2017
Electronics and
Telecommunications
Trends

네트워크 주소 이동 기술 동향

Trends in Network Address Moving Technology

박경민 (K.M. Park, kmpark@etri.re.kr) 지능보안연구그룹 연구원
우사무엘 (S. Woo, samuelwoo@etri.re.kr) 지능보안연구그룹 선임연구원
문대성 (D.S. Moon, daesung@etri.re.kr) 지능보안연구그룹 책임연구원/PL
김익균 (I.K. Kim, ikkim21@etri.re.kr) 지능보안연구그룹 책임연구원/그룹장

Moving Target Defense(MTD) is a novel security technology concept in which the IT infrastructure changes its form actively and prevents various types of cyber attacks. Network address moving technology is the field that has been most actively researched in terms of MTD. A number of studies on network address moving published over the last decade have suggested a virtual address-based network address moving technology for efficiency in the implementation. However, virtual address-based network address moving technology has serious vulnerabilities in terms of security and availability. This paper examines the technological characteristics of the existing studies and analyzes their limitations. It suggests security requirements to be considered when designing the network address moving technology through a technological analysis

* DOI: 10.22648/ETRI.2017.J.320609
* 본 연구는 2017년도 정부(미래창조과학부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임[No.2017-0-00213, 능동적 사전보안을 위한 사이버 자가변이 기술 개발].

Ⅰ. 서론

ICT 융합기술의 발전으로 인해 IoT 서비스의 상용화가 빠르게 확산되고 있다. 향후 5년 이내에 인터넷에 연결되는 IoT 디바이스의 수는 약 260억 개까지 증가할 것으로 예측된다[1]. IoT 디바이스의 증가는 미확인 공격 접점(Unknown Attack Surface)의 증가로 이어진다. 이처럼 보호 대상은 급격하게 증가하고 있지만, 현재 일반적인 IT 인프라들은 반응적/수동적 방어 형태의 보안 전략을 운영하고 있다. 이러한 보안 전략에서는 보호 대상 자체의 구성에는 변화가 없기 때문에 공격자들이 대상 시스템의 취약점을 찾을 수 있는 충분한 시간과 정보를 확보할 수 있다. 즉 사이버위협의 공격과 방어 측면에서 반응적·수동적 방어 전략은 항상 공격자가 우세할 수밖에 없는 비대칭적 관계가 형성된다.

따라서, 지능화되는 사이버 위협에 더욱 효율적으로 대응하기 위해서는 수동적 대응에서 능동적 예방으로 전략을 전환해야 한다. 보호 대상 IT 인프라에 대한 공격 노출점을 명확히 측정/진단하고, 각 객체(네트워크, 시스템, 서버, 데이터 저장소 등)별로 능동적 보안 기능을 적용할 수 있는 새로운 개념의 사이버 보안 기술이 필요하다. 이러한 요구를 만족시키기 위해 MTD (Moving Target Defense) 기술이 연구되고 있다[2].

MTD는 지능화되고 있는 사이버 공격에 능동적으로 대응하기 위한 혁신적인 보안 전략으로써 미국 백악관이 2011년에 발표한 '사이버보안 연구개발 전략' 중 가장 주목받았던 연구 분야이다. MTD는 사이버 공격 대상의 주요 속성들(네트워크 설정, 플랫폼, 소프트웨어, 데이터, 서비스 등)을 지속적으로 변화 또는 이동시킴으로써 공격자의 공격 또는 취약점 분석 행위를 능동적으로 방어하기 위한 보안 기술을 뜻한다.

MTD 연구 영역에서 가장 활발하게 연구가 진행되고 있는 분야는 네트워크 주소 이동 기술이다. MTD의 개념이 정립되기 이전부터 네트워크 주소 이동 기술은 꾸준히 연구되고 있었다. 대부분의 기존 연구들은 구현 측면의 효율성을 고려하여 NAT 또는 SDN 기반의 가상 주소를 이용한 보호대상 은닉 기술을 제안했다. 그러나 이 기술들은 보안성과 가용성 측면에서 심각한 문제점을 발생시킬 수 있다. 보안성 측면에서의 대표적인 문제점은 내부 공격자에 의해 특정 서브넷에 소속된 보호대상의 IP 주소가 노출될 수 있다는 것이며, 가용성 측면에서의 문제점은 가상 주소를 실제 주소로 변환하는 패킷 프로세싱으로 인해 네트워크 성능이 저하 될 수 있다는 것이다. 본고에서는 가상 주소 기반 네트워크 이동 기술의 한계점을 알아보고 실제 주소 이동 기술의 필요성을 설명한다. 이와 함께 Fingerprint 변환 기술과 Decoy 노드 운영 기술의 필요성을 설명한다.

