Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.28, NO.2, Apr. 2018 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2018.28.2.457

망혼용단말 탐지방법에 대한 연구 및 자동탐지시스템 구현

이 미 화,† 윤 지 원‡
고려대학교 정보보호대학원

A Study on Detection Method of Multi-Homed Host and Implementation of Automatic Detection System for Multi-Homed Host

Mi-hwa Lee,† Ji-won Yoon‡
Graduate School of Information Security, Korea University

요 약

본 연구에서는 망혼용단말(Multi-homed host)이 사라지지 않는 근본원인과 위험성을 알아보았다. 또한, 지금까지 연구·개발된 망혼용단말 탐지방법에 대해 비교 분석하여 개선사항을 도출하였다. 도출한 개선사항을 반영하여 망혼용단말을 효과적으로 탐지할 수 있는 자동 탐지시스템 모델을 제안하고 구현하였다. 아울러, 개발한 탐지시스템을 실제 망분리 기관과 유사한 가상실험환경에 설치한 후, 망혼용단말을 유형별로 발생시켜가며 탐지시스템의 기능과 성능을 측정하였다. 본 연구 범위에서는 오탐과 미탐 없이 정상 작동됨을 확인하였다. 제안한 탐지시스템은 에이전트(Agent) 기반 방식 중, 망혼용단말 탐지를 목표로한 최초의 학술 연구이다.

ABSTRACT

This study aimed to investigate the fundamental reasons for the presence of multi-homed host and the risks associated with such risky system. Furthermore, multi-homed host detection methods that have been researched and developed so far were compared and analyzed to determine areas for improvement. Based on the results, we propose the model of an improved automatic detection system and we implemented it. The experimental environment was configured to simulate the actual network configuration and endpoints of an organization employing network segmentation. And the functionality and performance of the detection system were finally measured while generating multi-homed hosts by category, after the developed detection system had been installed in the experiment environment. We confirmed that the system work correctly without false-positive, false-negative in the scope of this study. To the best of our knowledge, the presented detection system is the first academic work targeting multi-homed host under agent-based.

Keywords: detecting multi-homed host, clock skew, network security

I. 서 론

최근 글로벌 기업, ICS기반시설, 군사기관 등을 대상으로 피해규모가 큰 사이버공격이 지속되고 있다[1,2,3]. 공격자는 자금력이 충분한 산업스파이거나 국가차원의 후원을 받는 전문 집단으로 시간에 구애받지 않고 은밀한 공격을 수행한다[4]. 공격자의 주된 관심사는 망분리 환경을 극복하여 내부망으로 침투하는 것이다. 2016년 9월 확인된 국방부 해킹사고처럼 공격자는 핵심정보가 보관된 내부 폐쇄망(작전망)으로의 침투를 위해 협력업체에 접근하거나, 조직의 IT관리자PC를 이용하는 등 망혼용단말(multi-homed host)을 발견·경유하여 조직의 내부망으로 진입하게 된다[2].

Received(12. 06. 2017), Modified(1st:01. 29. 2018, 2nd:02. 14. 2018), Accepted(02. 23. 2018)
† 주저자, mimi@csc.motie.go.kr
‡ 교신저자, jiwon_yoon@korea.ac.kr(Corresponding author)

이렇게 위험한 망혼용단말은 왜 사라지지 않는 것일까? 망혼용단말은 협력업체나 내부직원이 사용한다[5]. 협력업체에서 고객기관의 시스템을 예방점검하기 위해 방문시마다 반입파일의 백신점검 및 유해성 유무 확인 등을 관리자 입회하에 실시하게 된다. 누락된 파일이 있을 경우 동일한 점검 과정을 거쳐야 하는데 의외로 이러한 상황이 빈번하고 또 협력업체 수가 많아 대기시간이 길어져 불편이 따른다. 이런 사유로 기관담당자 모르게 (또는 담당자 묵인 하에) 인터넷망과 내부망에 제약 없이 자료전송이 가능하도록 NIC을 1개 더 추가 장착하여 사용하는 경우가 있다. 정보시스템 관리자의 보안의식이 부족하여 망혼용서버가 운용되는 경우도 있다. NTP, DHCP 서버 등 효율성 때문에 1대로 운영하는 사례 등이다.

최근 몇 년 사이 망혼용단말을 탐지한다고 소개되는 상용 솔루션(I사, G사, W사)이 확인되었으나, 이들 탐지방식에 대한 직접적인 국내 연구문헌은 찾을 수 없었다. 국외 연구 중 Agentless 방식으로 원격에서 시각 편차(Clock Skew) 특성[6]을 이용하여 망혼용단말을 탐지하는 방법[7]을 확인하였으나, 기업 환경에서의 효과성, 정확성이 아직 검증되지 않았다. 기존 상용솔루션과 시각편차 등 4건의 탐지방식을 비교 분석하여 2건의 개선사항을 도출하였다. 첫째, 다중OS 환경의 망혼용단말을 탐지할 수 있어야 하고 둘째, 탐지시스템 자체가 망간의 접점이 최소화되어야 하고 보안성이 고려되어야 한다. 본고에서는 이들 개선사항을 해결한 탐지시스템을 구현하였다. 또한, 탐지시스템은 가용성 저해를 우려하여 Agent 설치를 꺼리는 서버 시스템에도 운용될 수 있도록 사용자 영역(User level)에서 구동되는 Python 스크립트로 개발하였다. 이로서 조직 내 Agent 가 미설치되는 사각지대를 없앤다면 망혼용단말을 적시에 식별하여 망혼용단말을 경유한 해킹사고를 미연에 예방할 수 있을 것이다.

본 논문에서는 Ⅱ장에서 기존 연구 및 상용 솔루션의 작동방식을 분석하고, Ⅲ장에서 망혼용단말의 위험성을 알아본다. 이후 Ⅳ장에서 기존 연구의 개선점을 도출한 탐지시스템의 기본모형을 설계하고 Ⅴ장에서 설계를 바탕으로 실험환경 구축 및 Agent 개발, 실험 진행 및 결과를 분석하였다. Ⅵ, Ⅶ장에서는 토론 이슈와 결론, 향후 연구방향을 다루었다.

Ⅱ. 관련 연구

2.1 배경 지식

망혼용단말은 Fig. 1. 처럼 운영체제에 NIC (Network Interface Card, 랜카드)이 2개 이상 장착(homed)되어 여러 망을 사용하는 정보통신단말을 의미한다[7]. 두 망 사이의 보안시스템의 통제를 받지 않고 우회가 가능하기 때문에 침입차단시스템(Firewall) 등 SecureOS 기반의 정보보호시스템을 제외하고는 사용을 금지하고 있다[8]. 망혼용단말은 복잡도를 낮추고 관리편의성이 개선되는 것처럼 보이지만 경계보안(Perimeter Security) 메커니즘을 우회한다[9,10,11]. NIC을 1개 사용하는 단말이더라도 시간 간격을 두고 다른 망으로 옮겨다니며 사용하는 것도 망혼용단말로 분류될 수 있다. 국내 주요정보통신기반시설에서는 시간 차이를 두고 망을 이동하며 사용하는 경우를 금지하고 있다.

망혼용의 대표적인 방법으로 PC, 노트북, 서버 등에 NIC을 추가 장착하여 사용하는 경우가 있다. NIC 인터페이스는 PC, USB 규격 등 다양하며 가상머신에 연결하여 사용될 수 있다. 그 외 웜홀 스위치(Worm-hole Switch)를 사용하여 2개 단말의 파일시스템을 서로 공유하여 파일 복사, 생성, 실행 등을 할 수 있는 방법도 있다.

