Journal of The Korea Society of Computer and Information
Vol. 22 No. 10, pp. 83-92, October 2017

www.ksci.re.kr
https://doi.org/10.9708/jksci.2017.22.10.083

Analysis of Threat Model and Requirements in Network-based Moving Target Defense

Koo-Hong Kang*, Tae-Keun Park**, Dae-Sung Moon***

Abstract

Reconnaissance is performed gathering information from a series of scanning probes where the objective is to identify attributes of target hosts. Network reconnaissance of IP addresses and ports is prerequisite to various cyber attacks. In order to increase the attacker's workload and to break the attack kill chain, a few proactive techniques based on the network-based moving target defense (NMTD) paradigm, referred to as IP address mutation/randomization, have been presented. However, there are no commercial or trial systems deployed in real networks. In this paper, we propose a threat model and the request for requirements for developing NMTD techniques. For this purpose, we first examine the challenging problems in the NMTD mechanisms that were proposed for the legacy TCP/IP network. Secondly, we present a threat model in terms of attacker's intelligence, the intended information scope, and the attacker's location. Lastly, we provide seven basic requirements to develop an NMTD mechanism for the legacy TCP/IP network: 1) end-host address mutation, 2) post tracking, 3) address mutation unit, 4) service transparency, 5) name and address access, 6) adaptive defense, and 7) controller operation. We believe that this paper gives some insight into how to design and implement a new NMTD mechanism that would be deployable in real network.

▸Keyword: Moving target defense, Network address mutation, Internet security

I. Introduction

해커들은 실질적인 공격에 앞서 상당히 긴 시간을 투자해 자신들이 공격할 목표 시스템에 대한 상세한 정보 수집과 함께 취약점 분석에 따른 구체적인 공격 방법을 마련한다[1]. 이와 같은 정찰(reconnaissance) 단계는 공격자의 업무부하(workload)의 95%를 차지하는 것으로 조사되고 있다[2]. 반면, 이들 해커들의 공격으로부터 자신을 방어하는 일반 시스템들은 공격을 당하는 시점부터 해당 공격에 대응해야 하는 시간적 비대칭성에 고전하고 있다. 이러한 시간적 비대칭성을 일부 극복하기 위해 방어 시스템들은 자신의 다양한 시스템 특징들을 시간의 변화에 따라 역동적으로 변경시키는 사이버 무빙 타켓 방어 (MTD: moving target defense) 기술을 도입하여 해커들의 공격 부담을 가중시키는 전략을 도입하고 있다[1].

사이버 MTD 기술은 컴퓨터 시스템에서 변경시킬 수 있는 모든 것을 포함하고 있다. 즉 IP 주소를 변경시키거나 메모리 레이아웃을 무작위화 시키거나 혹은 메모리 내 콘텐츠를 암호화시키기도 한다. 이들 MTD 기술들을 소프트웨어 스택 모델을 이용하여 주요 도메인별로 분류할 수 있다. 예를 들어, 네트워크 특징 및 설정을 변경하는 네트워크 기술, 시스템의 플랫폼 특징을 변

• First Author: Koo-Hong Kang, Corresponding Author: Koo-Hong Kang
*Koo-Hong Kang (khkang@seowon.ac.kr), Dept. Information and Communications Eng., Seowon University
**Tae-Keun Park (tkpark@dankook.ac.kr), Dept. of Applied Computer Eng., Dankook University
***Dae-Sung Moon (daesung@etri.re.kr), Information Security Research Division, ETRI
• Received: 2017. 08. 30, Revised: 2017. 09. 08, Accepted: 2017. 09. 25.
• This work was supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIT) (No.2017-0-00213, Development of Cyber Self Mutation Technologies for Proactive Cyber Defense).

경시키는 플랫폼 기술, 런타임 환경을 변경시키는 런타임 기술, 응용 코드를 변경시키는 소프트웨어 기술, 그리고 데이터의 포맷과 표현을 변경시키는 데이터 기술 등이 있다 [1]. 본 논문에서는 이와 같이 매우 광범위한 사이버 MTD 기술 중에서 DARPA의 Information Assurance (IA) 프로그램[2,3]을 통해 처음으로 시도되었던 해커가 수집한 공격 대상 호스트의 네트워크 정보들을 무력화시키는 네트워크-기반(Network-based) MTD (NMTD) 기술에 초점을 맞춘다. 즉 호스트의 IP 주소 및 포트 번호를 시간에 따라 역동적으로 변경시킴으로써 해커들의 공격 부담을 증가시키는 기술에 집중한다.

현재 국외 NMTD 기술개발 현황으로는, 기존 네트워크 인프라를 기반으로 구현하는 방법[2,3,4,5,6,7]과 software-defined networking(SDN)을 기반으로 구현하는 방법[8,9,10]이 연구되고 있다. IP 패킷 포워딩 하드웨어(forwarding hardware)로부터 제어플랜(control plane)을 분리시킨 새로운 네트워크 패러다임인 SDN은 자유로운 라우팅과 패킷 헤더 변환이 가능함에 따라 NMTD 기술로의 활용이 여러 연구에서 검토되었다. 그러나 SDN 활용에는 보다 신중한 접근이 필요하다. 왜냐하면 기존 네트워크 인프라 전체를 교체해야하는 경제적 부담과 SDN이 대규모 네트워크에 적용된 성공적인 사례가 아직은 보고된 바가 없기 때문이다. 따라서 본 연구에는 기존 네트워크 인프라와 TCP/IP 프로토콜을 그대로 활용한 NMTD 기술 개발에 집중한다. 즉, 본 연구는 기존 네트워크 인프라에서 보호대상 호스트의 IP 주소 및 포트 번호를 시간의 변화에 따라 지속적으로 무작위(randomization) 혹은 변이(mutation)하여 공격자의 정찰 단계에서 획득한 정보를 무력화시키는 NMTD 기술 분야에 한정한다.

SDN을 활용하지 않고 기존 네트워크 인프라에서 진행된 NMTD 관련 국외 기술 개발 현황을 살펴보면, 우리의 예상과는 달리 매우 제한적인 연구 결과들만 확인할 수 있다. NMTD 기술의 필요성에 비추어 볼 때, 주요 연구 결과는 여섯 개의 수준으로 매우 부족한 면이 있다. 뿐만 아니라, 실험실 수준을 넘어서 실제 네트워크에 적용된 사례를 찾아보는 것은 불가능한 실정이다. 여기에는 여러 가지 이유가 있을 수 있지만, SDN 기술을 사용하지 않고 기존 네트워크 인프라에서 호스트의 IP 주소 및 포트 번호를 시간의 변화에 따라 역동적으로 변화시키는 것이 기술적으로 여러 가지 어려움이 동반되기 때문이다. 본 논문에서는 기존 네트워크 인프라에서 활용 가능한 NMTD 기술의 개발을 위해, 기존 기술들에 대한 문제점들을 분석하고 위협 모델을 정립한 후, 실제 네트워크에서 가용한 시스템을 개발을 위한 요구사항 분석 및 개발 전략을 기술 항목 별로 마련하고 기존의 MTD 기술의 평가를 제시된 기술 항목으로 충족 여부를 판단한다. 또한 제시된 기술 항목들은 NMDT 기술 개발을 위해 노력하는 개발자들에게 다양한 영감을 줄 것으로 기대한다.