본고는 다음과 같이 구성된다. Ⅱ장에서는 네트워크 주소 이동 기술을 정의하고 기본 개념을 소개한다. Ⅲ장에서는 네트워크 주소 이동 기술 관련 기존 연구들을 비교 분석한다. Ⅳ장에서는 Ⅲ장의 분석 내용을 기반으로 기존 연구들의 장단점을 정리하고 네트워크 주소 이동 기술 연구를 위한 요구사항을 도출한다.

Ⅱ. 네트워크 주소 이동 기술의 정의

MTD 연구는 크게 다음과 같이 3가지 분야로 분류할 수 있다[2].

- MTD Theory: 효과적인 MTD 전략을 수립하는 방법을 연구한다. 보호 대상에서 어떤 대상을 언제 이동시킬 것인가에 대한 기본적인 설계 원리를 연구한다. MTD Strategy를 설계/개발하기 위한 가이드라인을 제시하는 연구 분야로 정의할 수 있다.
- MTD Strategy: MTD Strategy는 이동시킬 속성(예, 운영체제, 소프트웨어, 네트워크 구성 및 주소)을 선정하고 해당 속성에 적합한 네트워크 이동 기술을 설계하는 연구 분야이다. 3가지 연

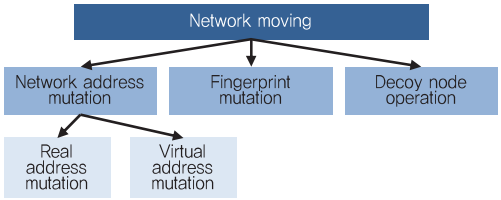
구 분야 중 가장 핵심이 되는 연구 영역이며 특히 네트워크 구성 및 주소 이동과 관련된 연구가 가장 활발히 진행되고 있다.

- MTD Evaluation: MTD Evaluation은 기존 연구들의 효율성을 측정하고 이를 기반으로 새로운 MTD Strategy 설계/개발을 위한 요구사항을 제공하는 것을 목표로 한다. 객관적 지표와 정보를 제공하기 위한 평가방법을 연구한다. 또한, 새롭게 설계/개발되는 MTD Strategy 기법들을 평가하는 중요한 척도를 마련하는 연구 분야이다.

본고에서는 MTD Strategy 연구 분야 중 네트워크 주소 이동 기술 동향을 중점적으로 다룬다. MTD Strategy 연구 분야에서 네트워크 주소를 이동 파라미터로 사용하는 연구들은 네트워크 주소 이동 기술로 분류된다[2], [3]. 그러나 최근 연구 동향을 고려했을 때 단순히 네트워크 주소만 변화시킨다고 능동적 보안 기능을 수행했다고 판단할 수는 없다. 주소가 바뀌더라도 호스트가 가진 몇 가지 고유한 특성들을 추적하여 해당 호스트를 쉽게 특정 지을 수 있기 때문이다. 이러한 문제점을 해결하기 위하여 네트워크 주소 이동 기술은 점차 진화하고 있다. 단순하게 IP, Port만 변경하던 기술에서 호스트의 Fingerprint도 변화시키고, 호스트와 유사한 Decoy 노드를 운영하는 기술들도 새롭게 제안되고 있다. 이는 단순히 네트워크 주소만 변화시키는 것이 아니라 호스트 정보를 다양하게 변화 시키는 새로운 개념의 네트워크 주소 이동 기술을 의미한다. 우리는 전통적인 MTD에서 정의했던 네트워크 주소 이동 개념뿐만 아니라 Fingerprint 변환, Decoy 노드 운용까지 포함한 네트워크 주소 이동 기술의 연구 동향을 살펴본다.

Ⅲ. 네트워크 주소 이동 기술 동향

네트워크 주소 이동 기술은 (그림 1)과 같이 크게 3가지 기술들의 융합으로 이루어진다.



(그림 1) 네트워크 주소 이동 기술 연구 영역 분류

〈표 1〉 네트워크 주소 이동 기술 연구동향

분류	Mutation metrics		Mutated factors		
	Direct (real adderss)	Indirect (virtual adderss)	Adress	Finger-print	Decoy
[4]	Don't care		○		
[5]		○	○		
[6]		○	○		
[7]		○	○		
[8]		○	○		
[9]	○		○		
[10]	Don't care		○		
[11]		○	○		
[12]		○	○		
[13]		○	○		
[14]		○	○	○	○
[15]	○		○		○
[16]	Don't care				○
[17]					
[18]		○		○	
[19]	Don't care			○	
[20]	Don't care			○	
[21]		○	○	○	
[22]		○	○	○	
[23]		○	○	○	
[24]		○	○	○	
[25]		○	○	○	

네트워크 주소 이동 관련 연구 동향은 〈표 1〉과 같다. 본고에서는 기존 연구들을 앞서 언급한 3가지 대표 기술 관점으로 분류하고 각 연구의 특징을 알아본다. 또한, 기존 연구들이 제안하고 있는 가상 주소를 사용하는 네트워크 주소 이동 기술의 취약점을 살펴본다.