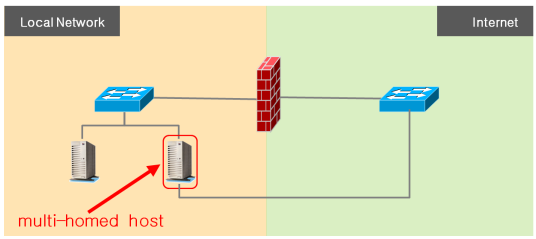

Fig. 1. Multi-homed host equipped with two NICs(Bypass the firewall)

2.2 망혼용단말 탐지방식

2.2.1 블랙리스트(MAC, IP) 기반

각 망에 존재해서는 안 될 블랙리스트(MAC 리스트)를 생성한 후 각 망의 NMS[1], NAC[2] 등에 등

1) NMS(Network Management System)
2) NAC(Network Admission Control)

록 후 탐지하는 방식이다. 예를 들어, 인터넷이 차단된 업무망, 폐쇄망의 MAC리스트를 조사한 후 이를 인터넷망 NMS, NAC 서버에 수기 등록하여 인터넷망에서는 해당 MAC이 통신되지 않도록 탐지·차단하는 방식이다.

2.2.2 망간 차단MAC 여부 질의

IP관리서버(NMS)에서 신규 단말 감지시, 해당 신규 단말이 타 망에 존재하는 MAC 주소인지를 알아보기 위해, 타 망의 IP관리서버로 TCP 기반 질의(Query)하는 방식이다. 질의 결과 타 망에 존재하는 단말이라면 격리하게 된다. 이러한 방식은 망간의 접점이 발생되기 때문에 망분리 기관에서는 위험하다. 예를 들어 인터넷망에서 업무망으로 질의할 때 업무망 TCP Port 가 개방되어 있으므로 취약한 구성이다. 공격자가 인터넷망 IP관리서버를 점령하면 업무망으로 건너갈 수 있는 거점으로 삼을 수 있기 때문이다.

2.2.3 망간 차단MAC 정보 전파

업무망 NAC 서버에서 인가단말 A 발생시 주변 망(인터넷 망) NAC 서버에 A단말의 MAC 주소를 차단토록 MAC 주소를 전파한다. 전파 방식은 SNMP 프로토콜을 사용한다. 주변 망의 NAC 서버에서는 망 내 신규 단말 인지시 〔차단 MAC리스트〕에 존재유무를 확인 하여 존재할 경우 해당 단말을 격리시킨다. 다른 방식이 모두 Agentless 인 데 반해 이 방식은 Agent 방식도 지원하였다.

2.2.4 SIEM[3] 기반

SIEM 기반의 탐지 방식으로는 방화벽 로그 기반과 Error 로그 기반이 있다. 첫째, 방화벽 로그 기반 방식은 인터넷망 방화벽 로그에서 업무망대역의 IP가 발견될 경우 (또는 그 반대) 해당 단말을 망혼용단말로 탐지하고 이벤트를 발생시킨다. 두 번째 Error 로그 기반 탐지 방식은 SIEM 의 일반적인 연동 기능〔12〕 외 네트워크 장비의 ACL, VLAN, 망연계 시스템의 정책 위반 로그가 발생될 경우 로그속의 IP가 해당 망의 비인가IP라면 망혼용단말로 간주하고 이벤트를 발생시키는 방식이다.

2.2.5 시각편차(Clock Skew) 기반

네트워크 패킷을 일정시간 캡처한 후 모든 TCP 패킷의 TIMESTAMP 값을 상세히 비교하면 각 패킷을 생성한 Host 들의 고유한 시각 편차를 구할 수 있고 이 편차(기울기값)를 가지고 각 Host를 유일하게 구별할 수 있는 방법이다〔7〕,〔13〕. 기울기값이 유사하면 동일 단말의 클럭(Clock) 센서에서 발생된 시간값을 의미한다. 이 방식은 라즈베리파이 기기 7대를 가지고 실험한 것으로 동일 서브넷(Subnet) 안에서 소수 단말간에 망혼용단말 기기를 특징지을 수 있었다. 그러나 여러 제조사의 하드웨어 OS, 여러 서브넷과 보안시스템이 설치된 Enterprise 환경에서는 아직 검증되지 않은 기술로 저자는 관련 연구를 계속 진행 중에 있다〔7〕.

2.3 탐지방법 요약

2.2에서 살펴본 5가지 방식은 단말이 망을 이동하며 사용할 경우 손쉽게 탐지됨을 알 수 있다. 그러나, 2.2.1~2.2.4의 탐지방식은 2개 이상의 NIC을 동시에 사용하는 단말을 탐지할 수 없다(단, 2.2.3의 Agent 방식은 제외). Agentless 방식이기 때문에 현재 망에 연결된 NIC만 분석할 수 있고, 해당 NIC이 설치된 단말의 내부에 설치된 다른 NIC의 존재에 대해서는 알지 못하기 때문이다. 예를 들어, A직원의 PC가 미흡한 보안절차를 거쳐 업무망과 인터넷망 모두에서 인가를 받았을 경우 A직원의 PC는 2.2.1~2.2.4 방식에서 탐지되지 않는다. 각 NIC이 망을 번갈아가며 사용하지 않았고 인가를 받았기 때문이다. 2개 NIC 중 1개라도 망을 번갈아 사용한다면 탐지되지만 그렇지 않고 계속 사용할 경우는 탐지되지 않는다. 이러한 사례는 용역계약 사업시에도 간혹 발생된다. 보안담당자가 망사용신청서 접수시 업무망과 인터넷망에 사용할 MAC 주소만 확인하고 인증해주는 경우이다.

2.4 기타 방법

금융기관에서 인가된 공인IP그룹(대역) 이외의 인터넷 사용 단말을 탐지하는 방법도 있다〔14〕. 탐지절차는 먼저 기관 내 단말의 IP, ARP, ROUTE,

3) SIEM(Security Event and Incident Management)

DNS 정보 등을 수집하고 이를 외부의 수집서버(WWW)로 전송한다. 그 다음, 외부의 수집서버에서는 정보를 전송한 패킷의 출발지IP를 확인하여 인가된 공인IP가 아닌 경우 비인가 단말로 판정한다.

III. 위협 모델

3.1 망혼용단말 발견 사례

국내 망분리가 적용되기 시작한 2009년부터 망혼용단말이 지속적으로 발견되고 있다. 주된 사례로는 직원 및 협력사 단말(업무용PC, 유지보수용 노트북), IT기반시스템(NTP, DHCP, 프린터 서버), 네트워크 관리(NMS), 보안솔루션(백신관리, 패치관리서버), 전화망 시스템(음성녹취서버) 등이다. 일부 시스템은 수년이 넘도록 발견되지 않은 사례도 있다.

