MITM 공격기법을 역이용한 보안시스템 구현

임영우O, 권중장*
O경성대학교대학원 컴퓨터공학과,
*경성대학교대학원 컴퓨터공학과
e-mail: xsapiens@ks.ac.kr*, jjkwon@ks.ac.krO

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

Young-woo RimO, Jung-jang Kwon*
ODept. of Computer Science, Kyungsung University,
*Dept. of Computer Science, Kyungsung University

● 요 약 ●

본 논문은 MITM 공격기법을 역이용한 네트워크 보안 기술 및 구현 방안을 제시한다. MITM(Man In The Middle) 공격은 통신 경로 중간에 개입하여 양 단간의 통신 내용을 가로채거나 행위 제어를 수행하는 전통적인 해킹 방법으로 그 공격 기법을 역이용하여 네트워크 공격을 방어하는 보안기술 및 시스템 구현에 대해 기술한다.

Linux 시스템을 이용하여 ARP Poisoning을 통해 양단간 통신 트래픽에 개입하며, Netfilter 및 Suricata를 이용하여 Network IDS/IPS 및 Firewall을 구현하였고, Contents 필터링 및 Anti-Virus 구현이 가능하며, 여러 기능을 확장하여 UTM(Unified Threats Management) 시스템을 구현하였다.

키워드: MITM, ARP Poisoning, IDS, IPS, Netfilter, UTM, Anti-Virus

I. Introduction

본 논문에서는 기성 네트워크보안장비의 높은 도입비용과 전문보안지식 및 기술을 요함으로 인해 중소기업이 네트워크보안을 흔쾌히 도입하지 못하고 잠재적 보안위협에 노출되어있는 문제를 해소하는 방안으로 MITM공격방식을 역이용한 네트워크보안기법을 제안한다.

II. Preliminaries

MITM을 응용하여 네트워크 접근 통제 기술에 적용된 사례는 NAC(Network Access Control)가 있으나 이를 활용한 진보된 통합 보안기능을 제공하는 사례(IDS/IPS, Firewall, Anti-Virus)는 찾아볼 수 없다.

III. The Proposed Scheme

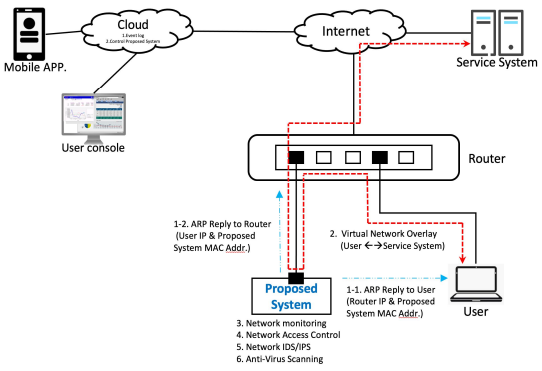

Fig. 1. MITM based Network Protection Architecture

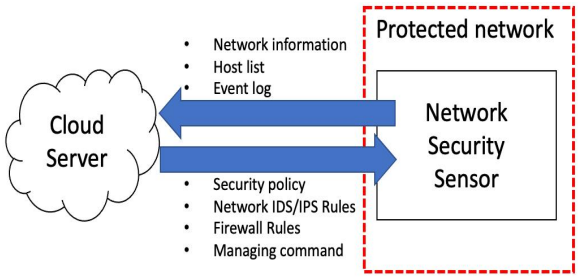

Fig. 2. Network security sensor and Cloud server

Network Security Sensor는 보호대상 네트워크에 직접 참여하여 네트워크 트래픽에 대해 감시와 허용 및 차단 등 일련의 네트워크 제어를 담당한다[1][2].

Cloud Server는 보호대상 네트워크 외부에 존재하며, Network Security Sensor와 통신하여 정책(보안정책, 관리정책)을 관리하고 Network Security Sensor로부터 보호대상 네트워크의 이벤트 로그를 전송받아 관리하는 등 일련의 관리기능과 관제기능을 담당한다.

