만약, 장비들이 스스로 능동적인 방어를 하게 된다면 유지관리의 가장 큰 문제가 해결될 것이다. 이러한 능동적인 보안을 통해 보호대상 시스템의 다양한 특징들을 시간의 변화에 따라 역동적으로 변경하는 MTD(Moving Target Defense)기법들이 개발되고 있다. 본 논문에서는 네트워크 기반의 NMTD(Network-based MTD)를 이용하여 호스트 서버에 IP 와 PORT 로 접속하는 SSH 에 적용하여 능동적으로 보호하고, OTP 를 활용하여 사용자 식별을 통해 SSH 에 대한 내부자 접속에 대한 보안을 강화하는 시스템을 설계 및 구현하였다.

1. 서론

4 차 산업혁명의 시대를 맞아 인터넷을 기반으로 다양한 네트워크와 5G 를 활용한 수많은 사물들이 인터넷에 연결되는 사물인터넷의 활용이 급증하고 있다. 또한 이러한 사물들을 관제 및 유지 보수하기 위해서 장비들에 보안 관제 시스템을 구축하고 모니터링을 하기 위한 많은 비용과 관리의 어려움을 겪고 있다. 한편 공간적으로 구분된 무선 CCTV 와 웹캠 같은 경우 개별적인 방화벽 구축이 거의 불가능하기 때문에 보안 사고가 잦은 실정이다.



<그림 1. 리눅스 root 접속 정보>

이와 같은 보안 사고를 방지하기 위해서는 인터넷에 연결된 장비들이 스스로 능동적인 방어를 할 수 있도록 설계되어야 한다. 이렇게 설계된 시스템은 방화벽이 없어도 적절한 방어 기능을 수행할 수 있을 뿐만 아니라 사물 인터넷 및 서버의 해킹에 대한 예방과 DDoS 공격 등을 사전에 차단할 수 있다. 이런 능동적인 보안을 위해 보호 대상 시스템의 다양한 특징들을 시간의 변화에 따라 역동적으로 변경하는 MTD(Moving Target Defense)기법들이 개발되고 있다[1].

본 논문에서는 네트워크 기반의 NMTD(Network-based MTD)를 이용하여 해커의 침입을 사전에 예방 및 방어하는 보안 시스템을 제안한다. 서버의 IP 와 PORT 에 대한 스니핑(sniffing)과 프로빙(Probing)기술을 이용하여 정찰 행위를 무력화 시키기 위한 사이버 자가 방어 기술 및 인터넷 주소 변이 기술을 활용하여 호스트 서버에 접속하는 인터넷 IP 와 PORT 를 사용하는 SSH 에 적용한다. 이를 통해 해커의 탐지를 무력화 시킴으로써 침임을 방지하고 더 나아가 공용 접속 계정을 쓰는 내부자 접속에 대한 식별 및 인증된 사용자의 OTP 를 이용한 SSH 접속 허가를 구현 및 적용하여 해커 및 내부자의 무단 접속을 원천적으로 방어하기 위한 서버 보안 시스템을 설계 및 구현하고자 한다.

본 논문의 구성은 1 장에서 연구의 배경과 연구 내용에 대하여 제시하고, 2 장에서는 NMTD 기술에 대한 배경 이론을 정리한다. 3 장에서는 제안 시스템의 구현과 실험을 기술하며, 마지막으로 4 장에서 결론을

기술한다.

2. Related Works

NMTD 는 능동적 보안 기술로써 네트워크의 특징과 설정을 능동적으로 변경하며 사이버 공격에 대하여 사전에 방지할 수 있다. DYNAT(Dynamic Network Address Translation)[2]는 IPv4 기반의 NMTD 기술이며, 시간에 따라 암호 키 값(Keying Parameter)이 변화하는 기법이다. 목적지 IP 주소의 네트워크 주소 부분을 제외한 나머지 정보를 모두 암호화 및 복호화를 통해 서버의 주소와 PORT 번호의 노출을 막는다.