3.2 공격 시나리오

Fig. 2 의 공격 시나리오를 통해 '망혼용단말'의 위험성을 알아보자. 첫째, 공격자가 스피어피싱 메일을 발송한다. 둘째, 메일을 수신한 기관 직원이 피싱 메일의 첨부파일을 클릭하여 감염된다. 셋째, 공격자는 감염PC에서 주변 단말을 공격하여 망혼용단말(시스템)을 찾아낸다. 넷째, 망혼용된 NIC을 경유하여 업무망을 유유히 돌아다니며 공격을 시도한다. 특히, Fig. 2의 4번 과정에서 망혼용단말이 장악되면 내부 업무망으로의 진입에 아무런 제한이 없음을 알 수 있다. 이러한 이점 때문에 공격자, 모의해커들은 망혼용단말을 선호한다[15].

IV. 제안 방법 및 모델

4.1 제안 동기

2.2 망혼용단말 탐지방식을 종합하여 망혼용단말의 유형 및 탐지기술 수준에 대해 정의해보면 Table. 1 과 같다. 유형 1은 망을 이동해가며 사용하는 단말이고 기존 상용 솔루션에서 탐지가 가능하다. 유형 2는 단일OS에 NIC을 2개 이상 사용하는 경우로 2.3에서 살펴본 바와 같이 미탐의 소지가 있다. 유형 3은 새롭게 정의한 유형으로, 다중OS(가상머신)에 NIC을 2개 이상 사용하는 단말을 말한다. 현재 이를 탐지하는 기술·솔루션은 확인할 수 없었다. 따라서, 유형 1 뿐만 아니라 2, 3까지 탐지할 수 있는 방안이 필요하다. 특히, 2개 NIC 중 1개가 가상머신(Guest OS)에 연결되어 있는 유형 3의 경우 가상머신이 타 망을 사용하는지 여부까지 조사할 수 있어야 한다.

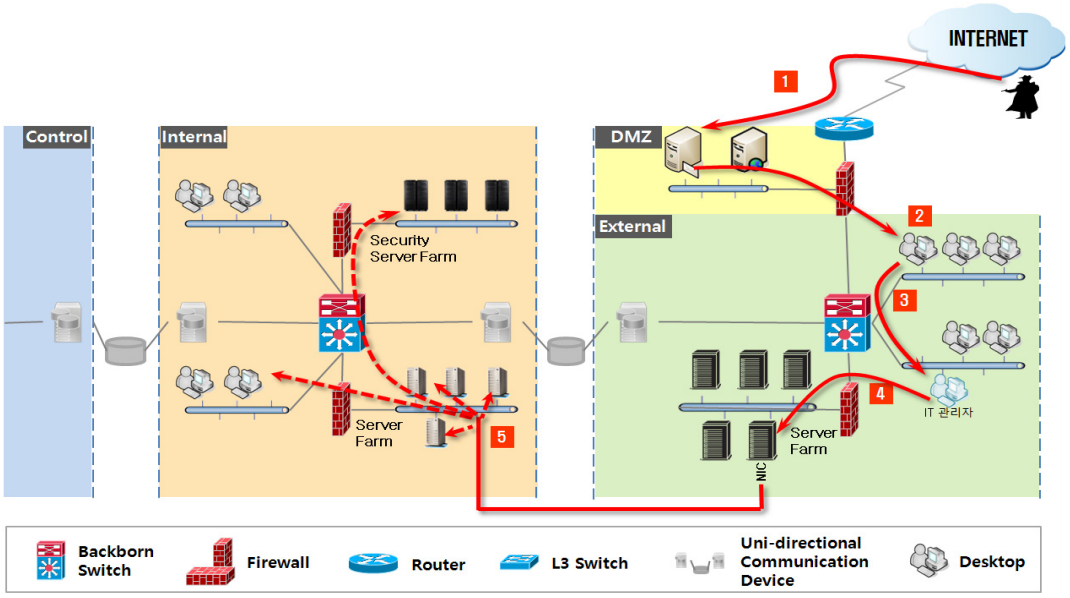

Fig. 2. Attack Scenario(Bypass the firewall)

Table 1. Multi-homed host type and detection tech level

Multi-homed host Type	Description	Detection Technology Level
Type 1	System(Endpoint) used to move the network (Use LAN cable alternately)	●
Type 2	Use Two or More NICs (Single OS)	◐
Type 3	Use Two or More NICs (Multi OS, Concurrent Use)	×

지금까지 살펴본 탐지기술의 한계점(Table. 2 빨간 상자)을 분석하고, 몇 가지 질문을 통해 종합적인 개선사항을 도출해보았다. 첫째, Table. 2의 ①~⑤에서 차단 MAC리스트에 존재하지 않는 단말은 어떻게 차단할 것인가? 가상머신을 사용하는 망혼용단말인 경우 OS수준에서 가상머신의 NIC정보를 수집할 수 있어야 한다. 결국, Agent 기반으로 구동되어야 한다. 둘째, ①~⑤에서 MAC Spoofing 되어 사용되는 단말인 경우 차단 가능한가? 단말에 설치된 모든 NIC의 실제 MAC 주소를 읽어 지속적으로 기록하고 변화 여부를 모니터링할 수 있어야 하므로 Agent 기반이어야 한다. 셋째, 망간의 접점을 없앨 수 있는 방법은 무엇인가? 망 구조를 새롭게 설계하여야 한다.

Table 2. Comparison of multi-homed host detection method

	Detection Method	Operation	Network Point of Contact	Risk Level	Type 1	Type 2	Type 3
①	Blacklist based	Manual	X	·	○	X	X
②	Query whether or not to block a MAC	Automatic	○	Very Vulnerable	○	X	X
③	Block MAC information propagation between networks	Automatic	○	Vulnerable	○	△	X
④	SIEM - Firewall Log based	Automatic	X	·	○	X	X
⑤	SIEM - Error Log based	Automatic	X	·	○	X	X
⑥	Clock Skew	Automatic	X	·	○	○	○

4.2 탐지 방법

탐지 시스템 구성과 프로세스는 Fig. 3, Fig. 4와 같다. 분석방법은 첫째, 각 망에 로컬서버를 1대씩 두고 망 내 모든 단말들의 NIC 정보를 수집하여 보관한다. 둘째, 로컬서버에 보관된 NIC 정보를 정기적으로 집계하여 중앙서버로 전송한다. 셋째, 중앙서버에서는 수집된 전체 NIC 정보를 바탕으로 특정 MAC 주소가 2개소(지역) 이상의 망에서 발견되는지 분석한다. 2개 이상 지역에서 사용하는 MAC은 망혼용단말에 포함된 NIC의 것이다. 넷째, 식별된 MAC이 있을 경우 망혼용단말이므로 관리자에게 SMS 메시지를 발송한다.

위와 같은 처리를 위해 몇 가지 사전조건이 갖추어져야 한다. 첫째, 인터넷망, DMZ망, 인터넷 서버팜, 업무망, 업무망 서버팜, 관제망 등 조직 내 모든 망에 대해 정의한다. 둘째, 각 망에서 운용되는 모든 단말에 Agent가 설치되어야 한다. 셋째, Agent는 NIC의 상세정보 및 Host에 대한 정보도 수집한다. 특히, 가상머신에서 구동중인 NIC 정보를 수집하기 위해 가상머신SW 제작사의 SDK (Software Development Kit)나 Tool을 활용한다[16,17,18].

