JKSCI

한국컴퓨터정보학회논문지
Journal of The Korea Society of Computer and Information
Vol. 26 No. 6, pp. 9-17, June 2021
https://doi.org/10.9708/jksci.2021.26.06.009

Implementation of a security system using the MITM attack technique in reverse

Young Woo Rim*, Jung Jang Kwon*

*M.Sc. Student, Dept. of Computer Engineering, Kyungsung University, Pusan, Korea
*Professor, Dept. of Computer Engineering, Kyungsung University, Pusan, Korea

[Abstract]

In this paper, we propose a reversely using the “Man In The Middle Attack” attack technique as a way to introduce network security without changing the physical structure and configuration of the existing network, a Virtual Network Overlay is formed with only a single Ethernet Interface. Implementing In-line mode to protect the network from external attacks, we propose an integrated control method through a micro network security sensor and cloud service. As a result of the experiment, it was possible to implement a logical In-line mode by forming a Virtual Network Overlay with only a single Ethernet Interface, and to implement Network IDS/IPS, Anti-Virus, Network Access Control, Firewall, etc.,. It was possible to perform integrated monitor and control in the service. The proposed system in this paper is helpful for small and medium-sized enterprises that expect high-performance network security at low cost, and can provide a network security environment with safety and reliability in the field of IoT and embedded systems.

▸ **Key words**: Network protection, MITM Attack, ARP Poisoning, Virual network overlay, IoT Cloud

[요 약]

본 논문에서는 기존 네트워크의 물리적인 구조 및 구성을 변경하지 않고 네트워크 보안을 도입할 수 있는 방안으로 “Man In The Middle Attack” 공격 기법을 역이용함으로, Single Ethernet Interface만으로 가상 네트워크 오버레이를 형성하여 논리적인 In-line Mode를 구현하여 외부의 공격으로부터 네트워크를 보호하는 초소형 네트워크 보안 센서와 클라우드서비스를 통한 통합관제 방안을 제안한다. 실험 결과, Single Ethernet Interface만으로 가상 네트워크 오버레이를 형성하여 논리적인 In-line Mode를 구현할 수 있었으며, Network IDS/IPS, Anti-Virus, Network Access Control, Firewall 등을 구현할 수 있었고, 초소형 네트워크보안센서를 클라우드서비스에서 통합관제하는 것이 가능했다. 본 논문의 제안시스템으로 저비용으로 고성능의 네트워크 보안을 기대하는 중소기업에 도움이 되고 또한, IoT 및 Embedded System 분야에 안전·신뢰성을 갖춘 네트워크 보안환경을 제공할 수 있다.

▸ **주제어**: 네트워크 보호, MITM 공격, ARP 포이즈닝, 가상 네트워크 오버레이, IoT 클라우드

• First Author: Young Woo Rim, Corresponding Author: Jung Jang Kwon
*Young Woo Rim (xsapiens@naver.com), Dept. of Computer Engineering, Kyungsung University
*Jung Jang Kwon (jjkwon@ks.ac.kr), Dept. of Computer Engineering, Kyungsung University
• Received: 2021. 04. 05, Revised: 2021. 06. 07, Accepted: 2021. 06. 07.
• This paper has extended the paper titled “Implementation of a security system using the MITM attack technique in reverse” of the Proceedings of 2021 Winter KSCI

http://www.ksci.re.kr pISSN:1598-849X | eISSN:2383-9945

I. Introduction

네트워크 보안은 악의적인 공격으로부터 네트워크 구성 설비 및 네트워크에 참여한 장비들을 보호하고, 내부의 정보가 의도치 않게 도난·유출되는 것을 방지하여 안전한 네트워킹과 인터넷을 보장하는 것에 그 목적이 있다.

네트워크 보안장비는 일반적으로 최소 두 개 이상의 Ethernet Interface를 탑재하고 있으며, 외부로 연결되는 회선과 내부로 연결되는 회선을 각각 연결함으로 통신경로 선상에 위치하는 이른바 In-line Mode로 설치하고 In-Bound/Out-Bound 트래픽이 네트워크 보안장비를 경유하게 하여 그 트래픽을 검사하여 보안위협요소의 유무를 판별하고 그 결과에 따른 합당한 Verdict에 근거하여 각 트래픽의 허용 또는 차단을 수행함으로 안전한 통신을 보장한다.

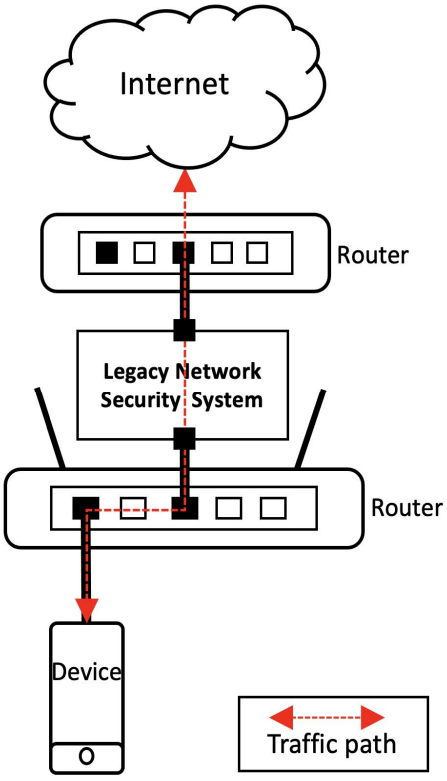


Fig. 1. Physical Position and Traffic Path of Legacy Network Security System

기존의 방식으로 네트워크보안을 구축하기 위해서는 네트워크의 구성을 변경하여 이중네트워크를 구성해야 하며, 네트워크의 전문 지식이 필요하고 이로 인해 도입비용이 높은 문제점을 감수해야 한다.