1. 네트워크 주소 변환

네트워크 주소 변환 기술은 호스트의 실제 주소를 변환시키는 방식과 가상 주소를 실제 주소와 맵핑한 뒤,

외부에 노출된 가상 주소만 변환시키는 방식으로 나뉜다. MTD 개념이 등장한 이후, 현재까지 대부분의 연구는 SDN, NAT, 게이트웨이 등의 네트워크 기술을 활용해 외부에는 가상 주소만 노출하고, 그것을 주기적으로 변환시키는 방식을 제안해왔으며, 대표 연구들은 다음과 같다.

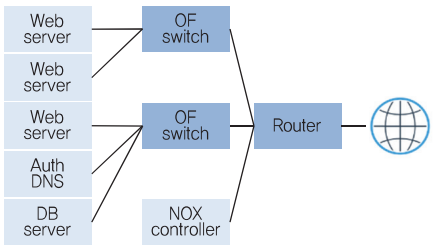
가. MT6D

MT6D(Moving Target IPv6 Defense)는 (그림 2)와 같이 IPv6 기반 네트워크 환경에서 전용 게이트웨이를 이용하여 주기적으로 IID(Interface IDentifier)를 변경하는 기법이다[4]. MT6D는 암호학적 알고리즘(일방향해쉬함수)에 현재 IID와 타임스탬프를 입력하여 새로운 주소를 생성하는 기법을 사용한다. 송신자와 수신자 간의 시간 동기화만 유지된다면 상호 간의 IID를 동기화시킬 수 있다. IPv6에서 인터페이스 ID를 통상 64bit로 유지하기 때문에 본 기법에서는 일방향해쉬함수를 이용하여 도출된 출력 값의 64bit만 사용한다. 출력 값 64bit 의 안전성은 2016년 현재, NIST에서 권고하는 수치 이하이기 때문에 MT6D는 일방향해쉬함수 안전성에 대한 검증이 일차적으로 필요한 기술이다.

(그림 2) MT6D 테스트베드 프로토타입

나. OF-RHM

OF-RHM(OpenFlow-Random Host Mutation)은 외부 공격자로부터 보호하고자 하는 호스트들에게 가상 IP를 할당하고, 그것을 주기적으로 변환시키는 대표적인 MTD 연구 사례이다[5]. OF-RHM의 네트워크 도메인은 (그림 3)과 같이 SDN 컨트롤러와 OF-Switch로 구성된다. OF-Switch는 호스트의 실제 IP와 가상 IP를 맵핑시키고 내-외부 트래픽에 대하여 패킷 레벨 프로세

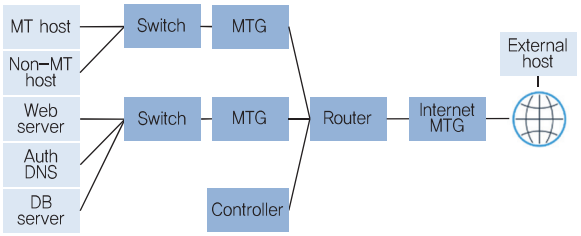


(그림 3) OF-RHM 네트워크 구조의 예

싱을 통해 외부에는 실제 IP를 은닉하고, 가상 IP만 공개하도록 한다. OF-RHM은 가상 IP를 주기적으로 변환시켜 공격자에게 네트워크 스캐닝을 통해 획득한 정보의 불확실성을 증가시키고 적법한 사용자에게는 투명한 서비스를 제공한다. 가상 IP 맵핑과 변환 주기 등에 대한 정책은 SDN 컨트롤러를 통해서 결정된다. OF-RHM은 SDN에서만 적용 가능한 기술로서 확장성이 부족하기 때문에 OF-RHM 연구팀은 Legacy 네트워크에서도 적용 가능한 RHM을 동시에 연구하였다.

다. RHM

RHM(Random Host Mutation)의 IP 변환 체계와 프로토콜은 OF-RHM과 유사하지만, RHM은 SDN을 대상으로 하지 않고 (그림 4)와 같이 Legacy 네트워크를 대상으로 하여 스위치와 라우터 사이에서 OF-Switch의 기능을 하는 MTG(Mutation Gateway)를 운용한다. 그리고 가상 IP 할당 방식에 있어서 LFM(Low Frequency Mutation)과 HFM(High Frequency Mutation)이라는 두 단계의 변환 주기를 운용하는 것에서 OF-RHM과 차이가 있다[6].