4.3 탐지시스템 설계

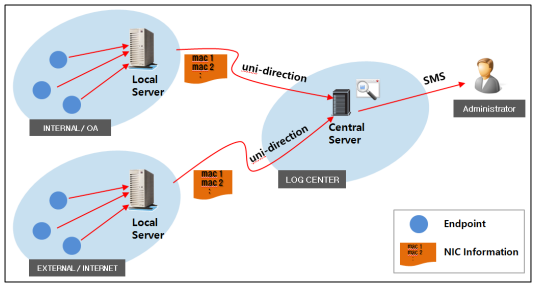

Fig. 3. Concept Map of Detection System

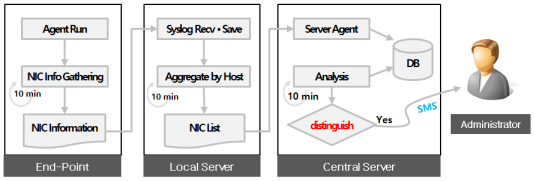

Fig. 4. Process Flow Diagram

4.3.1 시스템 구성

망과 망 사이 별도의 완충구간(로그망)을 두고 여기에 망혼용단말을 자동분석할 수 있는 중앙서버를 둔다. 안전한 망 구성을 위해 다수의 인라인 방화벽을 설치하고, 서브넷을 영역별로 구획하여 보호한다. 로그망의 경우 망간의 거점(Stepstone)이 될 수 있으므로 인접한 망에서 유입만 되고 건너편 망으로는 넘어갈 수 없도록 방화벽 정책을 엄격하게 적용한다〔11〕. 이렇게 구축된 로그망은 해킹을 당하더라도 인접망으로의 공격이 확장되지 않으므로 보안성이 높은 구조가 된다.

4.3.2 단말(End-point) 및 서버

단말의 NIC 관련 정보(NIC 개수, IP, MAC)를 수집한다. 향후 망혼용사용이 확인될 경우 추적자료로 활용하기 위해 여분의 정보(Hostname, OS명, 현재 사용자명 등)를 수집하고, 가상머신을 사용한 단기간 정보유출행위를 탐지하기 위해 실행주기를 5분 이내로 짧게 상정한다. 가상머신 발견 시에는 Hostname 뒤에 별도의 표식("(HAS_VM)")을 추가하고 가상머신의 NIC정보를 마지막 레코드 뒤에 기록한다. Fig. 5 는 수집 예시로 NIC개수, 사용자명, OS명, 사용자명, 망혼용단말 의심여부, 네트워크 인터페이스(Network Interface) 명, NIC 활성화 여부, MAC, IP, Subnetmask, GW가 수집된 로그를 보여주고 있다.

수집된 정보는 단말의 로그 디렉터리에 일자별로 기록한 후 로컬서버로 전송한다. 전송 메시지 규격은 Fig. 6 을 구분자 "|"로 구분하여 구성한다. 서버 데몬은 별도로 개발하지 않고, 안정적으로 단방향(Uni-direct) 통신이 가능한 SYSLOG를 사용한다.

로컬서버는 수신되는 정보를 /var/log/endpoint_info.log로 저장하고, 주기적으로 읽어들여 중앙서버로 전송한다. 중앙서버는 수신된 집계파일을 로컬 DB 에 저장한다. 로컬 데몬은 5분 단위로 DB 파일을 분석하여 망혼용단말을 추출한다. 식별된 망혼용

```
2|mimi|Windows-7-6.1.7601-SP1|IEUser|Intel(R) PRO/1000 MT Desktop Adapter|on|08:00:27:1d:5a:52|10.100.0.9|255.255.255.0|10.100.0.2|Intel(R) PRO/1000 MT Desktop Adapter|on|08:00:27:56:2c:a5|10.0.2.5|255.255.255.0||
```

Fig. 5. Log Example(End-point Agent)

```
Algorithm : Skeleton of Detection multi-homed host
// procedure type1_check
i ← 0;
record ← Query(OA.mac == INT.mac);
idx ← RowCount(record);
foreach i ∈ idx do
    if IsAlreadyDetected(record[i].mac) then
        print (Previous_Detected_Information(record[i].mac));
    else
        // Write Information
        Write_Detected_Information(record[i].mac);
        // Print host information by MAC address that has found
        print (GetHostInformationbyMAC(record[i].mac));

// procedure type2_check
record ← Query(
    // count of nic > 1
    NODES.cbIfaces > 1 and
    (
     // Has both external IP and internal IP
     (locate('10.200.', NODES.ips) and locate('10.100.', NODES.ips) or
     // Has both external IP and DMZ ip
     (locate('10.200.', NODES.ips) and locate('10.0.10.', NODES.ips) or
     // Has both internal IP and DMZ ip
     (locate('10.100.', NODES.ips) and locate('10.0.10.', NODES.ips)
    )
:

// procedure type3_check
record ← Query(locate('HAS_VM', NODES.hostname));
:
```

Fig. 6. Key Pseudo Code

단말 정보를 설치된 CDMA 모듈을 통해 관리자에게 SMS로 발송한다.

4.3.3 망혼용단말 탐지(분석)

첫째, 각 망별로 수집된 MAC 주소가, 다른 망에 존재하는지 건별로 비교한다. 둘째, 타 망에 존재한다면 〔망혼용단말 Table〕에 기록한다. 셋째, 망혼용의심 Flag가 설정된 레코드가 있다면 〔망혼용단말 Table〕에 기록한다. 넷째, 〔망혼용단말 Table〕에 신규 추가된 정보를 관리자에게 SMS로 발송한다.

Fig. 6은 망혼용단말 유형 1~3 검출과 관련한 주요 의사코드(Pseudo Code)를 나타낸다. 유형 1은 OA(Internal) 영역에 기록된 MAC 주소와 INT(External) 영역에 기록된 MAC 주소가 동일한 레코드를 추출한 후, 기존 탐지된 MAC 이면 과거 정보를 보여주고 그렇지 않으면 탐지정보를 기록하고 화면에 위반정보를 출력한다. 유형 2는 NIC 개수가 2개 이상이면서 OA망 대역 B클래스(10.100)와 INT망 대역 B클래스(10.200)을 포함한 레코드

를 추출한다. 유형 3은 Hostname 에 "HAS_VM" 플래그가 명시된 레코드만 추출한다. 중복 탐지 여부는 유형 2, 3도 유형 1의 것처럼 동일하게 수행한다.

V. 실험 및 결과 분석

4.3에서 설계한 시스템의 효과성을 검증하기 위해, 가상환경으로 네트워크 환경과 단말, 방화벽을 구축하고, Agent, 로컬서버와 중앙서버의 서비스 데몬을 개발하여 세부적인 기능과 성능을 실험시나리오에 입각하여 측정하였다.

5.1 실험 환경

실험 환경(서버 1대)에서 Network Emulator를 구동한 후 세부기능을 확인한다. 서버 사양은 CPU Intel Core i7/2.4Ghz, RAM 8GB, SSD 256GB, Ubuntu Linux 16.04 이다. 1차 실험에서는 가상단말 수를 최소화하여 기본적인 기능평가를 한 후, 가상단말 수를 점차 늘려가며 최대 성능을 평가하도록 2차 실험을 진행하였다. 중앙서버의 SMS 발송 기능은 구현범위에 포함하지 않았다. 실험에 사용된 Network Emulator는 CORE[19], Mininet[20], GNS3[21] 보다 통신 Overhead가 없고, 실험 환경 구동 속도가 빠른 IMUNES(ver 2.0)를 사용하였다[22].

5.2 환경 구축 및 개발

IMUNES 에뮬레이터를 사용하여 망 구성과 단말을 설계하고, 실험환경을 실행시킨다. 세부적인 라우팅 설정, 가상단말에 필요한 Python 스크립트와 Cron 설정 등은 별도의 초기화 스크립트로 작성하였다.