네트워크를 보호하기 위해 이미 많은 연구와 방안이 제시되었으며, NAC(Network Access Control)와 UTM(Unified Threat Management)이 대표사례라 할 수 있다.

NAC는 네트워크에 참여한 장비들과 Router에 ARP Poisoning을 수행하여 동 네트워크의 패킷들이 해당 장비를 경유하게 유도하고 패킷의 Source와 Destination을 정의된 임의의 정책에 근거하여 접근을 제어하는 방안이 제안되었고, 보다 섬세한 접근통제를 위해 각 장비에 에이전트를 설치하여 정책서버로부터 제어를 받아 통제하는 방법들이 제시되었으나, 각 OS 및 OS의 버전별 호환성을 가진 에이전트를 개발·유지·보수해야하는 문제가 존재한다[1].

UTM은 Firewall, Network IDS/IPS, Anti-Virus등의 기능이 하나로 통합하여, 네트워크를 위협하는 여러 가지 형태의 위협으로부터 네트워크를 보호하는 방안이 제안되었다. 그러나, 네트워크에서 Gateway의 역할을 수행해야 하므로 도입을 위해서는 기존의 네트워크구조의 변경이 불가피하다[2].

이에 본 논문에서는 네트워크의 전문지식이 필요하지 않고, 네트워크의 구성이나 구조를 변경할 필요가 없는 MITM 공격기법을 역이용한 가상 네트워크 오버레이 기반의 저전력·저예산·고성능의 네트워크보안센서와 클라우드 서비스를 통한 통합보안관제시스템을 제안한다.

II. Proposed System

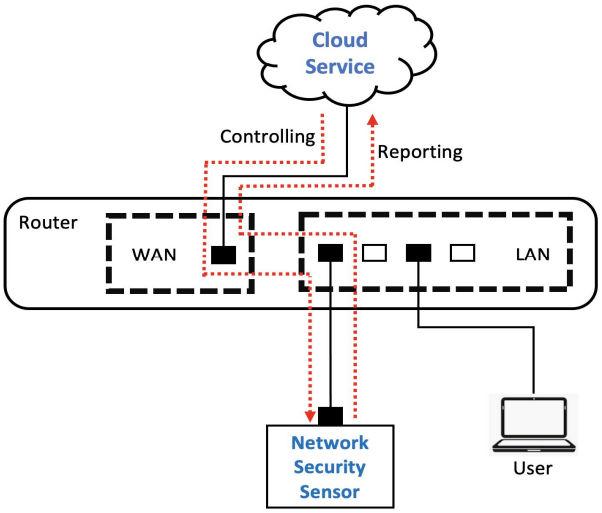


Fig. 2. Network Security Sensor and Cloud Service of Proposed System

본 논문에서 제안하는 네트워크 보안시스템은 네트워크 보안센서와 클라우드서비스로 구성된다.

제안시스템의 네트워크보안센서는 보호대상 네트워크에 직접 참여하여 네트워크를 보호하고 클라우드서비스를 통해 제어받으며 보호대상 네트워크의 정보와 보안이벤트 등을 클라우드서비스에 전송한다.

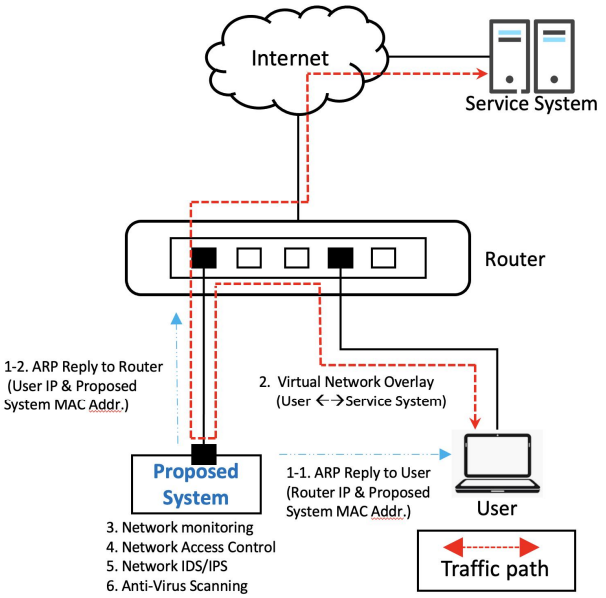


Fig. 3. Physical Position of Network Security Sensor and Traffic Path of Proposed System

제안시스템의 네트워크보안센서는 기존의 네트워크보안장비와 달리, 하나의 Ethernet Interface만을 탑재한 SBC(Single Board Computer)에 Embedded LINUX를 기반으로 MITM(Man In The Middle) 공격방식을 역이용하여 가상 네트워크 오버레이를 형성하고, 그 상위 계층에 보안소프트웨어를 탑재한다. 제안시스템의 네트워크보안센서는 이 방식으로 기존의 네트워크구성을 변경하지 않고, 구축하는 동안 외부와의 통신연결의 끊어짐이 없이 구축이 가능한 네트워크 보안 시스템이다.