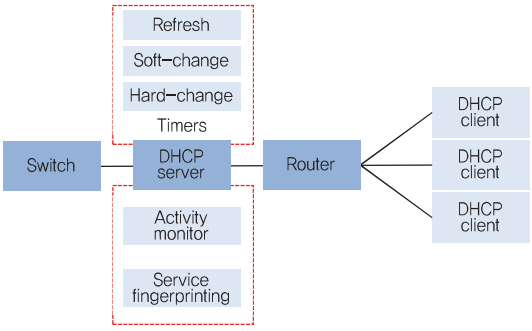


(그림 4) RHM 네트워크 구조의 예

라. NASR

MTD 개념이 등장하기 이전부터 네트워크 주소 변환 기술에 대한 연구들이 선행되어왔다. 대부분의 연구는 최근의 MTD 연구 동향과 마찬가지로 가상 IP를 변환하는 방식이지만[7], [8], NASR(Network Address Space Randomization)은 클라이언트의 실제 IP를 주기적으로 변환시킴으로써, 미리 계산해 놓은 네트워크 경로를 통해 전파되는 Hit-list Worm을 차단하는 목적으로 연구되었다[9].

NASR은 클라이언트들에게 IP를 할당하는 DHCP 서버의 IP 임대 시간을 동적으로 변경하면서 빈번하게 클라이언트들의 IP를 바꿔준다. 이로 인해 발생하는 커넥션 유실을 최소화하기 위한 방법으로, (그림 5)와 같이 서비스 모니터와 3가지 타이머를 이용하여, 서비스에 필요한 커넥션 활성화 상태를 모니터링하고, 동적으로 IP 임대 시간을 조절하는 타이머를 운용한다. 그러나 NASR은 클라이언트 IP 변환에만 해당되고 동적 주소 체계 기반에서만 가능한 제약이 있다.



(그림 5) NASR에서의 DHCP 기능

2. Decoy 노드 운용

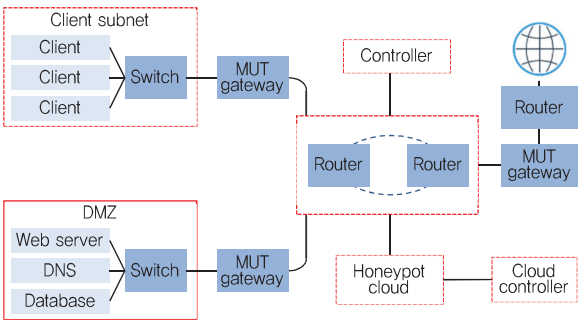
Decoy 노드는 기존에 싱크홀이나 블랙리스트 생성 등에 쓰인 허니팟과 유사하지만, 공격자가 네트워크를 스캐닝 하거나 타겟을 특정 짓는 단계에서의 오버헤드를 높이고 불확실성을 증가시키기 위한 공격 접점 증가의 개념을 갖는 MTD 기술에서 필수 요소이다.

가. Decoy-Based MTD

Decoy-Based MTD는 보호하고자 하는 서버와 동일한 LAN에 다수의 가상 Decoy 노드를 만들고 시간이 지남에 따라 실제 서버와 Decoy 서버들이 지속적으로 IP를 변경하는 모델을 제안하였고, Nmap 스캐닝 툴을 기반으로 시뮬레이션 결과를 제시함으로써 초기 MTD를 타겟으로 한 Decoy 노드 운용 연구의 대표적 사례로 꼽힌다[10].

나. HIDE

OF-RHM/RHM 연구팀은 2012년 이후로 RHM을 기반으로 지속적인 연구를 해오고 있다[11]-[13]. 이러한 연구들을 기반으로 최근에는 (그림 6)과 같이 RHM의 네트워크 모델에 대량의 허니팟을 운용하는 HIDE(Host IDEntify Anonymization)가 발표되었다[14]. 허니팟 클라우드는 보호하고자 하는 대상과는 다른 네트워크에 위치하고 있으며, 외부망과 연결된 MTG가 외부에서 들어오는 트래픽 중에서 유효한 호스트로 들어오지 않는 트래픽은 의심스러운 트래픽, 즉 공격 또는 스캐닝으로 판단하고 허니팟 클라우드로 Redirection 한다. 각각의 허니팟들은 실제 서버들과 유사하게 OS와 각종 서비스가 실행되고 있으며, 스캐닝에 대한 응답으로 실제 서버와 유사한 Fingerprint를 공격자에게 줌으로써 스캐닝 결과에 대한 불확실성뿐만 아니라 분석 및 공격 도구 생성에도 어려움을 줄 수 있다.

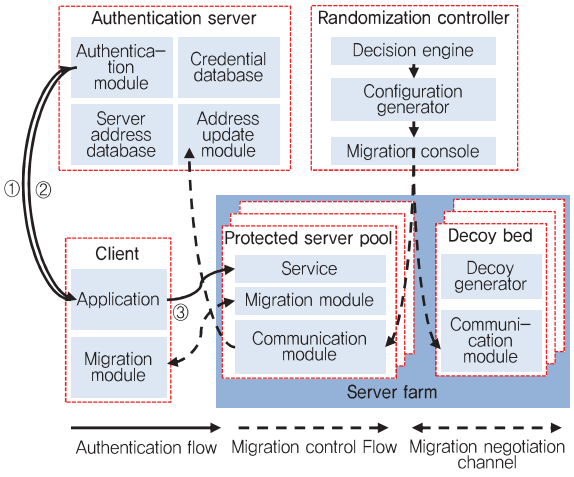


(그림 6) 허니팟 클라우드가 적용된 HIDE 구조의 예

다. DESIR

최근, 가상 IP를 사용하는 기존의 연구들과는 다르게 실제 IP를 랜덤하게 변환함과 동시에 그에 따른 효과를 강화하기 위해, 대량의 Decoy 노드들과 Decoy 네트워크를 생성하는 DESIR(Decoy-Enhanced Seamless IP Randomization)연구가 발표되었다[15].