큰 사이즈의 네트워크보안장비를 설치하기 부담스러운 중소기업의 특성을 고려하여, Network Security Sensor는 Raspberry PI나 Orange Pi등과 같은 초소형 Single Board Computer에 Embedded LINUX를 설치하고 아래의 기능들을 구현한다.

Table 1. Specification of Network Security Sensor

Item	Value
Single board	Raspberry Pi compatible
CPU	H6
Memory Size	1GB
Storage Size	16GB (CFCard)
OS	Embedded LINUX

Network Security Sensor는 HTTPS를 통해 Cloud Server와 통신하며, 네트워크에 참여한 모든 Host의 정보와 각 Host들의 IP Address, Mac Address, Host name, Ethernet device vendor, On/Off line상태, 인터넷사용내역 등을 전송하고, 변경된 정책(Network IDS/IPS 정책, Filrewall 정책, Network Access Control 정책, Anti-Virus정책등) 그리고, 환경설정변경사항 등을 내려받아 적용한다[3].

Cloud Server는 HTTPD, RDBMS가 구성되어있어며, Network Security Sensor의 주기적인 보고(Heartbeat)를 통해 수집된 정보를 RDBMS에 저장 및 갱신한다.

Network Security Sensor는 보안을 고려하여 Listen하는 Port를 가지지 않고 오직 Network Security Sensor가 Cloud Server에 HTTPS의 Client의 역할로 접속하여 통신한다.

Cloud server에서 원격기술지원 세션종료 요청 또는 일정 시간 후 이 세션은 자동 종료되며, Reverse-SSH 서비스도 동시에 자동 종료된다. 이 때, Reverse-SSH를 위한 One-Time-Password와 인증서는 동시에 자동 폐기된다.

IV. Experiments

Table 2. Comparation of functions

주요기능 및 성능	제안시스템	Sophos SG-135	ForiNet FG-200E	Ahnlab IPX-2000A
크기(cm x cm)	초소형 (신용카드 크기)	1U (84 x 84)	1U (84 x 84)	1U (84 x 84)
네트워크 접근통제 (방화벽)	O	O	O	O
네트워크 침입탐지 및 차단	O	O	O	O
가상 네트워크 오버레이	O	X	X	X
네트워크 구성 변경	변경없음	변경 복잡	변경 복잡	변경 복잡
장애발생 시 대응	네트워크에 영향없음	네트워크가 다운됨	네트워크가 다운됨	네트워크가 다운됨
도입예산	수십만원 이내	1천만 이상	1천만원 이상	1천만원 이상
연간 컨텐츠갱신 예산	없음	수백만원 이상	수백만원 이상	수백만원 이상

V. Conclusions

본 논문에서 제안하는 시스템의 실험을 통하여, 단수의 Ethernet Interface만으로 MITM공격방식을 역이용하여 가상 네트워크 오버레이를 구현할 수 있음이 확인되었으며, 네트워크상에서 Router의 역할을 담당하며 네트워크 트래픽을 논리적으로 유도하여 그 패킷을 제어하고 잠재적인 보안위협을 제거할 수 있음이 확인되었으며, 기존의 Inline-mode의 네트워크보안장비와 달리 네트워크보안장비 자체의 장애로 인한 네트워크마비현상을 피할 수 있음이 확인되었다. 또한, 기존의 네트워크환경을 변경하지 않고 네트워크보안설비를 구축할 수 있음이 확인되었으며, 저전력/초소형/저예산의 장비로 고성능의 네트워크보안시스템을 구현할 수 있음이 확인되었다.

REFERENCES

[1] DSNIFF Project, https://github.com/jcfs/dsniff
[2] Suricata Project, https://suricata-ids.org
[3] IEEE OUI-DB, http://standards-oui.ieee.org/oui.txt