제안시스템의 네트워크보안센서는 물리적으로 In-line Mode가 아닌, 네트워크에 참여한 기타 장비들과 동등한 위치에 연결되어 보호대상 네트워크에 직접 참여해 가상 네트워크 오버레이를 형성함으로써 보호대상 네트워크의 모든 In-Bound/Out-Bound 트래픽이 제안시스템의 네트워크 보안센서를 경유하도록 유도하여 논리적으로 In-line Mode에 위치하게 된다.

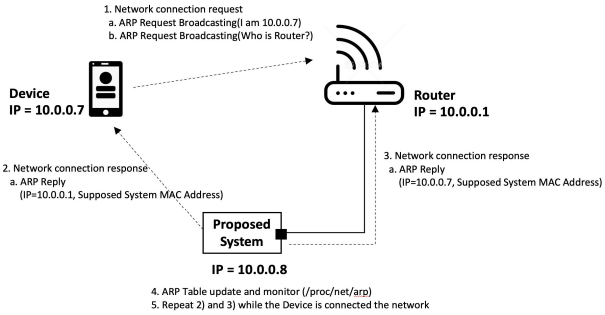


Fig. 4. Virtual Network Overlay

임의의 장비가 네트워크에 참여하려 시도할 때, 자신의 MAC Address 및 IP Address를 공포하고 어느 장비가 동 네트워크의 Router인지 질의하는 ARP Request Broadcasting(1-a, 1-b)을 수행한다. 이 때, Router가 해당 장비에게 ARP Reply를 수행하기 전에 제안시스템의 네트워크보안센서가 Router의 IP Address와 제안시스템의 네트워크보안센서의 MAC Address를 조합하여 생성한 ARP 패킷을 해당 장비에게 전송함으로써(2-a) 해당 장비로 하여금 제안시스템의 네트워크보안센서를 동 네트워크의 Router로 인지하게 한다. 이와 동시에 해당 장비의 IP Address와 제안시스템의 네트워크보안센서의 MAC Address를 조합하여 생성한 ARP 패킷을 Router에게 전송함으로써(3-a) Router로 하여금 제안시스템의 네트워크보안센서를 해당 장비로 인지하게 한다. 이를 통해 해당 장비가 외부와 통신하는 모든 In-Bound/Out-Bound 패킷을 제안시스템의 네트워크보안센서로 유도하고, 제안시스템의 네트워크보안센서는 해당 패킷을 원래의 목적지로 다시 Forwarding함으로써 가상 네트워크 오버레이를 형성한다.

제안시스템의 네트워크보안센서는 해당 장비가 네트워크에 참여하고 있는 동안 해당 장비와 Router에게 위와 같은 ARP패킷을 주기적으로 반복하여 전송함으로써 가상 네트워크 오버레이를 유지하도록 한다.

해당 장비가 네트워크에서 탈퇴하면 제안시스템의 네트워크보안센서는 해당 장비에게 ARP패킷을 더 이상 전송하지 않음과 동시에 Router에게도 해당 장비와 관련된 ARP패킷을 더 이상 전송하지 않음으로 해당 장비에 대한 가상 네트워크 오버레이를 종료한다.

Table 1. Features of Proposed System

Participating and collecting network information and host information
Drive all traffic through supposed system with virtual network overlay
Network IPS
Firewall
DNS Cache DB
Service Access Control
Internet Access Control
Anti-Virus
Monitoring with Cloud Server
Controlling with Cloud Server

제안시스템의 네트워크보안센서는 가상 네트워크 오버레이의 상위 계층에 Firewall, Network IPS, Anti-Virus, DNS Cache DB, Service Access Control, Internet Access Control등의 기능들을 탑재하여 네트워크 보안을 구현하고, 클라우드서버는 네트워크보안센서의 모니터링(네트워크보안센서의 상태, 보호 대상 네트워크의 참여 장비들의 상태, 보안 이벤트 로그 및 처리 로그 등)과 제어기능(보안 정책 하달, 네트워크 접근 통제 정책 하달, IPS 및 Anti-Virus의 Signature Update, Firmware Update)을 구현한다.