본 연구에서의 핵심기능은 모든 단말에서 가상머신의 구동 여부를 확인하는 부분이다. 본고에서는 Oracle VirtualBox에 한정하여 기능을 구현하였다. VirtualBox의 경우 VBoxManager 라는 관리

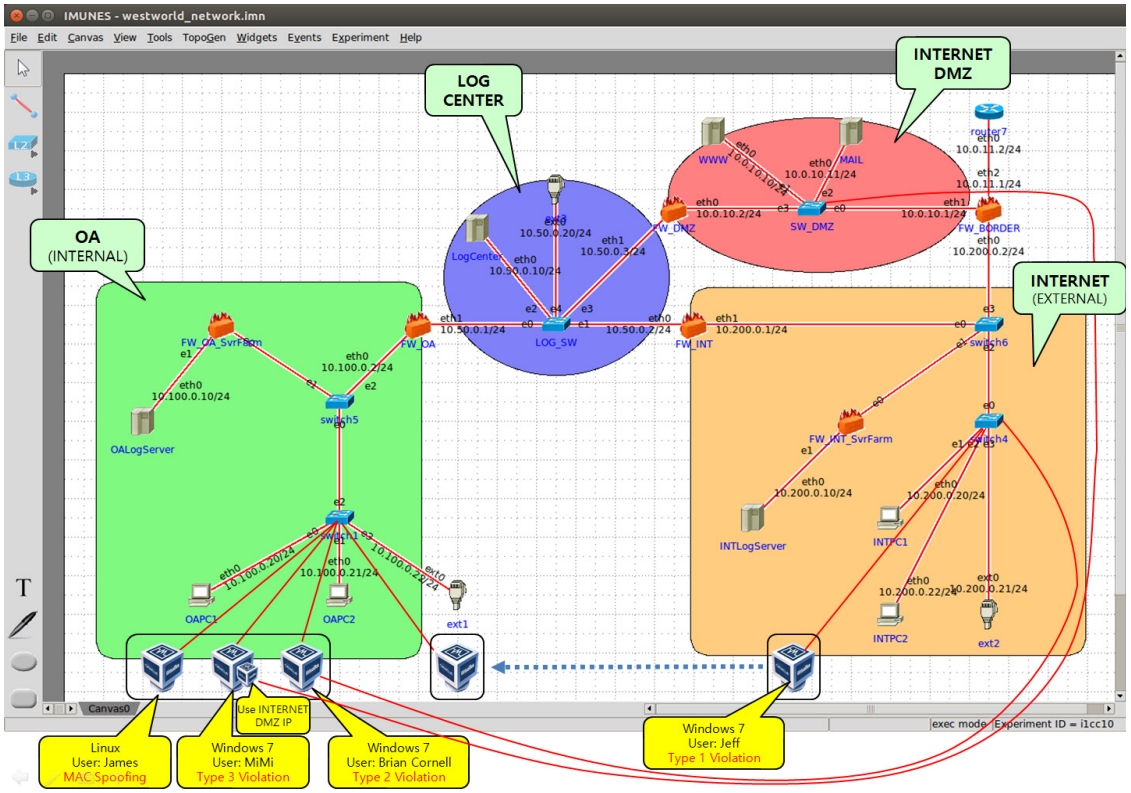

Fig. 7. Test Environment(Scenario). IMUNES with Virtual Machines. Scenarios that cause multi-homing violation types in virtual machines.

Tool을 활용하면 단말에 설치된 VirtualBox의 이미지 개수, 실행정보, 내부 상세 구성정보를 확인할 수 있다[16].

5.3 1차 실험(기능 평가)

실험은 Fig. 7 처럼 에뮬레이터 구성에 VirtualBox 가상머신 5대를 연결한 환경에서 기능평가 4개(5.3.1~5.3.4)를 실험하였다. IMUNES에서 제공하는 기본 단말은 리눅스 컨테이너(Container) 기반으로 네트워크와 관련한 상세설정(NIC 추가·삭제, 동적 IP 구성변경 등)에 제약이 있어 별도의 VirtualBox 가상머신을 활용하였다. 실험 순서는 망혼용 유형 1~3을 에뮬레이팅 환경에 발생시키고, 마지막으로 MAC Spoofing 상황을 발생시켜보았다.

5.3.1 시나리오 1 - 망혼용 유형 1

인터넷망에서 사용 중인 단말 1대(Windows 7, User: Jeff)를 업무망에 연결시킨 후 탐지여부를 확인하였다. 몇 분 뒤 중앙서버에서 '망혼용 유형 1' 위반 단말로 탐지하였다(Fig. 8)

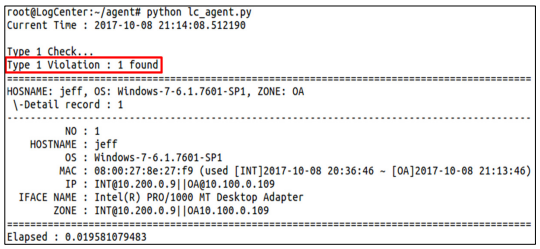

Fig. 8. Detection of Multi-homed host violation Type 1

5.3.2 시나리오 2 - 망혼용 유형 2

업무망을 사용하던 단말(Windows 7, User: Brian Cornell)에 NIC을 1개 더 장착하고 인터넷망 랜케이블을 연결한 후 인터넷망 대역 IP(10.200.0.119)를 설정하였다. 약 6분 경과 후 중앙서버에서 '망혼용 유형 2' 위반 단말로 식별되었다(Fig. 9).

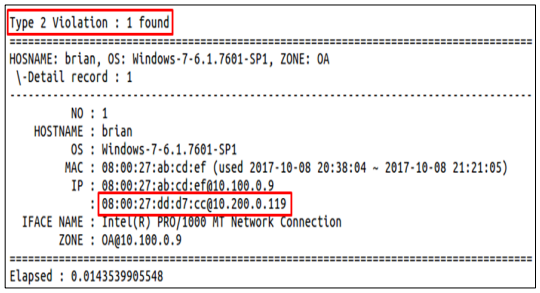

Fig. 9. Detection of Multi-homed host violation Type 2

5.3.3 시나리오 3 - 망혼용 유형 3

업무망 단말(Windows 7, User: MiMi) 사용자(관리자)가 VirtualBox를 이용하여 Linux를 설치하고 별도의 NIC을 가상머신에 인식시킨 후 DMZ망 케이블을 연결하여 인터넷을 시도하려고 할 때 이를 탐지하는지 실험하였다. 실험 결과, '망혼용단말 유형 3'(다중OS 환경) 검출 과정에서 위반 단말로 탐지됨을 확인하였다. 탐지시 Hostname 에 별도 식별표시"(HAS_VM)"를 확인할 수 있었고, 해당 가상머신 내부의 정보(MAC @IP@OS명#NIC개수# 인터페이스명)를 확인하였다(Fig. 10). OS명은 Linux, NIC은 1개, 인터페이스명은 eth0이다.