서론에 이어, 제2장에서는 SDN을 활용하지 않고 기존 네트워크 인프라에서 진행된 NMTD 관련 기존 기법들에 대해 간략히 언급하고, 제3장에서는 이들 기법들이 실제 네트워크에 적용되어 사용되기 위해서 반드시 해결해야할 문제점들을 분석하였다. 제4장에서는 NMTD 연구의 필요성 및 정당성을 뒷받침할 위협모델을 제시하였다. 제5장에서는 NMTD 개발을 위해 선행되어야할 필수적인 시스템 개발 요구 사항들을 제시하고, 마지막으로 제6장에서 결론을 맺는다.

II. Related Works

SDN을 활용하지 않고 기존 네트워크 인프라에서 진행된 NMTD 관련 연구는 [표 1]과 같다. 서론에서 언급한 바와 같이 우리의 예상과는 달리 소수의 연구 결과들만 확인할 수 있다. 본 장에서는 이들 기존 기법들의 동작 원리를 간략히 정리하고 실제 네트워크에 이들 기법들을 적용할 때 고려해야할 문제점들은 다음 장에서 자세히 다루기로 한다.

Table 1. Example of mechanisms for network address randomization in the legacy TCP/IP network

Scheme	ref
DYNAT (Dynamic Network Address Translation)	[2]
APOD (Application that Participate in their Own Defense)	[3]
NASR (Network Address Space Randomization)	[4]
RHM (Random Host Mutation)	[5]
DESIR (Decoy-Enhanced Seamless IP Randomization)	[6]
HIDE (Host IDEntity anonymization)	[7]

DYNAT[2]은 패킷이 네트워크의 공중망 ([그림 1]의 WAN)으로 진입할 때 TCP/IP 패킷 헤더 내 호스트 확인자(identity)를 모호(obfuscating)하게 만든다. 호스트 확인자는 두 호스트 사이 네트워크 연결을 결정하는 헤더 내 주소 정보를 의미한다. [그림 1]에서, 클라이언트 호스트가 전송하는 패킷의 목적지 주소 정보는 DYNAT shim에 의해 변환된다. 주소 정보 변환에 사용되는 알고리즘으로, 시간에 따라 변화하는 미리 설정된 키 값(keying parameter)에 의존적으로 동작하는 암호화 알고리즘이 적용되었다. [그림 1]에서, 수신 단에 있는 서버 DYNAT gateway는 원래 목적지 호스트 확인자 정보를 획득하기 위해 패킷 헤더 내 암호화된 주소 정보를 역-변환한다. 결과적으로, 공중망에 위치하는 공격자들은 해당 서버의 실제 주소가 아닌 시간에 따라 변화하는 암호화된 주소 정보만 확인할 수 있게 된다.

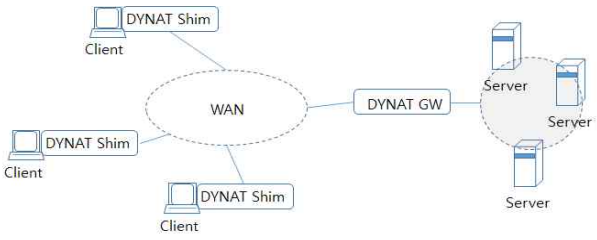

Fig. 1. DYNAT architecture

[그림 2]는 APOD[3]의 주요 요소들을 보여준다. 송신지와 목적지 호스트가 동일한 네트워크 세그먼트에 존재하면 포트 호핑(hopping)을 수행하고 서로 다른 세그먼트에 존재하는 경우는 포트와 주소 호핑을 동시에 수행한다. 그림에서 보듯이 호핑 기법은 hopping delegate라고 불리는 클라이언트 요소와 서버 쪽의 NAT gateway에 의해 구현된다. Hopping delegate는 클라이언트 호스트에 클라이언트 프로세스 형태로 직접 위치하여 실제 서버를 호출하는 콜을 가로채어 실제 주소 <realaddress : realport> 헤더 정보를 위장 주소 <fakeaddress : fakeport>로 변환한다. 한편 서버에 존재하는 NAT gateway는 <fakeaddress : fakeport>를 <realaddress : realport>로 역-변환한다. 이때 <fakeaddress : fakeport> 쌍은 가용한 IP 주소와 포트 범위 내에서 무작위(RNG: Random Number Generator)로 선택한다. 이러한 변환 주소는 일정 시간 사용되고 다시 새로운 주소가 무작위로 선택된다.

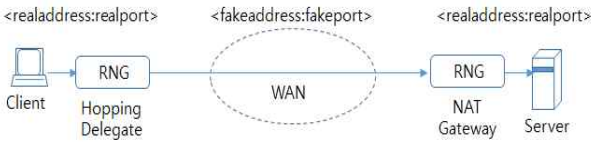

Fig. 2. Port and address hopping architecture

NASR[4]은 클라이언트-서버 통신을 수동적으로 감청(passively listen)하는 공격자보다는 스캐닝 등으로 사전에 작성된 웜 히트리스트 (worm hitlist)를 기반으로 하는 공격자에 대한 방어에 초점을 맞춘 프로액티브 방어 기법 (proactive defense mechanism)이다. NASR은 DHCP[11]로부터 동적으로 주소를 할당받는 호스트를 대상으로 구현되었으며 적절한 시간 간격마다 호스트에 할당된 DHCP 주소 임대 (leases)를 종료한 뒤 새로운 주소를 임대하는 형태로 주소 변이를 구현하였다. 표준화된 DHCP 서버는 호스트가 주소 임대 만료 전에 주소 갱신을 요청하는 경우에 주소 임대를 갱신한다. 이에 반하여 NASR에서는 주소 임대가 만료되기 전에 호스트가 DHCP 서버에게 주소 갱신을 요청하면 DHCP 서버가 새로운 주소를 할당할 수 있도록 수정되어야 한다. NASR의 저자들은 ISC open-source DHCP 구현을 기반으로 Wuke-DHCP라고 불리는 NASR-enabled DHCP 서버를 개발하였다.

RHM[5]은 기존의 기법들이 공격자에게 충분한 불예측성(unpredictability)를 제공하지 못할 뿐만 아니라 공격 패턴에 적응적인(adaptive) 변이 기법을 제공하지 못한다는 문제를 해결하기 위하여 제안되었다. RHM은 높은 불예측성을 제공하기 위하여, LFM (low frequency mutation)과 HFM (high frequency mutation)을 사용한다. LFM은 각 호스트에 할당될 수 있는 IP 주소의 범위 (unused address block)를 바꾸는 변이이며([그림 3]의 mutation controller(MC)가 담당), HFM은 LFM에 의해 할당된 IP 주소의 범위 내에 속하는 IP 주소 하나를 각 호스트에 ephemeral IP (eIP)로 할당하는 변이이다([그림 3]의 mutation gateway(MG)가 담당). 한편, 공격 패턴에 적응적으로 반응하기 위하여, RHM은 공격자의 실패한 프로브(probe)들이 non-uniform 또는 non-repetition 패턴에 속하는지 분석한다. 만일 이상의 두 가지 패턴 중 하나에 속한다고 판단되면, RHM은 실패한 프로브와 관련된 IP 주소 범위에 컴퓨터가 할당되지 않도록 조절한다.