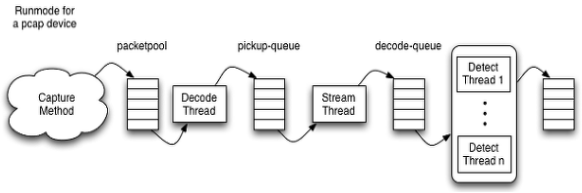


Fig. 5. Network IPS Work-Flow

제안시스템의 네트워크보안센서에 NFQueue를 생성하고, 가상 네트워크 오버레이를 통해 유도된 모든 패킷을 원래의 목적지(해당 장비 또는 Router)로 Forwarding하기 전에 그 패킷을 NFQueue에 먼저 Forwarding하고, NFQueue에 전달된 패킷을 분석하여 보안 위협 요소의 유무를 판단하고 그에 합당한 Verdict를 내리고, 그 Verdict에 근거하여 해당 패킷을 원래의 목적지로 Forwarding하거나 또는 Drop하여 구체적인 Network IPS와 Anti-Virus를 구현한다.

또한, 제안시스템에서 미리 정의된 Rule에 근거하여 In-Bound 및 Out-Bound패킷을 차단하여 Firewall기능을 구현하고, 보다 용이한 Firewall정책관리를 위해 Domain Name을 근거로 패킷을 허용 또는 차단하도록 제안시스템 Local에 DNS Cache를 구축·연동한다.

III. Experiment & Result

1. Function implementation of Proposed System

Table 2. Specification of Proposed System

Item	Value
CPU	AllWinner H6
RAM	1GB
Ethernet	1Gbps
Storage	16GB CFCard
OS	Embedded LINUX

Fig. 6. Inside of Network Security Sensor of Supposed system

Fig. 7. Front of Network Security Sensor of Supposed system

제안시스템의 네트워크보안센서의 전력소모를 최소화하기 위해 Raspberry Pi와 같은 초소형 SBC(DC5v/3A)에 Embedded LINUX를 탑재하고 네트워크설정은 Dynamic 또는 Static IP Address로 설정한 후 네트워크에 참여한 기타 장비들과 동등한 Layer에 연결하여 보호대상 네트워크에 직접 참여한다. 또한, 설정된 네트워크정보를 근거로 주기적으로 NMAP을 구동하여 네트워크를 Scan한 후 제안시스템의 네트워크보안센서Local의 ARP Table을 참조하여 동 네트워크에 참여한 모든 장비 및 Router의 정보와 네트워크 참여 상태를 취득 및 정형화하여 제안시스템의 네트워크보안센서Local DB에 저장하였다. 이러한 DB를 구축하기 위해 제안시스템의 네트워크보안센서에서 RDBMS인 MySQL을 사용하였을 때 제안시스템의 성능이 저하되는 것을 관찰할 수 있었으며, REDIS를 응용하여 Key-Value형태의 DB를 취하였을 때 성능저하문제가 해소되는 것을 확인할 수 있었다.

네트워크에 갓 참여한 장비의 경우 다음 네트워크 Scan주기가 돌아오기 전까지는 장비목록에 등록되지 않아 보호받지 못하는 Gap이 발생하는 문제가 있었는데, 이 문제는 LibPcap을 응용한 데몬으로 BOOTP패킷을 탐지 및 분석하여 새로운 장비의 네트워크 참여 시도를 탐지하

고 그 패킷을 분석하여, 해당 장비의 IP Address 및 MAC Address와 Host Name등의 정보를 취득해 보호 대상 네트워크에 참여한 장비목록에 실시간 반영하도록 함으로써 네트워크에 새로 참여하는 장비로 하여금 제안시스템의 기능적 혜택을 받지 못하는 시간대를 없앨 수 있었다.

IPTables를 이용하여 유도된 패킷을 인라인 모드(In-line Mode)로 네트워크 환경을 구성하였는데 이 때, 유도된 패킷을 NFQueue로 Forwarding 되게 설정하였다.

이렇게 Netfilter를 구성한 이유는 NFQueue의 내용을 Scan해 보안위협요소의 유무를 판단하고 합당한 Verdict를 내리기 위함이었으며, 그 Verdict에 근거하여 패킷을 Forwarding 또는 Drop함으로써 패킷의 보안위협요소유무에 따른 제어를 구현할 수 있었다[3].

제안시스템의 네트워크보안센서에 Multicore와 Multithread를 지원하는 오픈소스 Network IPS인 Suricata를 구축하였다. Suricata는 [Packet capture -> Decode -> Stream -> Detect]의 Work-flow를 가지며 이러한 과정을 Multithread로 처리한다는 것에 착안하여, 제안시스템의 네트워크보안센서의 패킷처리성능을 향상시키기 위해 여러 개의 NFQueue를 생성한 결과 Snort에 비해 빠른 처리성능을 보장하였으며, 하드웨어의 성능을 고려하여 본 실험에서는 네 개(0,1,2,3)의 NFQueue를 생성하고 Suricata의 옵션을 설정하여 NFQueue를 연동하고 그 내용을 검사하여 합당한 Verdic를 내릴 수 있도록 하였다[4,5,6].