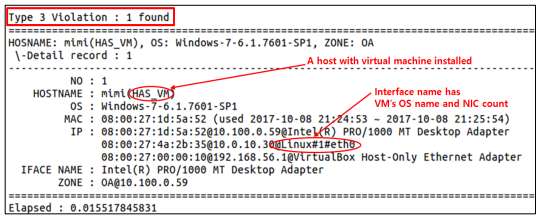

Fig. 10. Detection of Multi-homed host violation Type 3

5.3.4 시나리오 4 - MAC Spoofing(유형 4)

업무망 단말(Linux, User: James)에서 MAC 주소를 변경(08:00:27:5e:35:53 → 08:00:27:12:34:56) Spoofing 한 결과, '망혼용 유형 4' 위반 단말로 식별되었다(Fig. 11). 편의상 MAC Spoofing 실험을 유형 4로 명명하였다. 본 연구에서는 지역서버에서 중앙서버로 각 망의 단말정보를 주기적으로 전송할 때, MAC 정보를 별도로 추출하여 MAC 사용이력테이블(MAC_Used_History)에 기

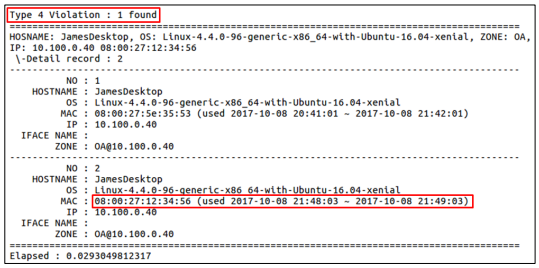

Fig. 11. Detection of Multi-homed host violation Type 4

록하고 향후 단말 간 비교자료로 활용토록 하였다. 단말 간의 구별은 소기의 연구목적상 Hostname + OS + MAC으로 한정하였다. 만약, 기존에 정상적으로 인가되어 사용되던 MAC주소가 다른 단말에서 Spoofing 되어 사용될 경우 MAC Spoofing 단말로 자동 탐지되게 된다. Spoofing 된 신규 단말의 Hostname이나 OS 정보가 기존 MAC사용이력테이블에 기록된 Hostname, OS값과 다르기 때문이다.

5.3.5 기타 실험(테더링)

망혼용을 위해 LTE Egg(Portable Router), Wifi Egg, 스마트폰 등을 이용한 테더링(Tethering) 기술이 사용될 수 있어 이를 탐지할 수 있는지 추가 실험하였다. 테더링 기술은 대상단말과 네트워크 공유를 위해 USB, Bluetooth, Wifi(Mobile Hotspot) 연결 방식을 사용한다.

Table 4. Tethering Type and NIC Name

Tethering Type	NIC(Logical Adapter) Name
USB	Remote NDIS based Internet Sharing Device
Bluetooth	Bluetooth Network Connection

USB, Bluetooth 방식은 대상 단말 OS에 가상의 NIC 어댑터를 생성시켜 연결(Table 4)하며, Wifi Hotspot 은 대상단말에 기 설치되어 있는 무선 NIC을 사용하여 연결한다. 스마트폰, 태블릿 등 이동형 기기는 대부분 위 3가지 테더링 기술을 모두 사용하고 Wifi Egg, LTE Egg는 연결효율이 높은 Wifi 나 USB 방식을 사용한다.

요약하면 사용자 단말에서 테더링 할 경우 단말에 가상의 NIC을 신규로 생성(USB, Bluetooth 방식)하거나, 기존의 무선 NIC을 사용(Wifi 방식)하여 연결하게 된다. 본 연구에서 구현한 탐지시스템은 운영체제가 제공하는 NIC 정보를 수집하여 분석한다. 그렇다면 테더링시 이용되는 NIC 정보를 모두 수집할 수 있을까? 그렇다면 망혼용단말을 탐지할 수 있을 것이다.

Wifi 테더링 방식은 기존에 설치되어 있는 일반 무선 NIC을 사용하므로 해당 NIC 정보는 정상적으로 수집할 수 있다. 그러나 USB, Bluetooth 방식에서 생성되는 가상NIC 정보는 정상적으로 읽혀질까? 가상 NIC은 운영체제의 하드웨어 추상 레이어(Hardware Abstract Layer)에 의해 표준 NIC처럼 변환되어 정보가 제공되므로 수집 될 것이라 추정된다. 이러한 가설이 맞는지 확인하기 위해 실험을

Table 3. Search Time by Multi-homed host Type

Test Period	10 hour 30 min (2017-10.22 21:10 ~ 10.23 07:40)						
Test Result	No	Time	Elapsed Time (hh:mm)	Query Response Time(Seconds)			
				Type 1	Type 2	Type 3	MAC Spoofing
	1	2017-10-22 21:10	00:00	0.001720190	0.001183987	0.000782967	0.002284050
	2	2017-10-22 21:15	00:05	0.007570028	0.001079083	0.000664949	0.002671957
	3	2017-10-22 21:20	00:10	0.003468037	0.001227856	0.000890970	0.002856970
	4	2017-10-22 21:25	00:15	0.017074108	0.004636049	0.001494169	0.008118868
	5	2017-10-22 21:30	00:20	0.017254114	0.002655983	0.000805140	0.002883196
	:	:	:	:	:	:	:
	126	2017-10-23 07:35	10:25	1.937278032	0.003106117	0.001865864	0.037803888
	127	2017-10-23 07:40	10:30	1.972023964	0.002962112	0.001968145	0.028430939
	Average Search Time			0.753337468	0.002357252	0.001561411	0.019215818
	Search Time Rank			4	2	1	3

진행하였다. USB 테더링은 Fig. 12의 LTE Egg로 실험하였고, Bluetooth 테더링은 Windows 8 환경의 노트북과 안드로이드 기반 스마트폰을 이용하였다. 실험 결과, 두 테더링 방식에서 신규 생성한 가상의 NIC 정보가 정상적으로 수집됨을 확인하였다(Fig. 13, 14). 이로서 조직 내 어느 단말에서 테더링이 발생되어도, 단말Agent 가 정상적으로 설치되어 있으면 테더링하는 단말의 모든 NIC 정보를 수집하여 망혼용유형을 탐지할 수 있음을 알 수 있다.

Fig. 12. LTE Egg (LG U+ MyFi LTE Router)

2|brian|Windows-7-6.1.7601-SP1|brian|Intel(R) PRO/000 MT Network Connection|08:00:27:ab:cd:ef|10.100.0.9|255.255.255.0|10.100.0.2|Remote NDIS based Internet Sharing Device|00:0A:3B:FF:FF:01|192.168.1.50|255.255.255.0|192.168.1.1||

Fig. 13. Log Example (USB Tethering)

3|bluecpu|Windows-8.1-6.3.9600|Jeff|Bluetooth 장치(개인 영역 네트워크)|on|5c:c5:d4:e8:ca:19|192.168.44.85|255.255.255.0|Microsoft KM-TEST 루프백 어댑터|on|02:00:4c:4f:4f:50|169.254.138.91|255.255.0.0||Intel(R) Dual Band Wireless-AC 7260|on|5c:c5:d4:e8:ca:15|172.30.1.17|255.255.255.0|172.30.1.254||

Fig. 14. Log Example (Bluetooth Tethering)

5.4 2차 실험(성능 평가)

단말수를 최대한 늘려 업무망 20대, 인터넷망 20대 및 기타 서버를 포함, 총 51대 가상단말을 구축하여 실험을 진행하였다. 진행시간은 약 10시간 30분이다. 실험 결과, 망혼용단말 유형 별 검색시간과 평균 검색시간은 Table. 5와 같다. 유형 3의 평균검색시간(0.001561411초)이 가장 빠른데, 이유는 Database 쿼리시 Hostname 컬럼에 "HAS_VM" 문자열이 포함된 레코드만 한정해서 가져오므로 검색속도가 빠르다. 유형 1, 2, 4의 경우는 Host와 NIC 테이블의 전체 레코드를 대상으로 비교 분석하므로 상대적으로 느리다. 특히, 유형 1의 경우는 각 망별 전체 레코드를 Group 지은 후 비교하기 때문에 가장 느리다(0.753337468초).