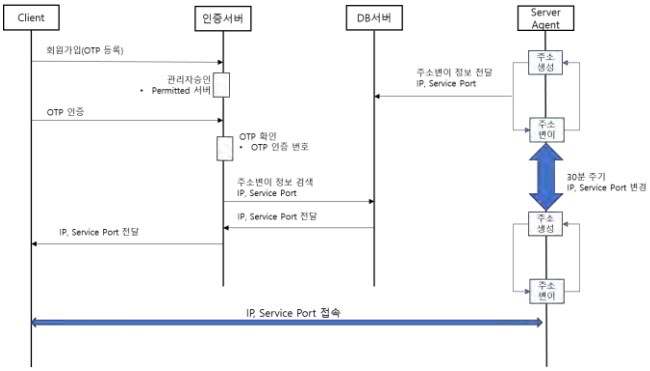
APOD(Applications that Participate in their Own Defense)[3]는 IP 주소와 Port 번호를 지속적으로 변경하여 공격자를 혼란에 빠뜨리는 방법이다. 패킷의 IP 주소와 PORT 번호를 각각 난수 발생기의 값들로 변경하여 패킷이 송신지 네트워크를 벗어날 때와 목적지 네트워크에 도착했을 때 동일한 난수 발생기를 활용해 원래 IP 주소와 PORT 번호로 복원한다.

NASR(Network Address Space Randomization)[4]은 서버의 IP 주소를 빈번하게 바꾸는 기법으로 이미 작성된 웜 히트리스트(Worm Hitlist)를 쓸모 없게 만든다. 동적 네트워크 주소 할당 서비스 인 DHCP(Dynamic Host Configuration Protocol) 서버로부터 호스트들이 일정 시간 간격마다 새로운 주소를 임대하게 하여 호스트의 IP 주소에 대한 변이(Mutation)를 구현하는 방법이다.

RHM (Random Host Mutation) [5]은 공격 패턴에 적응적으로 반응할 뿐만 아니라 주소 변환에 따른 오버헤드의 최소화를 위해 설계되었다. 오버헤드를 최소화하는 방법으로 RHM 은 LFM(Low Frequency Mutation)과 HFM(High Frequency Mutation)을 사용한다. LFM 은 호스트에 할당될 IP 주소의 범위를 바꾸는 변이이며, HFM 은 LFM 에 할당된 IP 주소의 범위에 속한 하나의 IP 주소 중 하나를 일정한 시간의 간격마다 호스트에 할당하는 방법이다.

3. 구현 및 실험

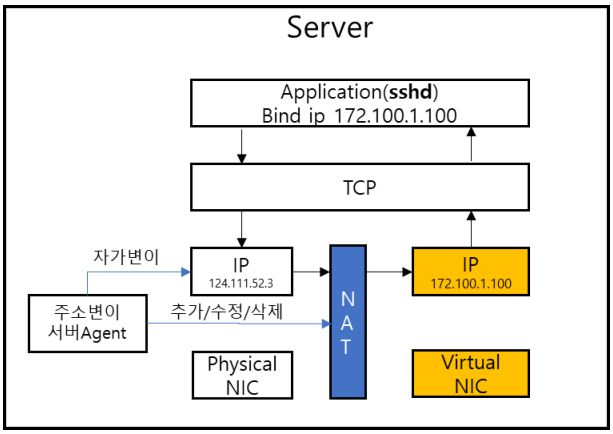
구현 시스템의 구성은 <그림 2>와 같다. 먼저 서버의 능동적인 인터넷 주소 및 PORT 변경을 위한 주소 변이와 서버의 변이 정책을 인증서버로 전송하는 서버 에이전트(Agent)와 변경된 IP 와 PORT 및 접속 사용자의 아이디와 패스워드를 관리하는 인증서버와 접속할 수 있는 IP 와 Port 를 알려주는 접속 클라이언트와 등록된 OTP(One Time Password)로 구성된다.



<그림 2. 능동형 인터넷 주소 자가변이와 OTP 를 활용한 서버 보안 시스템>

3.1 주소변이 서버 에이전트(Server Agent)

주소변이 서버 Agent 는 <그림 3>과 같이 IP 풀(Pool)안에 있는 IP 를 활용하여 접속용 IP 와 PORT 를 자가변이 시키면서 변경된 IP 와 PORT 를 정책서버로 SSL 통신을 이용하여 전송하고, 클라이언트에서 전송된 패킷을 SSH 용 가상 IP 와 PORT 로 전송될 수 있도록 NAT(Network Address Translation) 를 수정하여 SSH 데몬(Daemon)이 사설 IP 와 PORT 에서 수신된 패킷을 처리하게 한다.



<그림 3. 주소변이 서버 구성도>

서버에서 클라이언트로 패킷을 전달 할 때는 내부 인터페이스와 목적지 NAT 모듈은 관여되지 않으므로 정확한 접속 IP 와 PORT 만 있다면 정상적인 통신이 이루어 진다. 그러나, 주기적으로 접속 IP 와 PORT 가 바뀌게 되면 해당 통신은 끊어지게 되며 재 연결되지 않는다.