이로써, 제안시스템의 네트워크보안센서가 참여한 네트워크에서 가상 네트워크 오버레이를 형성하여 네트워크의 모든 In-Bound 및 Out-Bound 트래픽을 제안시스템의 네트워크보안센서의 NFQueue를 경유하도록 유도하고 Suricata를 통해 NFQueue의 패킷을 IPS Rule로 검사하여 보안 위협 요소 유무에 따른 Suricata의 Verdict에 근거하여 모든 패킷을 Forwarding 또는 Drop하여 Network IPS를 구현할 수 있었다.

제안시스템의 네트워크보안센서에 Anti-Virus를 구현하기 위해 ClamAV를 구동하였을 때 SBC의 제한된 리소스로 인해 그 성능이 저하되는 것을 관찰할 수 있었으며, 이를 해결하기 위해 ClamAV을 구동하지 않고 ClamAV 패키지에 포함된 “sigtool”을 이용해 ClamAV Signature DB로부터 Hash값을 구하여 Suricata의 Custom Rule에 Drop Rule로 적용하여 Anti-Virus를 구현하였을 때 성능저하 문제를 극복할 수 있었다.

네트워크에 참여한 장비의 불필요한 인터넷사용을 차단하기 위해 각 서비스별로 차단하는 기능을 구현할 필요가 있는데, 이는 Suricata의 Custom Rule을 응용하여 DNS 질의·응답패킷과 TLS의 SNI를 근거로 제안시스템의 네트워크보안센서에서 동영상 스트리밍 서비스, 인터넷 메시징 서비스, 소셜미디어 서비스등을 각 장비별로 허용 또는 차단할 수 있었다[6,7,8].

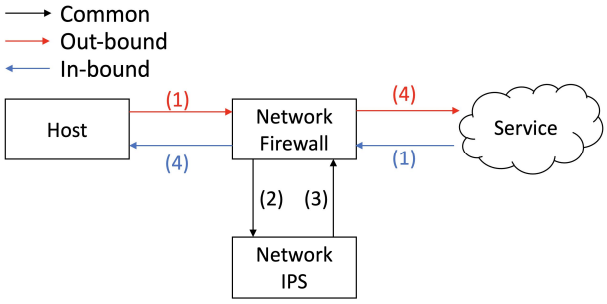


Fig. 8. Logical Position of firewall

제안시스템의 네트워크보안센서에서 IPTables를 응용하여 In-Bound 및 Out-Bound패킷과 Domain Name을 근거로 그 패킷을 차단하는 Firewall을 구현할 수 있었으며, IPTables Rule로 Drop될 패킷이 Suricata에서 검사된 후 IPTables Rule에 의해 Drop될 경우 Suricata가 불필요한 작업을 수행함으로 인해 그 성능이 저하되는 것을 피하기 위해 IPTables Rule의 우선순위를 조정하여 NFQueue로 패킷이 Forwarding되기 전에 IPTables Rule로 패킷을 제어하여 Firewall의 기능을 먼저 수행함으로써 Network IPS가 불필요한 패킷을 분석하는 리소스의 낭비를 줄일 수 있었다. 이는 IPTables에 Rule을 추가할 때 “ADD”명령이 아닌 “INSERT”명령을 수행함으로써 Rule의 우선순위를 조정하는 별도의 작업을 피할 수 있었다.

Firewall기능 중 Domain Name을 근거로 패킷을 차단하기 위해 IPTables Rule을 설정하여 차단대상 Domain Name을 포함한 패킷을 차단하였을 때 Rule이 많아질수록 성능이 저하됨이 확인되었고, 차단대상이 아닌 패킷에 차단대상 Domain Name과 동일한 String을 포함한 패킷이 차단되는 문제점이 확인되었다.

이에, 제안시스템의 네트워크보안센서에서 자체 DNS Cache DB를 구축하여 실시간으로 갱신하고 그 DB를 IPSET에 실시간 반영하도록 하여 IPSET과 IPTables Rule을 연동함으로써 IPTalbes Rule이 많아져 성능이 저하되는 문제와 차단 대상 Domain Name을 포함한 패킷을 오탐하여 Drop하는 문제를 해결할 수 있었다. 네트워크에 참여한 장비들이 Domain Name을 이용하여 외부 서비스에 접속하기 위해서는 DNS질의·응답이 선행되는 것에 착안하여 Suricata를 응용하여 DNS질의·응답내용을 정형화 하여 Event-Log를 발생시키고 그 Log를 분석하여 각 Domain

Name에 해당하는 IP Address 목록을 DB화함과 동시에 각 Domain Name에 해당하는 IPSET을 생성하고 갱신하여 Domain Name과 Sub-Domain Name을 모두 차단하는 Firewall을 구현할 수 있음이 확인되었다[9].

제안시스템의 네트워크보안센서가 보유하고 있는 각 장비들의 MAC Address를 근거로 특정 장비에 대해 TCP와 UDP를 차단하여 해당 장비가 인터넷에 접근하는 것을 통제하려 하였으나 일시적으로 인터넷사용이 차단되었다가 다시 복구되는 현상을 관찰할 수 있었다. 이는 IPTables Rule에 의해 차단되어 유실된 패킷을 ICMP에 의해 복구됨으로 인해 발생하는 문제로 확인되었으며, IPTables를 이용해 해당 장비 Source 또는 Destination에 포함한 패킷들에 대해 TCP와 UDP를 DROP하고 ICMP를 REJECT하는 Rule을 적용했을 때 해당 장비의 인터넷사용을 완벽히 차단할 수 있음이 확인되었다[10].