DESIR[6]는 다음 [그림 4]와 같이 클라이언트, 인증 서버(authentication server), 서버 풀 (server pool), 디코이 베드(decoy bed), RC (randomization controller) 라는 다섯 개의 주요 컴포넌트로 구성된다. RC는 구성 정보 세팅 ([그림 4]의 <configuration settings>)을 통해 서버 풀에 새로운 IP 주소를 할당하고 decoy bed에 새로운 설정 값 (decoy IP 주소, MAC 주소, 운영체제, 그리고 애플리케이션)을 바꿀 수 있다. RC는 이러한 구성 정보 세팅을 주기적으로 반복함으로써 DESIR이 추구하는 MTD를 수행한다. RC의 구성 정보 세팅에 의하여 새로운 IP 주소를 할당받은 서버는 해당 주소를 인증서버의 주소 데이터베이스를 갱신 ([그림 4]의 <IP address updates>)한다. 이러한 주소 등록을 위한 교환 메시지는 암호화되어 전달됨으로써 공격자가 확인할 수 없다. 그 결과, 인증서버는 모든 서버의 최신 IP 주소들을 유지하게 되며, 클라이언트가 서버에 접근하고자 할 때 인증 서버가 클라이언트에 대한 인증을 수행한 후에 해당 서버의 현재 IP 주소를 전달할 수 있게 된다. 클라이언트와 서버가 연결을 유지하고 있는 상황에서 RC의 구성 정보 세팅에 의해 IP 주소가 바뀌게 되면, 서버와 클라이언트는 암호화된 방식으로 바뀐 IP 주소의 정보를 교환함으로써 연결 이관 (connection migration)을 수행한다.

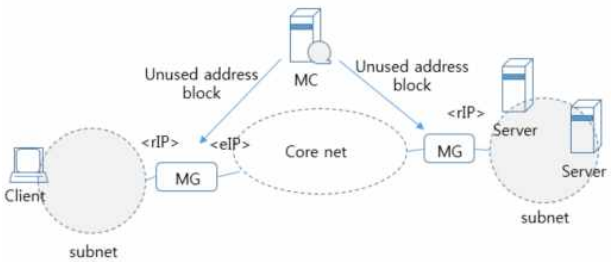

Fig. 3. RHM architecture

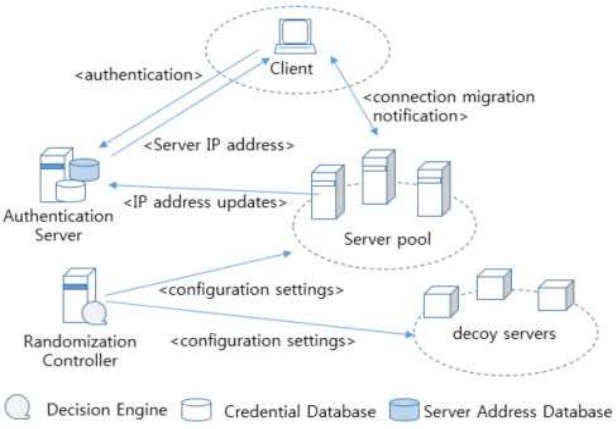

Fig. 4. DESIR architecture

HIDE[7]는 RHM을 확장한 방법으로, 기존 기법들이 자동화된 스캐닝 또는 웜(worm)에 대한 프로액티브 방어 기법 (proactive defense mechanism)으로 적합할 수는 있지만 전문적인 지식을 소유한 공격자에 대해서는 효율적이지 못하다는 사실에 기반하여 제안된 방어 기법이다. HIDE의 핵심 아이디어는 (1) 호스트 주소 변이, (2) 호스트 핑거프린트 변이, (3) 호스트 핑거프린트 익명화 (anonymization), (4) 허니팟(honypot) 배치, (5) honeypot에 context-aware content 배치를 통합 사용함으로써 지능적인 공격자의 정찰이 원활하게 이루어지지 않도록 하는 것이다.

[그림 5]는 TCP/IP 엔터프라이즈 네트워크에 HIDE 모델이 적용될 때의 네트워크 구조를 보여준다. [그림 5]에서 컨트롤러는 네트워크 호스트에 대한 변이를 결정하고, 결정된 변이를 서브넷의 물리적인 경계 (서브넷 스위치와 기본 라우터 사이)에 위치한 mutation gateway(MG)에 통지하는 역할을 담당한다. MG는 network address and port translation(NAPT) 디바이스와 유사한 역할을 수행하는데, 구체적으로는, controller가 통지한 새로운 변이에 따라 송수신되는 패킷의 IP 주소, port 번호 등을 변경하는 역할을 수행한다. HIDE의 또 다른 특징은 허니팟을 운영하는 것이다. 만일 공격자가 실존하지 않는 IP 주소나 포트 번호로 접속을 시도하면, HIDE 모델에서는 해당 Flow가 허니팟으로 전달 ([그림 5]의 flow redirection)되도록 한다. 예를 들어, 실존하지 않는 IP 주소인 IPrand의 포트 80번으로 접속을 시도하면, 허니팟 클라우드에 속한 웹 허니팟에게 해당 패킷이 전달되도록 하여, 공격자로 하여금 IPrand가 웹 서버에 의하여 실제 사용 중인 것으로 오인하도록 유도한다. 공격자가 동일한 IP 주소를 이용하여, 포트 21번으로 접근하면 이 패킷을 허니팟 클라우드에 속한 또 다른 FTP 허니팟에게 전달함으로써 FTP 서비스도 제공되는 것으로 오인하도록 유도한다.

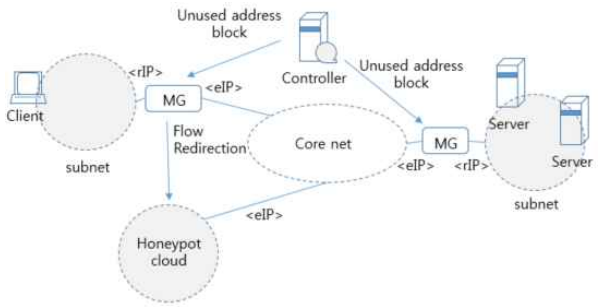

Fig. 5. HIDE architecture

III. Challenging Problems for the Network-based MTD Deployments

1. DYNAT

NYNAT[2]는 패킷의 정상적인 라우팅을 위해 목적지 IP 주소에서 NetID 부분을 제외한 HostID 부분과 목적지 포트번호를 변이시킨다. 이러한 주소 변이는 [그림 6]에서 보듯이 클라이언트와 서버가 설정한 초기 비밀 seed 값과 암호 (cryptographic) 알고리즘에 의해 수행된다. 클라이언트와 서버는 wall-clock을 이용해 변이 비밀 값 변경 시점을 동기화한 뒤, 변이 구간 (mutation interval)마다 비밀 값을 변경한다. [그림 6]에서, 클라이언트가 송신하는 패킷의 헤더 정보 내 목적지 서버의 IP 주소에서 호스트 ID와 포트번호 <rDstIP.hostID:rDstPort>는 DYNAT Shim에 의해 암호화를 거쳐 <eDstIP.hostID:eDstPort>로 변환되고 수신단 DYNAT Gateway는 복호화를 통해 원래의 주소 정보를 복구한다.