DESIR 연구팀은 공격자가 탐색 단계에서 작성한 Decoy 노드들에 대한 블랙리스트가 다음 주기에서는 무효화되도록 하기 위하여, 실제 서버뿐만 아니라 Decoy 노드들의 주소도 지속적으로 랜덤하게 변환시키는 방법을 제안하였다. 그리고 (그림 7)의 인증 서버를 통해 적법한 사용자들에게는 끊김 없는 서비스를 제공하기 위한 Seamless Connection Migration 기술을 제안하였다[16].



(그림 7) DESIR 구조

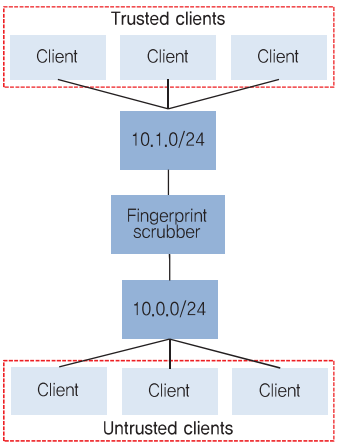
3. Host Fingerprint 변환

공격자는 대상 서버의 OS의 종류와 서비스 등의 정보를 정확하게 특정 짓지 못한 상태에서는, 취약점을 이용한 공격을 실행하기 어렵다. 이와 관련하여 MTD 관점에서의 두 가지 타입의 Fingerprint 변환 기술들이 연구되고 있다. 하나는 TCP 3-way 핸드 셰이크와 같은 세션 컨트롤 메시지를 조작하여 공격자에게 서버의 OS나 실행 중인 서비스에 대한 거짓 정보를 전달하는 기술이고, 다른 기술은 네트워크 보안장비들을 통해 의심스러운 트래픽을 감지한 뒤 해당 트래픽에 대하여 거짓 응답을 통해 공격자를 혼란 시키는 기술이다[17]. 전자와 같이 프로토콜 또는 헤더를 조작하여 Fingerprint를 바꿀 경우, 의도치 않은 네트워크 서비스 장애가 있을 수 있기 때문에 대부분의 연구는 후자로 진행되어왔다.

가. Fingerprint Scrubbing

Fingerprint 변환에 대한 과거의 대표 연구로서, TCP/IP Fingerprinting을 통한 호스트의 정보들이 노출되는 것을 방지하기 위하여, 패킷 헤더에서 호스트의 정보를 인식하는데 참조할 수 있는 데이터들을 삭제하거나 수정하는 연구가 있었다[18]. 이 연구는 input 패킷을 trusted 채널과 untrusted 채널로 구분하여 IP 포워딩 단계에서 normal 포워딩을 할지 Fingerprint scrubbing을 수행할지 결정하여 untrusted 채널로 나가는 트래픽에 대해서는 호스트의 OS를 노출되지 않게 한다. (그림 8)은 trusted/untrusted 채널을 통해 클라이언트들을 구분하는 예시이다.

그러나 Fingerprint scrubbing은 다양한 패킷 헤더의 정보를 삭제하거나 수정하는 과정에서 발생하는 네트워



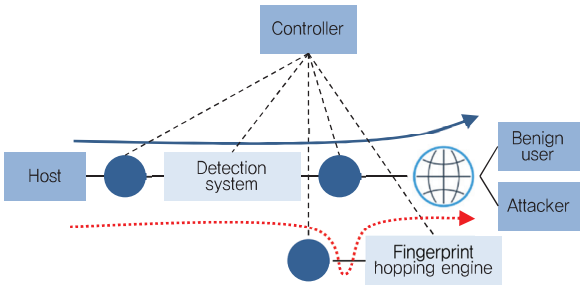
(그림 8) Trusted/untrusted 채널과 Fingerprint scrubber의 예시

크 성능 저하, 그리고 적법한 사용자와 공격자의 요청 모두를 동일한 방식으로 처리한다는 단점이 있다. 최근에는 이러한 단점을 개선하기 위하여 적법한 사용자만을 구분해내기 위한 방법들이 제안되었다[19], [20].