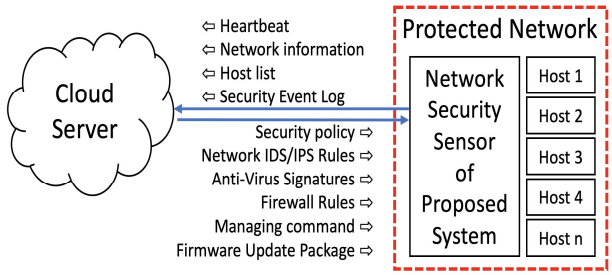


Fig. 9. Communication of Network Security Sensor and Cloud Server

제안시스템의 네트워크보안센서는 제한된 리소스를 최대한 확보하기 위해, 기능유지를 위한 최소의 정보만을 Local에 저장하고 보안 이벤트 로그 등 예측할 수 없으나 큰 저장 공간을 요하는 데이터는 클라우드서버에 전송하여 보관한다.

제안시스템의 네트워크보안센서는 클라우드서버와 HTTPS를 통해 정보(Heartbeat, 네트워크정보, 네트워크 참여장비목록, 보안이벤트로그 등)를 전송하고 명령(보안정책, 방화벽정책, 기타 설정정보)과 DB(IDS/IPS Rules, Anti-Virus Signatures 등)를 전달받아 Local에 적용한다.

제안시스템의 네트워크보안센서는 자체보호를 위해 어떠한 통신포트도 열려있지 않으며, 클라우드서버와의 통신은 네트워크보안센서가 능동적으로 클라우드서버에 접속하는 HTTPS Client의 입장을 취한다.

제안시스템의 클라우드서버에서는 허가된 클라이언트의 접속만을 허가하기 위해 허가된 네트워크보안센서의 MAC-Address를 사전에 RDB에 등록하고 White-List를 구성하여 운영한다.

제안시스템의 네트워크보안센서는 클라우드서버와의 통신에서 자신의 MAC-Address를 Payload에 항상 포함하여 전송하고, 클라우드서버는 그 MAC-Address를 근거로 DB에서 해당 네트워크보안센서의 정보를 조회 또는 갱신 등을 수행한다.

제안시스템의 클라우드서버에는 HTTPD와 RDBMS 그리고 NoSQL-DB를 구축하여 네트워크보안센서로부터 전달받은 정보(네트워크보안센서의 하드웨어 정보 및 네트워크 정보, 보호 대상 장비들의 정보, 보안 이벤트 로그, 보안 정책 정보 등)를 RDB에 저장한다. 특히, 보안 이벤트 로그와 같은 수시로 발생하는 정보들을 RDB에 바로 저장하였을 때 그 접속빈도가 높은 문제로 RDBMS의 성능 저하에 영향을 끼치는 것이 관찰되었으며, 이러한 자료들은 먼저 NoSQL-DB에 저장한 후 클라우드서버에서 별도의 데몬을 통해 주기적으로 데이터를 RDB로 이전함으로써 성능 저하 문제를 극복할 수 있었다.

본 실험의 클라우드서버는 LINUX기반에 Apache와 MySQL 그리고 REDIS를 사용하였다.

Table 3. Function List via UI on Cloud Server of Proposed System

Function	Details
Network Security Sensor Manager	• Monitoring • Add New Network Security Sensor • Delete Network Security Sensor • Change Network Security Sensor • Firmware Update
Host Manager for Protected Network	• Monitoring • Network Access Control
Security Event Log Manager	• IPS Log • Anti-Virus Log • Firewall Log
Security Policy Manager	• IPS Policy • Anti-Virus Policy • Firewall Policy

제안시스템의 클라우드서버에 Web기반의 UI를 구축하여 제안시스템을 모니터링 및 관리할 수 있도록 [Table 3]과 같은 기능과 기타 기능들을 구현한다.

이 기능들은 크게 모니터링을 위한 기능들과 제어를 위한 기능들로 구분할 수 있으며 특히, 제어를 위한 기능을 통해 변경된 정보는 네트워크보안센서에 전달되어 적용되어야 한다. 이는 네트워크보안센서로부터 온 Heartbeat의 Response Payload에 수행할 제어명령이 있음을 알 수 있는 데이터를 포함하여 전달하고, 네트워크보안센서는 이를 근거로 클라우드서버에 접속하여 수행해야할 제어정보들을 내려 받아 Local 또는 보호 대상 네트워크에 적용하고, 각

제어명령의 수행결과를 클라우드서버에 보고하여 클라우드서버가 그 수행결과를 알 수 있게 한다. 네트워크보안센서에서 정상 수행된 제어명령은 수행할 제어명령목록에서 삭제되고, 비정상 수행된 제어명령은 다음 Heartbeat를 통해 다시 하달될 수 있도록 하며, 비정상 수행 횟수를 카운팅하여 기능이상여부를 더 상세히 모니터링 할 수 있다.