암호화 키 값 생성을 위해 두 개의 파라미터 즉 UNIX epoch 시간과 초기 seed 값을 이용하였다. [그림 1]과 같이 여러 개의 클라이언트 DYNAT shim과 gateway가 wall-clock으로 동기화되어 있고 동일한 초기 seed 값을 공유한다면 변이 구간 동안 모두 동일한 키를 사용하게 된다. 따라서 매 변이 구간마다 시간적으로 동기화된 하나의 키 값에 의해 암호화되기 때문에 모든 서버 확인자 (identity)들이 동시에 일괄적으로 변화하게 된다. 이 때문에, 공격자들은 트래픽 모니터링을 통해 서버에 연결 중인 클라이언트 확인자를 기준으로 주기적으로 변이되는 목적지 서버 확인자들을 계속 추적할 수 있게 된다. 본 논문에서는 이러한 특징을 후위 트래킹 (post tracing)이라고 칭한다. 즉 공격자는 암호화된 서버 주소를 미리 예측할 수 없으나 발신지 주소를 기준으로 이들 서버 주소들이 어떻게 변화되었는지 추적할 수 있게 된다. 결과적으로, 특정 서버에 대한 공격자들의 다양한 정찰을 통해 해당 서버에 대한 지속적인 정보 수집과 연관성 분석이 가능해 진다. 한편, 연결 단위 혹은 클라이언트 단위로 암호화 키를 사용하지 않기 때문에 DYNAT가 실제 네트워크에 적용되기 위해서는 키 관리(key management)에 대한 구체적인 전략이 선행되어야 한다.

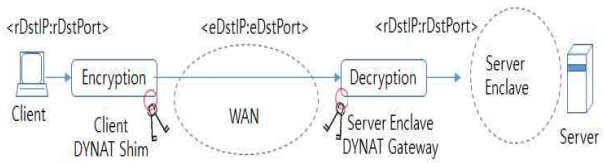

Fig. 6. DYNAT mutation technique

DYNAT 기술은 주소 변환을 이용한 MTD 기술로 보호할 서버들을 하나의 서브넷(server enclave)에 모은 뒤 DYNAT Gateway를 설치하여 이들 각각의 서버들의 주소 변환을 대행한다. 따라서 각 서버에 설정된 네트워크 주소 및 오픈된 포트번호는 MTD 기술과는 무관하게 고정적으로 유지되며, 기존 서비스들은 아무런 수정 없이 지속적으로 사용 가능해진다. 그러나 서버들의 서브넷 내([그림 6]의 server enclave)에서는 서버에 설정된 실제 IP 주소 및 오픈 포트 번호가 모두 노출되기 때문에, 서버가 위치한 서브넷 내에 침투한 공격자로부터 해당 서버들을 보호할 전략이 필요하다. 뿐만 아니라, 주소 변환을

수행하는 전용 장비를 네트워크에 설치 및 운영해야 하는 부담은 가장 큰 단점으로 지적된다.

2. APOD

포트 호핑은 클라이언트 hopping delegate의 RNG(Random Number Generator)에 의해 시간에 따라 무작위로 선택된 서버 쪽 포트 번호로 터널링하여 전달한다 ([그림 2] 참조). 이때 서버에 위치한 터널링 에이전트의 RNG는 클라이언트 RNG와 동기화되어 있다. [그림 7]에서 보듯이, 일반적으로 하나의 서버에는 여러 개의 서버 프로그램이 동작 가능하며 하나의 클라이언트 역시 동시에 여러 서버에 접근할 수 있다. 예를 들어, 하나의 클라이언트 내 여러 클라이언트 프로그램이 하나의 서버의 여러 서버 프로그램에 접근할 수 있다 ([그림 7]의 클라이언트 A와 서버 A 참고). 이때 포트 호핑을 위한 하나의 RNG 만을 이용해 클라이언트와 서버들이 이들 포트를 구분하는 것은 사실상 불가능하다. 또한 [그림 7]에서 클라이언트 B의 클라이언트 프로그램 A1과 A3의 경우, 서로 다른 서버 A와 서버 B에 연결된다. 따라서 모든 RNGs 들이 동기화 되어야 한다. 이러한 동기화는 여러 클라이언트에서 하나의 서버로 접근하는 경우도 동일하다([그림 7] 클라이언트 A와 B의 클라이언트 프로그램 A1과 서버 A의 서버 프로그램 A1). 즉 클라이언트 A와 B, 그리고 서버 A의 RNGs가 모두 동기화 되어야 한다. 결국, APOD는 동시에 여러 클라이언트 프로그램들이 복수의 서버에 접근하기 위해서는 보다 정교한 RNG 운영 전략이 제시되어야 한다.

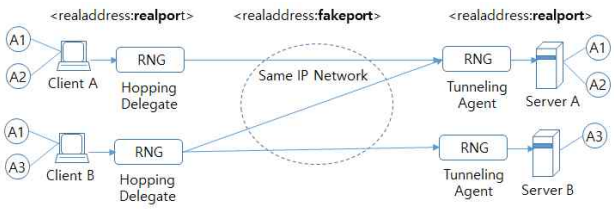

Fig. 7. An example of the APOD deployment

APOD는 앞에서 설명한 DYNAT와 매우 유사하게 NAT 게이트웨이를 사용한다. 따라서 '후위 트래킹' 및 'NAT 변환 전용 장비 운영'의 문제점을 그대로 가지게 된다. 하지만, DYNAT와 비교해 APOD는 호핑이라는 방법을 사용하며 포트 호핑을 통해 서브넷 내에 존재하는 공격자에게 서버의 포트번호를 위장하는 효과가 있다.

3. NASR

NASR은 빈번한 IP 주소 변경을 위하여, 동적으로 네트워크 주소 할당 서비스를 제공하는 DHCP 서버의 수정을 필요로 한다. NASR을 위하여 수정된 DHCP 서버인 NASR-enabled DHCP 서버는 기본적인 DHCP 서버 기능 이외에 AMM (activity monitoring module)과 SFM (service fingerprinting module)의 기능을 추가적으로 수행한다. AMM은 각 컴퓨터에서 사용 중인 연결 (예: TCP 연결)이 주소 변경으로 인해 끊어지는 등의 서비스 중단이 발생하지 않도록 현재 사용 연결을 모니터링하는 기능을 담당하며, SFM은 각 컴퓨터에서 제공되고 있는 서비스 종류를 파악하는 기능을 담당한다.

주소 변이를 위하여 NASR-enabled DHCP 서버는 refresh 타이머, soft-change 타이머 및 hard-change 타이머를 사용한다. Refresh 타이머는 서버에 대한 클라이언트의 IP 주소 요청을 강제하기 위한 타이머이며, soft-change 타이머는 AMM에 의하여 사용 중인 연결이 존재하지 않는다고 보고된 컴퓨터의 IP 주소의 변경 주기를 알려주는 타이머이다. 마지막으로, hard-change 타이머는 사용 중인 연결이 존재하더라도 클라이언트의 IP 주소를 무조건 변경해야 하는 주기를 알려주는 타이머이다. 그러나 이상과 같은 NASR의 주소 변이 정책은 연결을 장시간 유지 (long-lived connection)하는 호스트의 경우 긴 시간동안 주소 변이가 이루어지지 않음에 따라 다른 호스트에 비하여 공격자에게 쉽게 노출될 수 있도록 한다. 결국, 여러 클라이언트들과의 연결들이 장시간 유지되어야하는 서버의 경우에는 NASR 적용이 사실상 불가능하다고 판단된다. 따라서 Antonatos et al.[4]가 언급한 바와 같이 NASR은 단순히 웜 히트리스트에 근거한 웜의 전파를 방해하는 수준에서 사용될 수 있을 것이다. 뿐만 아니라, 이러한 히트 리스트를 기반으로 출현된 웜의 종류가 아직 보고된 바가 없어 NASR의 위협 모델의 타당성이 다소 부족하다.