5.5 실험결과 분석

망혼용 정책을 위반한 단말은 중복해서 탐지되지 않도록 정책위반 정보를 별도로 기록하여 성능을 개선하였다.

Fig. 15는 시간흐름에 따른 유형 2~4의 검색속도를 나타낸다. 우리의 주된 관심사는 유형 3(다중 OS + 다중 NIC)과 가장 느린 검색속도를 나타낸 유형 1이다. 기업 규모가 큰 환경에서의 성능을 가늠해 보기 위해 직원 2,000명일 경우의 예상검색시간을 예측해보았다. 예측 방법은 Table. 3 의 실측 데이터를 기반으로 향후 예상 검색시간을 trend와 growth 함수로 계산한 후, 결정계수(R2[4])가 높은 값을 선택하였다. trend 함수의 결정계수가 0.88로 growth(0.80)보다 높아 trend 추정 값을 채택하였다. Table. 5 는 향후 예상 검색시간 중 매 2,000번째의 레코드만을 간추려 표현한 것이다. 이는 PC 2,000대 환경에서의 탐지시간을 나타낸다.

예를 들어 유형 3의 경우, A직원이 탐지시스템 가동 후 30분이 경과한 시점에 가상머신을 구동하여 망혼용 사용을 시도할 경우, 다음 번 실행주기인 35분에 약 0.003초(❶) 이내 탐지가 가능하다. 실제관리자가 식별하기까지는 실행주기 5분(❷)을 고려하여야 하므로 ❶과 ❷를 더한 5분 0.003초 이내가 된다. 유형 1의 경우는 약 5분 5.204초 이내 탐지되는 것으로 예측되었다.

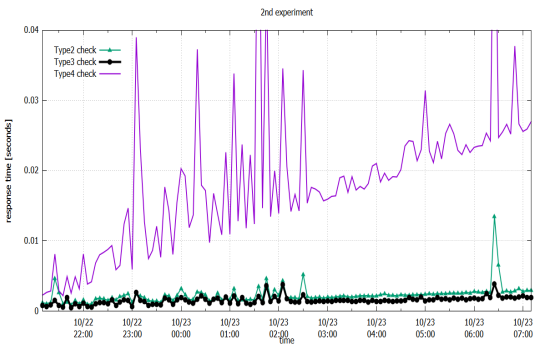

Fig. 15. Detection Time for Multi-homed host Type 2~4

4) 결정계수는 1에 가까울수록 신뢰도가 높다.

Table 5. Estimated Detection Time for Multi-homed Host Type 1, 3 When the Execution Cycle of Central Server is 5 minutes(❷)

Num of Executions (Elapsed Time)	Central Server (Table records)	Estimated Detection Time❶ (seconds)	
		Type 1	Type 3
1st (00:05)	2,000	0.535431194	0.001454529
2nd (00:10)	4,000	1.313667886	0.001836251
3rd (00:15)	6,000	2.091904577	0.002217972
4th (00:20)	8,000	2.870141269	0.002599694
5th (00:25)	10,000	3.648377961	0.002981416
6th (00:30)	12,000	4.426614652	0.003363138
7th (00:35)	14,000	**5.204851344**	**0.003744860**
8th (00:40)	16,000	5.983088036	0.004126582

5.6 평가

본 연구에서는 망혼용단말의 유형을 정의하고, 기존 탐지방법에 대한 개선사항을 도출 및 구현하여 실제 환경과 유사한 가상환경에 적용해봄으로써 실제의 작동기능과 성능을 확인하였다. 망혼용 유형을 순차적으로 유발시켜보고 탐지여부를 확인하였다. 탐지방식은 단말정보 저장 후 MAC 주소 비교와 같은 단순한 프로세스로 본 연구 환경하에서는 오탐과 미탐을 발견할 수 없었다. 또한, 본고에서 제시한 망혼용단말 탐지시스템의 모델은 단말로부터의 해킹위험을 최소화하기 위한 일방향 통신(SYSLOG, UDP 사용), 별도의 로그망 설계시 인접망으로부터 수신만 되고 타 망으로의 이동이 불가한 구조, 기존 망혼용단말 탐지솔루션이 탐지하지 못하는 가상머신을 이용한 유형 3 탐지가 가능하다는 데 의의가 있다. 또한, 본 연구에서 개발한 Agent는 사용자 영역(User level)에서 작동하여 시스템 가용성에 영향을 미치지 않으므로 서버에 설치가 가능하다. 이로서, 가용성이 중요한 서버에도 Agent가 설치되면 서버군에 존재하는 모든 망혼용단말을 적시에 탐지할 수 있을 것이다. 결국, 서버군의 망혼용단말을 경유한 침해사고를 예방할 수 있을 것이다.

VI. 토론 이슈

본 연구에서는 망혼용단말 유형 1~3까지를 MAC, 가상머신 사용 여부 등 기본 정보를 바탕으로 식별하였다. 향후에는 Table. 6 의 예시처럼 식별방식을 세분화하여 평가기준식을 마련할 필요성이 있다. 또한, Agentless 방식의 시각편차 기법을 혼합하여 사용하는 방법도 고려해 볼 수 있을 것이다.

본 연구에서는 기본적인 탐지기능의 효과성을 확인하고자 최적화된 시스템을 설계하지는 않았다. 성능개선을 위해 호스트를 유일하게 구분 짓기 위한 방법(CPU ID, CMOS UUID, HDD Serial 등) 활용, 불필요한 로깅 최소화 및 저장 프로시저 활용 등 최적화 방안이 마련되어야 할 것이다.

또한, 사용자 임의로 망혼용단말 Agent를 삭제할 수 있으므로 별도의 보호조치가 필요할 것이다. 사용자 단말의 망혼용단말 Agent는 NAC의 기능을 통해 삭제·변조를 보호하고, 서버군에 설치된 Agent는 각 망에 설치된 별도의 트래픽모니터링시스템 등을 활용할 수 있겠다. 네트워크 활동은 하지만 로컬서버로 NIC정보가 수집되지 않는 단말을 식별하여 운영유무를 점검할 수 있을 것이다. 예를 들면, 각 망의 백본스위치에서 트래픽모니터링시스템으로 패킷 미러링하거나 Netflow 정보를 전송하도록 하고, 트래픽모니터링시스템에서는 수집된 네트워크활동 단말정보를 로컬서버로 전송한다. 로컬서버에서는 ①네트워크 활성화된 단말과 ②NIC정보가 수집되고 있는 단말을 비교하여 NIC 정보가 수집되고 있지 않는 단말(망혼용Agent의 미설치/미작동 단말)을 식별하여 중앙서버에Alert 정보로 전송할 수 있을 것이다.