제어명령들은 사전에 코드로 정의하여 네트워크보안센서와 클라우드서버간에 공유함으로써 제어를 위한 실 명령어를 전달하지 않고 각 명령에 해당하는 코드만 전달함으로써 통신데이터량을 줄임과 동시에 통신의 보안성을 향상할 수 있다.

Table 4. Example of Control Protocol

Major Code	Command	Minor Code	Command
0010	Host Managing	0010	Change host name
		020	Change managed status
		0030	Delete host
		0040	Set BAN time
0020	Firewall Rule Managing	0010	Add Rule
		0020	Delete Rule
		0030	Edit Rule
0030	Sensor Managing	0010	Reset
		0020	Reboot
		0030	Shutdown
		0040	Set Heartbeat Cycle
		0050	Set Network Config.
0040	IPS Managing	0010	Turn On
		0020	Turn Off
		0030	Update Rules
		0040	Reload Rules
0050	Remote Technical Support	0010	Open Reverse SSH Port
		0020	Close Reverse SSH Port
		0030	Upload Analysis Data

제어명령코드는 크게 Major Code와 Minor Code로 구분하여 제어규약을 보다 세밀하게 체계화 할 수 있다.

Table 5. Example of Control Command Format

```
{
    "MAJOR": "0030"
  , "MINOR": "0040"
  , "VAL": 5
  , "DURATION": 600
}
```

각 명령들의 특성에 따라 명령인자들을 첨부할 수 있고, JSON등의 포맷을 적용하여 보다 유연성 있는 명령체계를 구현할 수 있다. 가령, [Table 5]와 같이 JSON포멧의 명령전달을 통해 600초 동안 네트워크보안센서의 Heartbeat 주기를 5초 간격으로 유지하고, 600초 후 그 주기를 다시 기본 값으로 되돌릴 수 있다.

Table 6. Sample definition and measurement method

Key Performance Indicators	Sample Definition	Measurement Sample (n ≥ 5)	Method of Measurement (Specification, Environment, Calculation of Result, etc,...)
Number of IDS/IPS Signature	ET Open Rules	5	Load 10,000 of Suricata ET Open Rules
Number of Anti-Virus Signature	Clam AV Virus DB	5	Load over 300,000 of ClamAV Virus DB
Network Performance	Network performance with Firewall + IPS + AV	350 Mbps	Enable Firewall, IPS(Intrusion Prevention System) and AV(Anti-Virus)
※ Less than 5 Samples (n<5)			

제안시스템의 네트워크보안센서에 활성화한 기능에 따라 네트워크처리 성능에서 차이를 보였는데, Firewall만 가동하였을 때 600Mbps를 보장하였고, Firewall과 Network IDP를 동시에 가동하였을 때 500Mbps를 보장하였으며, Firewall과 Network IDP와 Anti-Virus를 동시에 가동하였을 때 350Mbps를 보장하는 높은 성능을 확인할 수 있었다.

특히, 상용화되어있는 기업용 침입 탐지 및 방지 시스템(IDP: Intrusion Detection & Prevention)에 탑재된 보안규칙이 3~4천 개 수준인데 비해 본 논문의 실험에서는 10,000개 이상의 보안규칙을 탑재하였으며, 상용화되어있는 기업용 Anti-Virus시스템이 1만개 수준의 Virus Signature를 탑재하고 있는데 반해 본 논문의 실험에서는 30만개 이상의 Virus Signature를 탑재하였음에도 불구하고 네트워크 트래픽 처리 속도 면에서 우수한 성능을 보였다.

IV. Conclusions

본 논문에서 제안하는 시스템은 실험을 통하여, 하나의 Ethernet Interface만으로 MITM 공격방식을 역이용하여 가상 네트워크 오버레이를 구현함으로써 네트워크의 물리적인 구조변경이 없이 네트워크상에서 Router의 역할을 담당하며 네트워크 트래픽을 논리적으로 유도하여 Network IDS/IPS, Anti-Vrisus, Firewall 등의 기능으로 그 패킷을 제어하고 잠재적인 보안 위협 요소를 제거할 수 있음이 확인되었다. 또한, 기존의 Inline Mode의 네트워크보안장비와 달리 네트워크보안장비 자체의 장애로 인한 네트워크 중단현상을 피할 수 있다.