빈번한 IP 주소 변경을 활용하는 프로액티브 방어 기법의 효과를 극대화하기 위해서는 IP 주소 풀(pool)의 크기를 최대화하여야 하는데, 글로벌 IP 주소 전체에 대하여 NASR을 적용하기에는 라우팅 테이블 업데이트 비용, 주소 변이 결정 비용 및 글로벌한 협력 필요 등의 어려움이 너무 크다고 알려져 있다[4]. 따라서 NASR의 저자들은 자신들이 조사한 ISP의 경우 서브넷의 95%에서 사용중인 IP 주소의 비율이 50%가 넘지 않는다는 사실에 근거하여 NASR을 서브넷 단위로 적용할 것을 제안하였다. 하지만 국내의 경우, 대부분의 기관들이 충분한 공인 IP 주소를 할당받지 못하였기 때문에 서브넷의 주소 공간 활용도(address space utilization)가 훨씬 높은 값으로 측정될 가능성이 높다.

4. RHM

NASR이 서브넷 단위로 적용된 것과 유사하게, [그림 3]에서 보듯이, RHM의 MG도 각 서브넷 당 하나씩 설치되어 있지만, 비용을 절감하기 위하여 하나의 MG가 여러 개의 서브넷을 담당하게 하는 것도 가능하다. 그러나 하나의 MG가 여러 개의 서브넷을 담당하게 되면, 클라이언트 또는 서버와 MG 사이에 여러 개의 홉이 존재할 수 있기 때문에 스니핑과 같은 수동적 정찰 (reconnaissance) 공격에 노출될 가능성이 더욱 높아질 수 있는 사실에 주의해야 한다. 또한, RHM이 적용된 네트워크에서는 공격자가 서버의 도메인 네임만 알고 있다면, 공격자도 정상적인 클라이언트와 동일하게 해당 서버의 eIP를 항상 알아낼 수 있기 때문에, 도메인 네임을 이용한 공격자에 대처할 수

있는 방안도 마련되어야 한다. 이 외에, RHM에서는 연결을 장시간 유지 (long-lived connection)하는 호스트를 위하여, 연결이 설정되는 시점에 해당 호스트에 할당된 eIP를 연결이 끊어질 때까지 유지하도록 한다. RHM의 저자들은 이러한 정책을 사용하더라도 해당 eIP들을 제외한 나머지 주소들은 주소 변위를 위하여 사용될 수 있기 때문에, 공격자의 공격 속도 지연이 가능하다고 주장하고 있다. 그러나 중요 업무를 수행하는 서버들이 장시간 유지되는 연결들을 가지고 있을 가능성이 높은 환경에서는 이상의 정책이 오히려 주요 서버를 공격자에게 노출시킬 위험을 높일 수 있다.

RHM은 DYNAT와 APOD와 마찬가지로 주소 변환을 수행하는 게이트웨이를 해당 서브넷에 설치 및 운영해야 한다. 따라서 이러한 형태의 MTD 기법에 가진 문제점들을 RHM도 그대로 상속하게 된다.

5. DESIR

NASR과 같이 DESIR에서는 호스트에서 주소 변이가 이루어진다. 하지만 NASR과는 달리 호스트 주소 변이는 현재 서비스 중인 연결의 존재 유/무와는 상관없이 지속적으로 이루어진다. 그런데 TCP/IP 프로토콜은 연결이 지속되는 동안 변하지 않는 IP 주소와 포트 번호를 필요로 하기 때문에 한쪽 혹은 양쪽 호스트의 IP 주소 혹은 포트 번호가 변경되면 연결이 단절되는 상황이 발생한다. 따라서 호스트의 주소 변이에 관계없이 사용자에게 투명한 연결 서비스를 제공하기 위해 서비스 이관 또는 연결 이관(service or connection migration) 기법[12]이 필요하다. DESIR은 서비스 또는 연결 이관을 위해 클라이언트와 서버의 특정 데몬(daemon)을 통해 미리 설정된 제어 메시지를 교환하도록 한 뒤, 주소 변이에 따라 바뀐 송수신자의 IP 주소를 송수신 패킷에 반영하기 위하여 호스트 내부의 가상 인터페이스 (virtual interface)뿐만 아니라 내부-외부 주소 매핑(internal-external address mapping)을 업데이트한다. 그런데, 이와 같은 업데이트는 현재 사용 중인 연결들을 일시적인 중단을 야기한다. DESIR의 저자들은 하나의 연결 당 일시 중단 시간이 약 50msec 수준으로 감내할만 하다고 주장하지만, 중요 업무를 수행하는 서버들은 많은 연결을 유지할 수 있기 때문에 관련된 모든 연결들에 대한 연결 중단 누적 시간에 따른 영향 분석 및 대응책 마련이 필요하다.

한편, DESIR에서 인증 서버는 공격자와 정상적인 클라이언트를 구분할 뿐만 아니라 서버의 현재 IP 주소를 제공하는 DESIR 운영의 핵심적인 역할을 수행함에도 불구하고 인증 서버는 MTD의 대상에 포함되어 있지 않다. 따라서 DESIR에서 인증 서버에 대한 추가적인 보호 방안 마련이 필요하다. 뿐만 아니라, 서버 풀에는 다수의 서버들이 존재하기 때문에 클라이언트가 인증서버에서 자신이 원하는 서버의 IP 주소를 받아오기 위해서는 해당 서버의 확인자(naming)가 필요하다. 결국, DESIR이 실제 네트워크에 구현되기 위해서는 보다 구체적인 인증 및 네이밍 전략이 필요하다.

6. HIDE

HIDE는 기존 네트워크 인프라를 기본으로 하는 구현과 SDN을 기반으로 하는 구현 모두를 포함하고 있다. 그런데, 앞서 언급한 바와 같이, 본 논문은 기존 네트워크 인프라와 TCP/IP 프로토콜을 그대로 활용하는 NMTD 기술에 초점을 맞추고 있다. 따라서 NMTD 관점에서 HIDE 동작은 RHM의 동작과 거의 유사하다. 결국 RHM에서 언급된 특징들과 문제점들을 HIDE에서도 동일하게 발생할 수 있다. 이에 추가로, HIDE에서 클라이언트와 MG 및 DNS 서버와의 메시지 교환 절차가 RHM에서의 교환 절차와 달라졌음을 확인할 수 있는데, 이는 DNS 서버의 물리적인 위치 및 DNS 서버에 대한 보호 방안 마련 등에 대한 추가적인 연구가 필요하다는 것으로 해석할 수 있다.