나. SDN-Based Fingerprint Hopping

최근에는 네트워크 보안 장비들의 발달로 인하여 IDS와 Fingerprint Hopping 엔진을 이용한 SDN 기반의 OS 랜덤화, 그리고 은닉에 대한 연구가 진행되었다[21], [22]. 이러한 연구들은 IDS를 통해 적법한 사용자의 트래픽과 공격자로 의심되는 트래픽을 구분하여, 공격자로 의심되는 트래픽에 대해서는 (그림 9)와 같이 Fingerprint Hopping 엔진을 통해 패킷의 헤더를 수정함으로써 실제 서버의 OS가 아닌 다른 OS로 보이게 한다. 그러나 이러한 연구들은 IDS에 의존하기 때문에 IDS를 통해 구분해내지 못하는 숙련된 공격자의 Fingerprinting에 대해서는 적절한 대응을 할 수 없다는 단점을 갖는다. 완성도 높은 MTD 기술을 위해서는 IDS가 배제된 상황에서도 네트워크 장애를 피해갈 수 있는 Fingerprint 변환 기술에 대한 연구가 필요하다.

OS Fingerprint Hopping은 아니지만, Fingerprint 추적과 유사하게, 네트워크 주소 외에 서버가 갖는 고유한 특성이라고 볼 수 있는, 열린 port를 통해 제공되는 특정 서비스의 패턴도 공격자가 타겟을 특정 짓는 데에 이용할 수 있는 요소이며, 이와 관련된 Port Hopping 기술들도 연구되었다[23]-[25].



(그림 9) Detection system을 이용한 Fingerprint hopping

Ⅳ. 기대 효과 및 요구사항

1. 기대 효과

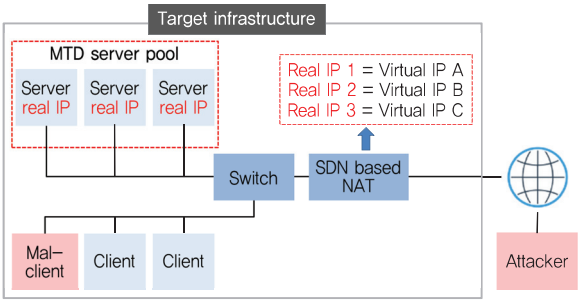
네트워크 주소 이동 기술은 보호 대상의 다양한 네트워크 속성을 능동적으로 변화시킴으로써 공격자의 분석 복잡도를 증가시켜 취약점 분석 과정을 무력화시키는 '공격 노출점 교란' 효과와 공격자의 의도된 일련의 과정을 무력화시키는 '공격 체인 단절' 효과를 제공한다. 네트워크 주소 이동 기술을 통해 공격자 우세의 비대칭적 공방 관계를 방어자 우세의 비대칭적 관계로 역전시키는 매우 의미 있는 결과를 얻을 수 있을 것이라 생각된다.

2. 요구사항

〈표 1〉에서 알 수 있듯이 네트워크 주소 이동 기술과 관련된 대부분의 연구는 가상 주소 운영 방식을 사용하고 있다. 또한, 3가지 파라미터(네트워크 주소, Fingerprint, Decoy 노드)를 함께 변화시키는 기술들은 아직까지 많이 연구되고 있지 않다. 기존 연구들의 한계점과 제약사항을 분석한 결과 다음과 같은 추가 요구사항을 만족하는 네트워크 주소 이동 기술이 필요할 것으로 예상된다.

가. 실제 주소 변환의 필요성

가상 주소가 아닌 실제 주소를 변환해야 하는 필요성은 보안성 측면과 가용성 측면으로 나뉘어 설명할 수 있다. 보안성 측면의 요구사항은 다음과 같다. 가상 주소 기반 네트워크 주소 이동 기술은 호스트의 실제 네트워크 주소를 변경하는 것이 아니라, 외부에 공개된 가상 주소를 실제 주소로 맵핑 시켜주는 기술이다. 해당 기술은 공격자가 보호 대상 외부에 존재할 경우에만 의미 있는 방어를 수행할 수 있다. 만약 (그림 10)과 같이 보호 대상과 동일한 내부망에 공격자가 위치한다면 공격자는 고정된 상태로 사용되고 있는 보호대상의 실제 주소를



(그림 10) Virtual IP Mutation 기술의 취약점

획득할 수 있다. 즉 내부 공격자에 대한 방어 기능은 전혀 수행할 수 없는 문제점이 있다.

이러한 문제점을 극복하기 위해서는 악성코드에 의해 네트워크 내부 호스트가 감염되거나 심지어 내부에 공격자가 있을 경우에도, 보호 대상의 실제 네트워크 주소를 랜덤하게 변경함으로써 공격자가 공격 대상의 실제 주소를 획득하지 못하게 하는 기술의 개발이 필요하다.

