Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.33, NO.6, Dec. 2023 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2023.33.6.939

네트워크 보호체계에서 네트워크 주소변이 기술 적용에 대한 영향성 연구*

이 수 원,[1†‡] 황 세 영,[2] 홍 석 규[3]
[1,2,3]한화시스템 (수석연구원, 전문연구원, 연구원)

A Study on the Impact of Applying Network Address Mutation Technology within the Network Protection System*

Suwon Lee,[1†‡] Seyoung Hwang,[2] SeukGue Hong[3]
[1,2,3]Hanwha System (Chief Engineer, Senior Engineer, Junior Engineer)

요 약

IT 기술이 급속히 발전하는 현대 초연결 환경은 네트워크 장비들이 다양해지고 네트워크 구성이 복잡해짐에 따라 사이버 공격자가 침투경로로 활용될 수 있는 공격표면(attack surface) 또한 증가하게 되었다. 이러한 환경에서 사이버 공격을 원천적으로 방어하기 위해 공격표면을 변이하는 MTD(Moving Target Defense) 기술이 연구되고 있다. 그중에 네트워크를 통해 공격이 시작됨에 따라 주요 속성 네트워크 주소를 변이하는 기술이 있으나, 대부분 운용환경이 기존 고정 IP 기반으로 운용되기 때문에 주소변이 기술이 기존 네트워크 보호체계 내에 적용되었을 때 어떠한 영향이 있는지 연구가 필요하다. 본 논문에서는 기존 네트워크 보호체계에서 네트워크 주소변이 기술이 적용되었을 때의 영향성을 연구하였고 연구 결과로서 네트워크 보호체계의 주요 시스템인 방화벽, NAC, IPS와 네트워크 주소변이 기술이 동시 적용되었을 때 운용 측면에서 고려해야 할 요소를 도출하였다. 또한 사이버 대응체계 내에서 네트워크 분석시스템과의 연동성을 위해 네트워크 주소변이 기술에서 관리해야하는 요소를 제안하였다.

ABSTRACT

In the hyper-connected network, which network equipment is diverse and network structure is complex, the attack surface has also increased. In this environment, MTD(Moving Target Defense) technology is being researched as a method to fundamentally defend against cyber attacks by actively changing the attack surface. network-based MTD technologies are being widely studied. However, in order for network address mutation technology to be applied within the existing fixed IP-based system, research is needed to determine what impact it will have. In this paper, we studied the impact of applying network address mutation technology to the existing network protection system. As a result of the study, factors to be considered when firewall, NAC, IPS, and network address mutation technologies are operated together were derived, and elements that must be managed in network address mutation technology for interoperability with the network analysis system were suggested.

Keywords: network address mutation technology, network protection system, MTD

Received(09. 13. 2023), Modified(10. 19. 2023), Accepted(11. 02. 2023)

* 본 논문은 2021년도 정부(방위사업청)의 재원으로 국방기술진흥연구소의 지원을 받아 수행된 연구임(KRIT-CT-21-037)

† 주저자, suwon.lee@hanwha.com
‡ 교신저자, suwon.lee@hanwha.com(Corresponding author)

I. 서 론

일반적으로 사이버 환경에서 공격자는 공격 대상을 선정하기 위해 공격표면(attack surface)를 이용하여 주요 시스템의 취약점 등을 수집하고, 사이버 공격을 위한 발판을 준비한다. 따라서 종래의 방어적 수단으로 공격표면을 최대한 노출되지 않도록 하거나 노출 경로를 차단하려는 방법이 활용되었다. 하지만 네트워크 구성이 복잡해지고 네트워크를 구성하는 장비들이 다양해짐에 따라 공격표면이 증가하게 되었고 공격표면에 대한 관리 업무도 늘어나게 되었다. 이런 환경에서 근본적인 방어 수단으로 공격표면이 될 수 있는 시스템의 주요 속성을 능동적으로 보호하는 MTD(Moving Target Defense) 기술이 연구되고 있다[1][2]. MTD 기술은 IP 주소, 포트, 플랫폼 등의 시스템 주요 속성을 변경하기 때문에 주요 속성 기반으로 운용되었던 기존 시스템에 영향성이 있을 수 있다. 경우에 따라 기술적으로 동시에 운용될 수 없는 환경도 있기 때문에 MTD 기술이 기존 환경에 어떠한 영향성이 있는지 운용 측면에서 검토가 필요하다. 본 논문에서는 기존 네트워크 보호체계 운용환경에서 네트워크 주소 변이기술을 도입하였을 때의 영향성을 분석하기 위하여 네트워크 보호체계의 주요 시스템인 방화벽, NAC, IPS와 사이버 대응체계 내 운용되는 네트워크 분석시스템을 대상으로 분석하였다.