IV. Threat Model for Network-based MTD

Okhravi et al.[1]은 NMTD 기술의 가장 큰 단점으로 잘 정의된 위협 모델(threat model)이 없다는 것을 지적하였다. 즉 인터넷은 기본적으로 클라이언트-서버 모델을 지향하고 있어 public 서버를 숨기거나 접근을 제한하는 행위는 이러한 모델에 위배되는 것이다. 따라서 클라이언트-서버 모델의 개방형 네트워크에 어떠한 부정적인 영향도 미치지 않는 NMTD의 위협 모델을 제시하여야만 한다.

실제 공격에 앞서 공격자들은 목표 시스템의 취약점을 확보하기 위해 정찰단계를 거친다. 이때 공격자들은 수동적으로 미러링(mirroring) 혹은 태핑(tapping) 등을 통해 네트워크 트래픽을 수집하여 분석하는 스니핑(sniffing)[13] 기술과 능동적으로 스캐닝 툴 등을 이용한 다양한 프로빙(probing)[14] 기술을 활용하여 목표 시스템에 대한 정보를 획득하게 된다. 뿐만 아니라, 보다 지능적인 공격자들은 수집된 정보들을 대상으로 연관성(correlation) 분석을 통해 자신들이 원하는 정보를 획득하게 된다[15]. 예를 들어, 시간의 흐름 즉 변이 구간마다 주소 변이를 일으키는 NMTD 기술이 적용되었다는 것을 공격자가 감지할 경우, 매 변이 구간마다 획득한 정보의 일부분들을 모아 연관성 분석을 통해 목표 시스템을 추적할 수도 있다. 한편, 이들 공격자들이 획득하고자하는 정보의 종류에 따라 위협 모델은 보다 세분화될 수 있다. 하나의 예로서, Kewley et al.[2]가 의도한 목표 시스템의 정보의 종류는 다음과 같다.

- IP 주소와 포트 번호
- 플랫폼 타입(Sun 혹은 인텔)
- OS 버전
- 서버 타입(Apache, Netscape, etc.)
- LAN IP 범위 및 서브넷 마스크

공격자가 정찰 과정을 통해 획득하고자하는 정보의 종류는

공격자의 지능화 정도와 업무부하(workload)와 직접적인 연관성을 가진다. 예를 들어, [그림 8]에서 보듯이 가장 기본적인 IP 주소와 포트 번호를 정찰 단계에서 획득하는 위협 모델은 공격자의 지능화와 업무부하가 가장 낮은 수준으로 볼 수 있다. 이에 반해, 타켓 시스템의 운영체제 버전 혹은 서비스 종류를 정찰 단계에서 획득하는 위협 모델은 가장 높은 수준으로 판단한다. 만약 낮은 수준의 위협 모델을 정의한다면, 시스템 개발 과정에서 보다 자세한 목표 시스템의 정보 수집에 요구되는 최소한의 변이 구간 길이 (minimum mutation interval length) 혹은 연관성 분석에 대한 우려를 배제하여도 무방할 것이다.

공격자의 위치 정보에 따라 위협모델은 더욱 다양해질 수 있다. 제2장 및 3장을 통해 분석한 기존 NMTD 기술 중에서 DYNAT, RHM, 그리고 HIDE는 NMTD가 적용된 보호 대상 호스트의 서브넷 내에서는 어떠한 변이도 발생하지 않는다. 따라서 서브넷 내에서는 NMTD 적용이 배제된다. 즉 해당 세그먼트는 공격자로부터 안전하다는 가정 하에서 시스템이 설계된 경우이다. 그러나 우리가 해당 세그먼트 내에 존재하는 호스트 역시 공격자가 직접 접근 혹은 간접 경유지로 활용한 위협 모델을 정의할 수 있다. 결국, NMTD의 위협모델은 (i) 공격자의 공격 능력, (ii) 공격자의 정보 수집 범위, 그리고 (iii) 공격자의 위치에 따라 다양한 조합이 가능하다. [그림 8]은 이들 세 가지 요소를 기준으로 NMTD를 위한 표준 위협모델의 한 예를 보여준다. 본 논문에서 논의된 대부분의 NMTD 기법들은 외부 공격자에 의한 IP 주소 혹은 포트번호 획득 수준의 위협모델을 가정하고 있다. 하지만, NMTD 기술을 실제 네트워크에 적용하기 위한 당위성을 확보하기 위해서는 보다 확장된 개념의 위협모델 정의가 반드시 필요하다. 또한, 이러한 위협모델 정의는 NMTD 개발과 관련된 시스템 개발 요구사항과 직접적인 상관관계를 형성하게 된다.

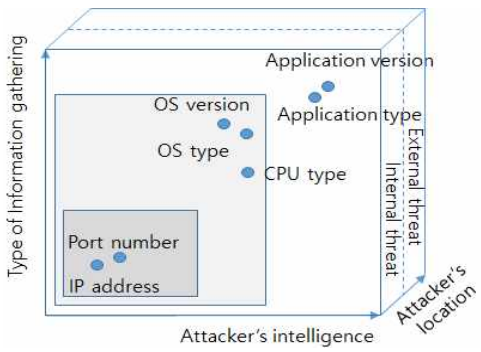

Fig. 8. An example of the threat model

V. Requirements for Network-based MTD

1. End-host Address Mutation

NASR과 DESIR은 단말에 할당된 IP 주소를 변이시킨다. 이에 반하여, DYNAT, APOD, RHM 및 HIDE는 가상 주소(virtual address)를 정의하고 가상주소와 단말에 할당된 IP 주소의 1:1 매핑 관계를 유지하면서 가상주소를 변이시킨다. 이하에서 단말에 할당된 IP 주소를 가상주소와 대비되는 용어로 실제주소(real address)라고 칭한다. 이상의 기법들은 시간에 따라 변이되는 가상주소들만 공중망에 노출되도록 함으로써 공격자들의 정찰단계를 무력화시키려 한다. 그러나 종단간(end-to-end) 통신을 위해서는 응용 프로그램에 패킷이 도착하기 전에 NAT 장치를 활용하여 가상주소를 실제주소로 변환하여야 하는데, NAT 장치에 의해 변환된 실제주소로 통신하는 서브넷 내에 공격자가 존재하는 위협모델에서는 DYNAT, APOD, RHM 및 HIDE과 같은 기법은 취약할 수 있다. 따라서 공격자의 위치에 상관없이 NMTD 기술이 적용되기 위해서는 반드시 단말 주소 변이 방안을 마련하여야 한다. 한편 이러한 단말 주소 변이 방식은 NAT 기능을 수행하는 게이트웨이를 네트워크에 설치 및 운영할 필요가 없어 실제 NMTD 기술로 적용될 가능성이 훨씬 높다.

2. Post Tracking

다음 [그림 9]는 2분 단위의 변이 구간을 가지는 NMTD의 예를 보여준다. 만약 현재 시점을 T_k (12:04:00-12:06:00) 라고 가정하면, 공격자들은 T_k 이전의 변이 과정을 알아내기 위하여 연결 단위 별 정보인 5-튜플(tuple) 정보를 수집하고 분석할 수 있다. 5-튜플(tuple) 정보란 <발신지 IP 주소, 발신지 포트 번호, 목적지 IP 주소, 목적지 포트 번호, 프로토콜 타입>를 의미한다.