3.2 인증서버

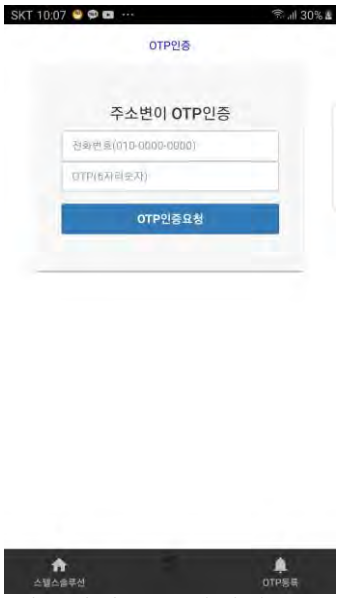
주소변이 서버 에이전트에서 SSL 로 전송되어온 변이된 주소와 PORT 를 데이터베이스에 저장하는 역할과 사용자 등록 및 허가 모듈 및 OTP 등록 모듈로 구성되어 있으며, 안드로이드 앱 또는 웹을 통해 접속하여 전화번호와 OTP 로 2 패스 인증을 완료 시 접

근 권한이 있는 서버의 현재 IP 와 PORT 를 알려준다.

3.3 사용자 인증 클라이언트

사용자 인증 클라이언트는 <그림 4>, <그림 5>와 같이 앱으로 구현된다. 설치된 인증 앱을 통하여 읽어들인 핸드폰의 구글 어카운드 계정 이메일과 핸드폰 번호를 이용하여 생성된 QR 코드를 이용하며, 앱 OTP(예, 구글 OTP) 등에 등록하여 해당 앱 OTP 를 사용할 수 있고 별도의 H/W OTP 를 사용할 필요 없이 구동이 가능하다.

<그림 4. 사용자인증 클라이언트-OTP 등록>



<그림 5. 사용자인증 클라이언트-OTP 인증>

4. 결론

본 논문은 네트워크 기반의 NMTD(Network-based MTD)를 이용하여 해커의 침입을 방어하는 기술로서 서버의 IP 와 PORT 에 대한 스니핑(sniffing)기술과 프로빙(Probing)기술을 이용한 정찰행위를 무력화 시키기 위하여 인터넷 주소 자가변이 데몬(Daemon)을 활용하여 호스트 서버에 접속하는 인터넷 IP 와 PORT 를 사용하는 SSH 에 적용하여 해커의 탐지를 무력화 시킴으로 써 해킹을 차단하고, 허가 받지 않은 내부자 접속에 대한 보안 대책으로서 공용으로 사용하는 SSH 계정에 대한 분별을 하고자 인증된 사용자의 스마트폰의 구글 계정과 전화번호 및 별도의 OTP 를 활용하여 SSH 의 IP 와 PORT 를 조회하는 최종 사용자의 접속 로그를 남김으로써 공용 계정에 대한 신원을 분별하여 무단 접속을 예방하는 효과를 줄 수 있다. 또한 IP 변경이 특정한 간격으로 이루어 짐에 따라 장시간 접속에 따른 차단 효과가 있으므로 자리를 비운 사이 또 다른 침입을 예방할 수 있다.

또한, 구현 시스템의 특징과 효과로서 방화벽을 통한 해킹 방지로는 할 수 없는 내부 접속자에 대한 식별과 예방이 가능하다는 것이다.

향후 구현 시스템에 블록체인 기술을 접목하여 보다 향상된 보안 시스템을 설계 및 구현하고자 한다.

참고문헌

[1] Kyungmin Park, “Network Address Mutation for Proactive Cyber Security,” Ph.D. Thesis, Chungnam National University Daejeon, Korea, 2018.

[2] D. Kewley, R. Fink, J. Lowry and M. Dean, “Dynamic Approaches to Thwart Adversary Intelligence Gathering,” Proceedings of the DARPA Information Survivability Conference and Exposition, pp. 176-185, August 2001.

[3] M. Atighetchi, P. Pal, F. Webber and C. Hones, “Adaptive Use of Network-Centric Mechanisms in Cyber-Defense,” Proceedings of the sixth IEEE International Symposium on Object-Oriented Real-Time Distributed Computing, pp. 183-192, 2003.

[4] S. Antonatos, P. Akritidis, E. P. Markatos, K. G. Anagnostakis, “Defending against Histlist Worms using Network Address Space Randomization,” Computer Networks, vol.51, no.12, pp.3471-3490. August 2007

[5] J. H. Jafarian, E. Al-Shaer and Q. Duan, “An Effective Address Mutation Approach for Distructing Reconnaissance Attacks," IEEE Transactions on Information Forensics, vol.10, no.12, pp. 2562-2577, August 2015.