본 논문의 구성은 다음과 같다. 서론에 이어 2장에서는 관련 연구로서 MTD 기술과 기존의 네트워크 보호체계에서의 주요 시스템에 대해서 설명하고 3장에서는 기존 네트워크 보호체계의 주요 시스템과 네트워크 주소변이 기술이 같이 운용되었을 때의 영향성에 대한 분석 내용을 설명하였다. 끝으로 4장은 결론 및 향후 연구 방향에 대해 기술하였다.

II. 관련 연구

2.1 MTD(Moving Target Defense)

MTD(Moving Target Defense)는 공격자가 침투경로 및 공격에 활용될 수 있는 공격표면(attack surface)을 변경함으로써 공격의 준비 및 시도를 사전에 무력화하는 기술이다. 공격표면의 예로는 네트워크 주소, 포트, 프로토콜, 플랫폼 등이 있다. MTD 기술은 크게 네트워크와 호스트 기반 MTD로 크게 구분할 수 있으며, 대부분의 사이버 공격이 네트워크를 이용한 정찰단계부터 시작하기 때문에 네트워크 기반의 MTD 기술이 많이 연구되고 있다. 네트워크 기반 MTD 기술에는 IP 주소와 포트를 변이하는 RPAH(Random Port and Address Hopping)[3], 보호대상 호스트의 실제 IP를 램덤하게 변경하는 NASR(Network Address Space Randomization)[4], Decoy 노드를 활용하는 HIDE(Host IDEntify Anonymiztion)[5], DESIR(Decoy-Enhaned Seamless IP Randomization)[6] 기술 등이 있다. 위에서 설명한 것과 같이 네트워크 기반 MTD 기술은 가상주소, 실주소 변이, Decoy 운용[7] 여부, Decoy 주소변이 여부, 주소변이를 위한 게이트웨이 유무 등에 따라 매우 다양하다. 본 논문에서는 다양한 네트워크 주소변이 기술에 대해 모두 비교 분석하는 것은 아니며 클라이언트와 서버 간에 실 네트워크 주소를 변이하며 통신하는 MTD 기술을 대상으로 분석하였다.

2.2 네트워크 보호체계

네트워크 MTD 기술은 네트워크 주요 속성을 변경하기 때문에 기존 고정 IP 기반의 운용환경에서 어떠한 영향이 있는지 검토가 필요하다. 정보화업무훈령[8]에서는 정보보호체계를 네트워크를 보호하기 위한 네트워크 보호체계, 보안 OS 및 백신 등으로 구성된 서버/단말 보호체계, SIEM 등으로 구성된 사이버 대응체계, 자료교환 및 포렌식 장비 등으로 구성된 보안관리체계, 암호장비 및 기기인증으로 구성된 암호체계 체계 5가지로 분류하고 있으며 본 논문에서는 네트워크 기반 기술과 밀접한 보호체계의 주요시스템 대해 관련 연구를 수행하였다. 이외 체계에 대해서는 향후 연구과제에서 수행할 계획이다.

Table 1. information protection system

Category	Main Corresponding System
network protection system	- Network Firewall - Unified Threat Management - Network Access Control - Intrusion Prevention System - DDoS Response System - Virtual Private Network

Category	Main Corresponding System
Server/device protection system	• Web Firewall • Hacking Mail/Harmful Site Blocking System • Secure OS • Virus Protection System • Digital Rights Management • Data Loss Prevention
Cyber response system	• Threat Management System • Security Information and Event Management • Network Threat Analysis System
Security management system	• Mobile Device Management • Access Control System • Secret Management System • Data Exchange System • Security Evaluation System • Personal Information Protection System • Digital Forensic Equipment
cryptosystem	• Encryption Equipment • Encryption Key Management System • Device Authentication System • Military Public Key Infrastructure

2.2.1 네트워크 방화벽(Firewall), UTM

방화벽은 시스템의 보안을 위해 네트워크 상에서 외부에서 내부로, 내부에서 외부로의 불법적인 접근은 차단하는 보안 솔루션으로 주로 네트워크 자산(서버 등) 구조의 최상단에 위치하며 인터넷과 같은 외부망으로부터 들어오는 접근 시도를 1차로 제어, 통제(허용/거부)함으로써 내부 네트워크를 보호기능을 담당한다. UTM은 다중 위협에 대해 보호기능을 제공할 수 있는 포괄적 보안 솔루션으로 UTM이 제공하는 가장 주요한 장점으로는 단순하고, 설치 및 사용이 간결하며, 모든 보안 기능이나 프로그램을 동시에 갱신할 수 있는 장점이 있다.