일반적인 인터넷 서비스 사용 형태인, 여러 개의 클라이언트가 NMTD로 보호되는 하나의 서버를 일정 시간 액세스하는 상황을 가정하자. 매 변이 시간마다 여러 개의 클라이언트들은 주소 변이가 일어난 동일한 서버를 액세스할게 될 것이기 때문에, 공격자는 해당 목적지 주소를 대상으로 후위 트래킹(post tracing)하는 것이 가능하다. 물론 트래킹 중인 연결들의 주소가 T_{k+1} 시점에는 어떻게 변이할지 공격자가 예측할 수는 없지만 매 변이 주기(mutation interval)마다 변이되어 노출되는 주소 정보를 이용해 공격자들은 해당 변이 주기 내에서 정찰 정보 수집이 가능할 뿐만 아니라, 연관성 분석을 통해 공격자가 원하는 다음 정보 수집단계로 진입할 수 있다. 따라서 NMTD 개발에서 후위 트래킹 가능성을 최대한 억제할 수 있는 방안이 강구되어야 한다.

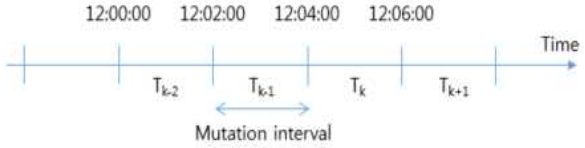

Fig. 9. An example of mutation intervals

3. Address Mutation Unit

주소 변이는 [그림 9]의 변이 주기마다 이루어질 수도 있지만, RHM과 HIDE는 종단간(end-to-end) 연결이 설정되기 직전에 할당받은 주소를 연결이 종료될 때까지 사용하는 연결단위 주소 변이 방법을 사용한다. 이러한 연결단위 주소 변이는 장시간 유지되는 연결(long-lived connection)에 의한 재사용 가능한 주소 범위가 감소하며, 또한 공격자에게 현재 사용 중인 네트워크 주소가 노출될 수 있는 충분한 시간을 제공할 수 있다. 그러나 연결 시작 시점에서부터 종료될 때까지 동일한 주소를 유지함으로써 서비스 또는 연결 이관이 필요 없는 장점을 가진다. 반면, 연결 단위와 관계없이 매 변이 주기마다 새로운 네트워크 주소를 할당받는 고정 시간 단위 주소 변이는 변이의 빈도를 증가시킴으로써 공격자의 작업부하를 한층 증가시킬 수 있다. 그러나 연결 중 주소 변화에 따른 연결 이관에 따른 지연 혹은 중단의 문제점을 극복해야 한다. 따라서 주소변이를 위한 연결단위 혹은 고정시간 단위 변이 각각의 장점을 극대화하면서 단점을 보완할 수 있는 방안을 마련한 필요가 있다.

4. Service Transparency

TCP/IP 프로토콜은 연결이 지속되는 동안 변하지 않는 IP 주소와 포트 번호를 필요로 하기 때문에 한쪽 혹은 양쪽 호스트의 IP 주소 또는 포트 번호가 변경되면 연결이 단절되는 상황이 발생한다. 따라서 호스트의 주소 변이에 관계없이 사용자에게 투명한 연결 서비스를 제공하기 위해 서비스 이관 또는 연결 이관 기법이 필요하다. 만일 이전 절에서 살펴본 연결단위 주소 변위의 단점을 보완하기 위하여, DESIR에서와 같이, NAPT 기능을 활용하여 매 변이 주기마다 새로 할당받은 주소로 송수신되는 패킷의 주소를 변환하는 경우, DESIR에서 언급한 연결 중단 시간 누적 문제가 발생할 수 있다. 따라서 연결 중단 시간을 최소화할 수 있는 투명한 이관 방안을 마련하여야 한다.

5. Name and Address access

NMTD 기술을 이용해 보호해야할 대상 호스트는 크게 두 가지 종류로 분류할 수 있다. 첫째, 공중망을 통해 접근하는 외부 사용자들도 자유롭게 이용할 수 있는 서버 호스트(예: 웹 서버, 메일 서버 등)들과 둘째, 내부 네트워크에 속해 있으면서 내부 사용자들이 주로 클라이언트로 사용하는 호스트들로 분류할 수 있다. 서버 호스트들 중에서 데이터베이스 서버와 PMS(Patch Management System) 서버의 경우 내부 네트워크에서만 접근할 수 있도록 구성되기도 하지만, 대부분의 서버 호스트들은 해당 서버의 도메인 이름을 알고 있는 클라이언트 호스트들이 DNS(Domain Name System) 서버를 통해 해당 서버의 IP 주소를 알아낼 수 있다면 언제든 접근 가능하도록 구성된다. 물론 서버의 도메인 이름을 DNS 서버에 등록하지 않은 채, 서버의 IP 주소를 알고 있는 클라이언트들만 접근하도록 구성하는 경우도 존재한다. 그러나 기존 NMTD 기술들의 일부는 도메인 네임 기반 접근만 고려하거나 혹은 IP 주소 기반 접근만 고려하여 설계되었다. 따라서 보다 유연한 NMTD 기술로 완성도를 높이기 위해서는 클라이언트가 서버에 접근하는 시점에 도메인 이름을 이용하는 경우와 IP 주소를 이용하는 경우 모두를 고려하여 NMTD 기법을 설계하여야 한다.

6. Adaptive Defense

대부분의 기존 NMTD 기술들은 예방적(proactive) 한 기법들이다. 즉 공격자의 행위에 상관없이 선제적으로 주소 변이를 일으키는 방법을 취하고 있다. 그러나 방어는 공격으로부터 자신을 보호하는 수단이기 때문에 필요하다면 공격자의 행위에 대응하여 주소 변이의 패턴에 변화를 줄 필요가 있다. 예를 들어, RHM은 공격자의 실패한 프로브들이 일정하지 않거나(non-uniform) 혹은 반복적이지 않은지(non-repetition)를 분석한 뒤, 일정한 규칙이 발견되면 해당 주소 공간을 주소 변이를 위한 할당 공간에서 배제한다. 이와 같이 공격자의 정찰 행위를 분석하고 적응적 동작을 수행할 수 있도록 NMTD 기법을 설계할 필요가 있다.

7. Controller operation

기존의 NMTD 기술들은 주소 변환를 위해 NAT 기능을 수행하는 소프트웨어 모듈 또는 네트워크 장치이외에도 주소 변이를 위한 다양한 컨트롤러, 인증 서버, DNS 서버 등을 필요로 한다. 하지만, 앞서 DESIR의 인증 서버 보호 방안 필요성과 RHM 및 HIDE의 DNS 서버 보호 방안 마련의 필요성에서 언급한 바와 같이, NMTD 기술 구현을 위한 컨트롤러 혹은 서버들의 보호 방안, 특히 주소 변이에 대한 방안이 마련되어야 한다.