가용성 측면의 요구사항은 다음과 같다. 가상 주소를 사용하는 기술들은 네트워크 장비들을 통해 별도의 패킷 프로세싱을 해주거나, 보호하고자 하는 서브넷 또는 호스트 앞 단에 게이트웨이를 두어서 가상-실제 주소 변환을 시켜줘야 한다. 이와 같은 방식은 네트워크 장비나 게이트웨이에 대한 보안 정책을 계속 바꿔줘야 한다는 관리 측면의 추가 비용과 패킷 프로세싱으로 인해 발생하는 네트워크 성능 저하의 단점을 갖는다. 실제 주소를 변화시키는 네트워크 이동 기술은 위와 같은 단점들은 존재하지 않지만, 스트리밍이나 파일전송 서비스와 같이 지속적인 트래픽이 발생하는 서비스의 경우 네트워크 연결이 유실된다는 단점이 있다.

MPTCP(Multi-Path TCP)로 대표되는 다중 경로 네트워킹 기술은 서버와 클라이언트 간에 단일 커넥션으로 인해 발생하는 실제 주소 변환의 단점을 보완해줄 수 있는 차세대 네트워킹 기술이다[26], [27]. MPTCP의 본래 목적은 단말들의 네트워크 인터페이스를 모두 활용하여 네트워크 대역폭을 좀 더 효율적으로 사용하기 위한 것이었으나, 이것의 장점은 연결 유실이 없는 TCP Session Migration 및 연결 재구성을 통한 MTD 기술에도 활용될 수 있을 것이다[28].

나. 이동 파라미터 다양화

네트워크 주소 변환만 사용하는 것으로는, MTD의 목표인 공격자 입장에서의 불확실성, Kill-chain 단절 등의 효과를 크게 낼 수가 없다[22]. 가용 주소 범위 내에서 지속적으로 주소를 바꾼다 하더라도 유효한 호스트의 개수가 적은 상황에서는 공격자가 타겟을 특정 지을 수 있는 확률이 높아진다. 그뿐만 아니라 공격자는 네트워크 주소 외에 보호 대상의 Fingerprint, 열린 Port와 서비스 패턴 등의 고유한 성질을 지속적으로 추적하여 타겟을 특정 지을 수 있다. 이러한 이유로 Decoy 운영 및 Fingerprint 변형을 고려한 연구들이 발표되고 있다.

최근의 MTD 연구들은 보호 대상이 되는 호스트 외에 가상화된 다수의 Decoy 호스트를 같은 네트워크에서 운영함으로써 공격 접점을 넓힘과 동시에, 다양한 방법으로 Fingerprint와 Port, 그 외에도 공격자가 타겟을 특정 짓는데 이용할 수 있는 다양한 파라미터들을 변화시킴으로써 공격자가 타겟을 특정 짓기 어렵도록 이동 파라미터를 다양화시키는 추세를 보이고 있다.

V. 결론

네트워크 환경에서 공격과 방어는 비대칭적인 관계를 유지하고 있다. 비대칭적 관계는 공격을 수행하는 비용(Cost: 시간, 정보 등)과 공격을 방어하는 비용 측면에서 발생한다. 반응적/수동적 정보보호 기술은 공격자에게 많은 시간과 정보를 제공한다. 이처럼 공격자의 우세한 비대칭적(Asymmetric) 조건 때문에 중요 시스템을 완벽하게 방어하는 것은 매우 어렵다. 네트워크 주소 이동 기술을 통해 공격자 우세의 비대칭적 공방 관계를 방어자 우세의 비대칭적 관계로 역전시키는 매우 의미 있는 결과를 얻을 수 있을 것이다.

약어 정리

ICT	Information and Communication Technology
IoT	Internet of Things
MTD	Moving Target Defense
NAT	Network Address Translation
SDN	Software Defined Networking
LAN	Local Area Network

참고문헌

[1] Gartner, "The Internet of Things," WorldWide, 2013.

[2] G. Cai et al., "Moving Target Defense: State of the Art and Characteristics," *Frontiers Inform. Technol. Electron. Eng.*, vol. 17, no. 11, Nov. 2016, pp. 1122-1153.

[3] G. Cai et al., "An Introduction to Network Address Shuffling," *Int. Conf. IEEE Adv. Commun. Technol.*, Pyeonchang, Rep. of Korea, Jan. 31-Feb. 3, 2016, pp. 185-190.

[4] M. Dunlop et al., "MT6D: A Moving Target IPv6 Defense," *Military Commun. Conf.*, Baltimore, MD, USA, Nov. 7-10, 2011, pp. 1321-1326.

[5] J.H. Jafarian, E. Al-Shaer, and Q. Duan, "Openflow Random Host Mutation: Transparent Moving Target Defense Using Software Defined Networking," *Proc. Workshop Hot Topics Softw. Defined Netw.,* Helsinki, Finland, Aug. 13, 2012, pp. 127-132.

[6] E. Al-Shaer, Q. Duan, and J.H. Jafarian, "Random Host Mutation for Moving Target Defense," in *SecureComm 2012: Security and Privacy in communication Networks*, Heidelberg, Berlin: Springer, 2012, pp. 310-327.

[7] D. Kewley et al., "Dynamic Approaches to Thwart Adversary Intelligence Gathering," *DISCEX'01. Proc. IEEE*, Anaheim, CA, USA, June 12-14, 2001. pp. 176-185.