Table 7. Comparison of Proposed System and Commercial Products

Key Function and Performance	Proposed System	Sophos SG-135	ForiNet FG-200E	Ahnlab IPX-2000A
Size(cm x cm)	Small (Same with Credit Card)	1U (84 x 84)	1U (84 x 84)	1U (84 x 84)
Network Access Control (Firewall)	O	O	O	O
Network IDS and IPS	O	O	O	O
Virtual Network Overlay	O	X	X	X
Changing Network Structure	No Change	Complicated	Complicated	Complicated
Response of Failure	No Side Effect on Network	Network Down	Network Down	Network Down
Introduction Cost	Less than $200	Over than $10,000	Over than $10,000	Over than $10,000
Annual Contents Renewal Cost	X	Over than $1,000	Over than $1,000	Over than $1,000

네트워크보안을 위해 네트워크보안센서와 클라우드서버의 조합을 구성하고, 대량의 정보는 클라우드서버에 저장함으로써 네트워크보안센서의 스토리지를 줄일 수 있었고, 보안 이벤트 로그와 환경설정 및 보안정책들을 클라우드서버에 저장함으로써 네트워크보안센서의 설치 및 교체 등의 행위를 위해 네트워크의 전문지식이 없이 저예산·저전력·고성능의 네트워크보안을 구현할 수 있음이 확인되었다.

본 논문에서 제안하는 시스템은 네트워크보안장비의 높은 비용부담, 네트워크 전문인력 보유의 부담, 기존의 네트워크의 구조변경이 불가피함 등의 문제로 네트워크 보안을 도입하지 못하고 잠재적 보안위협에 노출되어있는 중소기업과 IoT장비 및 Embedded System 보호에 도움이 될 것으로 기대한다.

본 논문에서 제안하는 시스템의 성능을 보다 더 향상시키기 위해서는 네트워크보안센서와 클라우드서버 간의 통신 데이터 량 축소에 관현 연구가 더 수행되어야 할 것이다.

REFERENCES

[1] Rami Radwan Omar, Tawfig M. Abdelaziz. A Comparative Study of Network Access Control and Software-Defined Perimeter. ICEMIS'20: Proceedings of the 6th International Conference on Engineering & MIS 2020 September, pp.1-5 2020 , DOI:10.1145/3410352.3410754

[2] Saqib Ali; Maitham H. Al Lawati; Syed J. Naqvi. Unified Threat Management System Approach for Securing SME's Network Infrastructure. ICEBE '12: Proceedings of the 2012 IEEE Ninth International Conference on e-Business EngineeringSeptember, pp.170-176 2012, DOI:10.1109/ICEBE.2012.36

[3] Mariano Graziano, Corrado Leita, Davide Balzarotti. Towards network containment in malware analysis systems. ACSAC '12: Proceedings of the 28th Annual Computer Security Applications ConferenceDecember, pp.339-348 2012, DOI:10.1145/2420950.2421000

[4] SuricataUserGuide, Dec.04.2020, *https://suricata.readthedocs.io*

[5] Myeong Ki Jeong, Seongjin Ahn, Won Hyung Park. A Comparative Study on Function and Performance of Snort and Suricat, Journal of Korea Society of Digital Industry and Information Management Volume 12 Issue 1 pp.1-12 2016, DOI:10.17662/ksdim.2016.12.1.089

[6] BillKarakostas. A DNS Architecture for the Internet of Things: A Case Study in Transport Logistics Bill Karakostas, Procedia Computer Science Volume 19, pp.594-601, 2013, DOI:10.1016/j.procs.2013.06.079

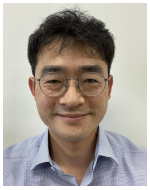
[7] T. Dierks and E. Rescorla. The Transport Layer Security (TLS) Protocol Version 1.2. RFC 5246 (Standards Track). DOI:10.17487/RFC5246

[8] Jeonghun Park, Wonchi Jeong, Sangik Oh, Namje Park. Policy Proposal to Improve Illegal Web Blocking Policy Based on SNI Blocking Technique, Journal of Korea Multimedia Society, vol.23, no.3, pp. 430-439 Mar.2020, DOI:10.9717/kmms.2020.23.3.430

[9] Zakir Durumeric, David Adrian, Ariana Mirian, James Kasten, Elie Bursztein, Nicolas Lidzborski, Kurt Thomas, Vijay Eranti, Michael Bailey, J. Alex Halderman. Neither Snow Nor Rain Nor MITM...An Empirical Analysis of Email Delivery Security, IMC '15: Proceedings of the 2015 Internet Measurement ConferenceOctober Pages 27-39 2015, DOI:10.1145/2815675.2815695

[10] Kyung Sung. Analysis of Linux firewall based on Firewalld, Journal of Digital Contents Society Vol. 21, No. 3, pp.561-567 2020, DOI:10.9728/dcs.2020.21.3.561

Authors



Young Woo Rim was born in Korea, on June 6, 1975. He is a network information analysis and protection engineer. From 2004 to 2019, he worked as an online service and server security programmer in Beijing, China. Currently, he is a network information analysis and protection engineer in Seoul, Korea and a M.Sc. student in the Department of Computer Engineering at Kyungsung University.

Jung Jang Kwon received the B.E. degrees in Electronic Engineering from Pusan University, Korea, in 1985. M.S. and Ph.D. degrees in Electrical Engineering from KAIST, Korea, in 1987 and 1993, respectively.

Dr. Kwon joined the faculty of the Department of Computer Engineering at Kyungsung University, Pusan, Korea, in 1993. He is currently a Professor in the Department of Computer Engineering, Kyungsung University. He is interested in Computer vision, Deep learning , IoT, and embedded systems.