다음 [표 2]는 본 장에서 다루어진 주요 시스템 요구사항을 중심으로 기존 NMTD 기술이 만족하고 있는 수준을 항목별로

Table 2. Functionally satisfactions of the desired requirements for the network-based MTD techniques

	End-host address mutation	Connection based address mutation	Service transparency	Named access	Address access	Adaptive address mutation
DYNAT	×	×	○	×	○	×
APOD	×	×	○	×	○	×
NASR	○	△	△	○	×	×
RHM	×	○	○	○	○	○
DESIR	○	×	△	○	×	×
HIDE	×	○	○	○	○	○

표시하였다. [표 2]의 세모 표시는 해당 항목을 부분적으로 만족함을 나타낸다. 예를 들어, [표 2]에서 NASR은 연결 단위 주소 변이 항목을 부분적으로 만족하는 것으로 표시되었다. 왜냐하면, NASR에서 사용 중인 연결이 존재하는 호스트에게는 기본적으로 서비스 이관을 위하여 가능하면 새로운 주소를 할당하지 않으려 하지만, 연결이 일정 시간 이상 지속될 경우 해당 호스트에게 강제로 새로운 주소를 할당하게 되고, 그 결과 연결이 끊어질 수 있기 때문이다. 동일한 사유로, NASR은 서비스 투명성 측면에서도 부분적으로 만족함으로 표시되었다. DESIR의 경우에는 주소 변이에 의해 야기되는 연결의 일시 중단 누적 시간 크기에 따라 서비스 투명성에서의 성능 저하 문제가 발생 가능하므로 서비스 투명성 측면에서 부분적으로 만족하는 것으로 표시하였다.

VI. Conclusions

본 논문에서는 SDN을 활용하지 않고 기존 네트워크 인프라에서 NMTD 기술을 개발하기 위하여, 지난 수년간 국외 연구진들이 제안한 여섯 가지 NMTD 기술의 동작원리를 요약한 뒤, 이들 기술들이 실제 네트워크에 적용되기 위해 해결해야할 문제점들을 자세히 분석하였다. 또한, 공격자의 지능화 수준, 공격자의 정보 수집 범위 및 공격자의 공격 위치를 기준으로 NMTD의 가장 큰 문제점으로 지적되고 있는 위협 모델에 대하여 서술하였으며, 기존 네트워크 인프라에 적용할 NMTD 기법 개발을 위한 핵심적인 일곱 가지 요구 사항을 제시하였다.

최근 유연한 라우팅과 패킷 헤더 변환 기능을 제공하는 SDN의 출현으로 NMTD 기술에서의 SDN 활용이 검토되고 있다. 그러나 기존 네트워크 인프라 전체를 교체해야하는 경제적 부담과 SDN이 대규모 네트워크에 적용된 성공적인 사례가 아직은 보고된 바가 없어 이들 기술을 NMTD에 직접 적용하기 위해서는 보다 신중한 접근이 필요하다. 따라서 본 논문에서 초점을 맞추고 있는 기존 네트워크 인프라용 NMTD 기술의 개발 및 적용이 선행되어야 할 것으로 판단된다. 그러나 앞서 제안된 NMTD 기술이 실제 네트워크에 적용된 사례는 아직 보고되지 않았다. 이러한 현실은 본 논문에서 서술한 바와 같이 실제 네트워크에 적용하기 위해서는 해결해야할 어려운 문제점들이 존재하기 때문으로 판단된다. 따라서 본 논문을 출발점으로 많은 국내 연구진들이 NMTD 관련 기술에 관심을 기울이고 한 단계 더 나아가 기술 개발에 집중하는 계기가 되기를 희망한다.

REFERENCES

[1] H. Okhravi, T. Hobson, D. Bigelow and W. Streilein, "Finding Focus in the Blur of Moving-Target Techniques," In IEEE Security&Privacy, vol.12, no. 2, pp. 16-26, March 2014.

[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. 2007.

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

[6] J. Sun and K. Sun, "DESIR: Decoy-enhanced seamless IP randomization," Proceedings of the IEEE ONFOCOM, 2016.

[7] J. H. Jafarian, A. Niakankahiji, E. Al-Shaer and Q. Duan, "Multi-dimensional Host Identity Anonymization for Defeating Skilled Attacks," Proceedings of the 2016 ACM Workshop on Moving Target Defense, pp. 47-58, 2016.

[8] J. H. Jafarian, E. Al-Shaer and Q. Duan, "OpenFlow Random Host Mutation: Transparent Moving Target Defense using Software Defined Networking," Proceedings of the first worshop on Hot topics in software defined networks, pp. 127-132, 2012.

[9] Z. Zhao, F. Liu and D. Gong, "An SDN-Based Fingerprint Hopping Method to Prevent Fingerprinting Attacks," Proceedings of the Security and Communication Networks, 2017.

[10] B. A. Nunes, M. Mendonca, X. Nguyen, K. Obraczka, and T. Turletti, "A Survey of Software-Defined Networking: Past, Present, and Future of Programmable Networks," IEEE Communications Surveys & Tutorials, vol.16, no.3, pp.1617-1634. Feb. 2014.

[11] R. Droms, Dynamic Host Configuration Protocol, RFC 2131, http://www.rfc-editor.org, Mar. 1997.

[12] G. Su and J. Jieh, "Mobile Communication with Virtual Network Address Translation," Technical Report CUCS-003-02, Department of Computer Science, Columbia University, 2002.

[13] S. Ansari, S. G. Rajeev and H. S. Chandrashejar, "Packet

sniffing: a brief introduction," IEEE potentials, vol.21, no. 5, pp.17-19, 2002.

[14] G. F. Lyon, Nmap network scanning: The official Nmap project guide to network discovery and security scanning, Insecure, 2009.

[15] C. Kreibich, M. Handley and V. Paxson, "Network intrusion detection: Evasion, traffic normalization, and end-to-end protocol semantics," Proceedings of USENIX Security Symposium, 2001.

Authors

Koohong Kang received the B.S. and M.S. degrees in Electronics Engineering from Kyungpook National University and Chungnam National University, Korea, in 1985 and 1990, respectively, and then Ph.D. degree in Computer Science and Engineering from POSTECH, Korea, in 1998. From 1985 to 2000, Dr. Kang was a researcher and a senior researcher at ETRI participating in various research projects in TDX switching system, ATM networks, and network security. He is currently a Professor in the Department of Information and Communications Engineering, Seowon University. He is interested in computer networks and Internet security.

Taekeun Park received his B.S., M.S., and Ph.D. degrees in Computer Science and Engineering from POSTECH, Pohang, Korea in 1991, 1993, and 2004, respectively. He joined POSTECH PIRL in 1993 and moved to SK Telecom in 1996. From 2000 to 2001 and from 2001 to 2002, he worked for 3Com Korea and Ericsson Korea, respectively. In 2004, he joined in the department of Multimedia Engineering, Dankook University, Korea. He is currently on the faculty of the department of Applied Computer Engineering at Dankook University. His research interests include data processing, IoT, wireless/mobile communications, and distributed services.

Daesung Moon received his MS degree in computer engineering from Pusan National University, Rep. of Korea, in 2001. He received his PhD degree in computer science from Korea University, Seoul, Rep. of Korea, in 2007. He joined the Electronics and Telecommunications Research Institute(ETRI), Daejeon, Rep. of Korea, in 2000, where he is currently a senior researcher. He has also been a Chief major professor with the Department of Information Security Engineering, University of Science and Technology, Daejeon, Rep. of Korea. His research interests include network security, data mining, biometrics, and image processing.