[8] M. Atighetchi et al., "Adaptive Use of Network-Centric Mechanisms in Cyber-Defense," *IEEE Int. Symp. Object-Oriented Real-Time Distrib. Comput.*, Cambridge, MA, USA, Apr. 18, 2003, pp. 179-188.

[9] S. Antonatos et al., "Defending Against Hitlist Worms Using Network Address Space Randomization," *Comput. Netw.*, vol. 51, no. 12, Aug. 2007, pp. 3471-3490.

[10] A. Clark, K. Sun, and R. Poovendran, "Effectiveness of IP Address Randomization in Decoy-Based Moving Target Defense," *IEEE Annu. Conf. Decision Contr.*, Florence, Italy, Dec. 10-13, 2013, pp. 678-685.

[11] J.H.H. Jafarian, E. Al-Shaer, and Q. Duan, "Spatio-Temporal Address Mutation for Proactive Cyber Agility Against Sophisticated Attackers," *Proc. ACM Workshop Moving Target Defense*, Scottsdale, AZ, USA, Nov. 2014, pp. 69-78.

[12] J.H.H. Jafarian, E. Al-Shaer, and Q. Duan, "Adversary-Aware IP Address Randomization for Proactive Agility Against Sophisticated Attackers," *IEEE Conf. Comput. Commun.*, Kowloon, Hong Kong, 2015, pp. 738-746,

[13] J.H.H. Jafarian, E. Al-Shaer, and Q. Duan, "An Effective Address Mutation Approach for Disrupting Reconnaissance Attacks," *IEEE Trans. Inform. Forensics Security*, vol. 10, no.12, 2015, pp. 2562-2577.

[14] J.H.H. Jafarian et al., "Multi-dimensional Host Identity Anonymization for Defeating Skilled Attackers," *Proc. ACM Workshop Moving Target Defense*, Vienna, Austria, Oct. 24, 2016, pp. 47-58.

[15] J. Sun and K. Sun, "DESIR: Decoy-Enhanced Seamless IP Randomization," *Annu. IEEE Int. Conf. Comput. Commun.*, San Francisco, CA, USA, Apr. 10-14, 2016, pp. 1-9.

[16] W. Fan, D. Fernández, and Z. Du, "Versatile Virtual Honeynet Management Framework," *IET Inform. Security*, vol. 11, no. 1, 2016, pp. 38-45.

[17] S. Jajodia et al., *Moving Target Defense: Creating Asymmetric Uncertaintyfor Cyber Threats*, New York, USA: Springer Science & Business Media, 2011.

[18] M. Smart, G.R. Malan, and F. Jahanian, "Defeating TCP/IP Stack Fingerprinting," *Usenix Security Symp.*, Denver, CO, USA, Aug. 14-17, 2000.

[19] M.A. Rahman, M.H. Manshaei, and E. Al-Shaer, "A Game-Theoretic Approach for Deceiving Remote Operating System Fingerprinting," *IEEE Conf. Commun. Netw. Security*, National Harbor, MD, USA, Oct. 14-16, 2013, pp. 73-81.

[20] M. Albanese et al., "Manipulating the Attacker's View of a System's Attack Surface," *IEEE Conf. Commun. Netw. Security*, San Francisco, CA, USA, Oct. 29-31, 2014, pp. 472-480

[21] Kampanakis, Panos, Harry Perros, and Tsegereda Beyene, "SDN-Based Solutions for Moving Target Defense Network Protection," *IEEE Int. Symp. WoWMoM*, Sydney, Australia, June 19, 2014, pp. 1-6.

[22] Z. Zhao, F. Liu, and D. Gong, "An SDN-Based Fingerprint Hopping Method to Prevent Fingerprinting Attacks," *Security Commun. Netw.*, vol. 2017, 2017.

[23] D. Ma et al., "A Self-Adaptive Hopping Approach of Moving Target Defense to thwart Scanning Attacks," in *Information and Communications Security*, New York, USA: Springer, 2016. pp. 39-53.

[24] L. Shi et al., "Port and Address Hopping for Active Cyber-Defense," in *Intelligence and Security Informatics*, Heidelberg, Berlin: Springer, 2007, pp. 295-300.

[25] Y.B. Luo, et al, "RPAH: Random Port and Address Hopping for Thwarting Internal and External Adversaries," *Trustcom/BigDataSE/ISPA*, Helsingki, Finland, Aug. 20-22, 2015, pp. 263-270.

[26] Linux Kernel Multipath TCP Protect, Accessed 2017. https://www.multipath-tcp.org/

[27] M. Scharf and A. Ford, "Multipath TCP (MPTCP) Application Interface Considerations," No. RFC 6897, 2013.

[28] C. Pearce and S. Zeadally, "Ancillary Impacts of Multipath TCP on Current and Future Network Security," *IEEE Internet Comput.*, vol. 19, no. 5, 2015, pp. 58-65.