마지막으로 기존 인가된 단말에서 사용되던 NIC을 다른 단말에서 사용할 경우의 작동방식에 대해 알아본다. Fig. 7에서 정상적으로 사용되던 Jeff 의 NIC을 분리하여 Brian Cornell 단말에 장착할 경우, Jeff의 기존 MAC 사용이력이 중앙서버에 기록되어있기 때문에 조직 내 어떤 단말에서 사용하더라도 기존 정보와 비교되어 검출되게 된다. Jeff 단말이 인터넷망에서 사용되고 있을 때 NIC을 떼어 업무망 Brian 단말에 장착하면 망혼용유형1로 탐지되고, 5.3.1의 실험시나리오 1을 수행한 이후(업무망에서도 사용) Jeff 의 단말을 떼어내어 Brian Cornell 단말에 장착하면 다중 NIC 사용으로 망혼용유형2로 탐지된다. 만약, Brian Cornell에서 사용되던 NIC을 제거하고 Jeff의 NIC을 장착하면 기존 MAC 사용

이력과 비교되어 OS명· Hostname 은 동일한데 MAC이 다르므로 MAC Spoofing 된 망혼용유형4로 탐지된다.

VII. 결 론

본 연구에서는 망혼용단말의 위험성과, 이를 완전히 제거하는 것의 어려움을 살펴보았다. 이에 대한 대안으로 망혼용단말을 적시에 자동으로 탐지하여 관리자에게 통보해주는 시스템이 필요하다. 그러나 현재까지 구현된 방식으로는 NIC 2개 이상을 사용한 단말탐지가 제한적이고, NIC 1개를 가상머신에 연동하여 사용하는 다중OS 환경의 단말 또한 탐지할 수 없음을 알아보았다. 본 연구에서는 해결방안으로 다중OS 환경의 망혼용단말 등 NIC 2개 이상 사용단말을 탐지할 수 있는 자동탐지시스템을 설계, 구현하여 효과를 확인하였다.

이러한 자동탐지시스템을 운영할 경우 망혼용단말을 경유한 해킹위협을 적시에 제거할 수 있을 것이다. 향후 연구 방향으로는 VMWare, Virtual PC 등 더 많은 가상화 SW 지원, 중첩 가상화 단말(Nested Virtual Machine)의 정보 수집, Multi Boot 환경에서의 타 OS 네트워크 설정 확인, 아웃바운드 트래픽에 대한 패킷조사로 폐쇄망 단말의 포함여부를 조사[23]하는 등 망혼용단말 사각지대를 최소화하기 위한 방안도 연구되어야 할 것이다.

References

[1] Kyung-bok Lee, "Security Threats and Countermeasures according to the Environmental Changes of Smart Work", Journal of Digital Convergence, 9(4), p. 30, 2011.

[2] Yonhap News, http://www.yonhapnews.co.kr/bull etin/2016/12/06/0200000000AKR20161206117900014 .HTML, Dec. 2016.

[3] Reuters, https://www.reuters.com/article/us-usa- fed-bangladesh/bangladesh-bank-exposed-to-hackers-by-cheap-switches-no-firewall-police-idUSKCN0XI1UO, April. 2016.

[4] Kyoung-gon Kim, "State-Sponsored Hacker and Changes in hacking techniques", NetSec-KR 2017, April. 2017.

[5] Asia Economy, http://www.asiae.co.kr/news/vie w.htm?idxno=2015091713570518605, Sep. 2015.

[6] T. Kohno, A.Brioido, and K. C. Claffy, "Remote physical device fingerprinting," IEEE Transactions on Dependable and Secure Computing, vol. 2, pp. 93-108, 2005.

[7] Martin, Bryan J, "Detecting a multi-homed device using clock skew", Calhoun(Institutional Archive of the Naval Postgraduate School), pp. 2-4, Sep 2016

[8] NIST SP800-82 Rev2, "Guide to Industrial Control Systems (ICS) Security", pp. 5-7, May 2015.

[9] Barrigas, Jorge Filipe, "Security Probes for Industrial Control Networks", Universidade de Coimbra, pp. 8-9, 2014.

[10] "Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies", p. 24, Sep. 2016.

[11] Stephen Northcutt, "Inside Network Perimeter Security" 2nd Edition, SANS INSTITUTE, p. 311, p. 331, Mar. 2005.

[12] JinGuk-Um, "Model Proposal for Detection Method of Cyber Attack using SIEM", The journal of the institute of internet, broadcasting and communication, 16(6), pp. 43-54, Dec. 2016.

[13] L. Polcak, "Comment on Remote Physical Device Fingerprinting", IEEE Transactions on Dependable and Secure Computing, vol.11, pp. 494 - 496, Oct. 2014.

[14] Hyoung-jin Jo, "Detection of Unauthorized Internet Access Nodes in Financial Closed Network Environments", Korea University, 2015.

[15] E. Byres, https://www.tofinosecurity.com/blog/ dual-homed-machines-are-juiciest-targets, Tofino Security, 2010.

〔16〕 Oracle Virtuabox User Manual - VBoxManage guestproperty https://www.virtualbox.org/manual/ ch08.html#vboxmanage-guestproperty, 2017.
〔17〕 Performing common virtual machine-related tasks with command-line utilities (2012964), https://kb.vmware.com/s/article/2012964, 2012.
〔18〕 Listing all the IP Addresses used by VMs, https://blogs.msdn.microsoft.com/virtual_pc_guy/2014/04/18/listing-all-the-ip-addresses-used-by-vms/, Apr. 2014.
〔19〕 J. Ahrenholz "Core: A realtime network emulator,"MILCOM 2008. IEEE, pp. 1-7, Nov. 2008.
〔20〕 B. Lantz "A network in a laptop: rapid prototyping for software-defined networks" 9th ACM SIGCOMM, p. 19, Oct. 2010.
〔21〕 Y. WANG and J. WANG, "Use gns3 to simulate network laboratory," Computer Programming Skills & Maintenance, vol. 12, pp. 113-114, 2010.
〔22〕 Denis Salopek, "A network testbed for commercial telecommunications product testing", IEEE SoftCOM, p. 373, 2014.
〔23〕 Chul-won Lee, "A Study on Analysis and Control of Circumvent Connection to the Private Network of Corporation", Journal of the Korea Institute of Information Security and Cryptology, 20(6), pp. 183-194, Dec. 2012.

〈저자소개〉

이 미 화 (Mi Hwa Lee) 정회원
2002년 2월: 공주대학교 대기과학과 졸업
2004년 6월~2007년 6월: 한국전자통신연구원 부설 국가보안기술연구소
2007년 12월~현재: 한전KDN(주) 과장 산업통상자원사이버안전센터 근무
2018년 2월: 고려대학교 정보보호대학원 석사 졸업
〈관심분야〉 침해사고분석, 위협사냥, 위협모델링, 망분리 보안

윤 지 원 (Ji Won Yoon) 종신회원
2003년 2월: 성균관대학교 정보공학사 졸업
2005년 2월: University of Edinburgh, 정보학과 석사 졸업
2008년 11월: University of Cambridge 전자공학과 박사 졸업
2008년 2월~2009년 5월: University of Oxford, 로봇연구소 박사후과정
2009년 5월~2011년 5월: University of Dublin 통계학과 연구원 및 강사
2011년 7월~2012년 8월: IBM 연구소 정규 연구원
2012년 9월~2016년 2월: 고려대학교 정보보호대학원 조교수
2016년 3월~현재: 고려대학교 정보보호대학원 부교수
〈관심분야〉 신호정보처리, 응용통계, 빅데이타 분석 기술, 도감청 탐지기술