2.2.2 네트워크접근제어(NAC)

네트워크에 접근하는 접속 단말의 보안성을 강제화할 수 있는 보안 시스템으로 허가되지 않거나 웜·바이러스 등 악성코드에 감염된 PC 또는 노트북, 모바일 단말기 등이 회사 네트워크에 접속되는 것을 원천적으로 차단해 시스템 전체를 보호하는 보안 솔루션이다.

2.2.3 침입방지시스템(IPS)/DDoS 차단시스템

IPS는 네트워크 패킷을 분석하여 공격 시그니처(Signature)를 찾아내 제어함으로써 비정상적인 트래픽을 중단시키는 보안 솔루션이다. 수동적인 방어 개념의 방화벽이나 침입탐지시스템(IDS)과 달리 침입 경고 이전에 공격을 중단시키는데 초점을 둔 개념의 솔루션으로, 해당 서버의 비정상적인 행동에 따른 정보 유출을 자동으로 탐지하여 차단함으로써 인가자의 비정상 행위를 통제할 수 있다. DDoS 차단 시스템은 대량의 트래픽을 전송해 시스템을 마비시키는 DDoS(DDoS: Distributed Denial of Service, 분산서비스거부) 공격 전용의 차단 솔루션으로, 대량으로 유입되는 트래픽을 신속하게 분석해 유해트래픽 여부를 판단해 걸러줌으로써 보호대상 네트워크의 가용성과 안정성을 높여주며, 해당 서비스의 연속성을 보장하는 데 중요한 역할을 한다.

2.2.4 가상사설망(VPN)

인터넷망 또는 공중망을 사용하여 둘 이상의 네트워크를 안전하게 연결하기 위하여 가상의 터널을 만들어 암호화된 데이터를 전송할 수 있도록 만든 네트워크로 공중망 상에서 구축되는 논리적인 전용망이다.

2.2.5 분석 대상 선정

본 논문에서는 기능상 다소 차이가 있을 수 있으나 기술 매커니즘이 비슷한 시스템 중의 하나를 분석 대상으로 선정하였고 그 결과 방화벽와 기능적으로 유사한 UTM, IPS와 DDoS 차단시스템, 별도 가상 터널링으로 통신하는 VPN은 제외하고 방화벽, IPS, NAC을 분석대상으로 선정하였다. 또한 네트워크 수집정보를 기반으로 네트워크를 정보를 분석하는 네트워크 분석시스템을 분석 대상에 포함하였다.

III. 본 론

3.1 분석 대상 네트워크 주소변이 시스템

네트워크 주소변이 기술은 변이 범위 대상 및 방

식에 따라 매우 다양하다. 본 논문에서는 다양한 네트워크 주소변이 기술에 대해 네트워크 보호체계와의 영향성을 모두 기술할 수 없기 때문에 Fig. 2에서와 같이 주소변이 클라이언트, 주소변이 서버, 변이정책 서버로 구성되는 환경을 대상으로 분석하였다. 기본 환경은 서버-클라이언트 구조에서 공격의 최종 공격 목표가 될 수 있는 주소변이 서버의 실제 NIC(network interface controller) 주소가 변이되는 구조이다. 이 구조에서는 주소변이 클라이언트는 자신의 IP는 변경하지 않고 네트워크 패킷의 목적지 주소를 주소변이 서버의 주소로 변경하며 주소변이 서버와 통신을 한다.

운용 절차에 따라 관리자가 변이정책 서버를 통해 주소변이 정책을 수립 및 적용하면 변이정책 서버가 주소변이 클라이언트와 주소변이 서버에 주소변이 정책을 보내준다. 주소변이 서버는 주소변이 정책에 따라 변이시점에 자신의 IP를 변경하고 클라이언트는 변이되는 서버의 IP를 목적지 주소로 변경하며 통신을 하는 구조이다. 예를 들면 클라이언트는 192.168.0.2의 IP를 사용하고 서버의 IP가 192.168.0.11~75 범위 내에서 임의로 변경하는 정책인 경우, 서버는 주소변이 정책에 따라 192.168.0.11~75 범위 내에서 IP를 변경한다. 클라이언트는 수신한 주소변이 정책을 통해 변이된 서버 IP 주소를 알 수 있으며 통신 시점에 서버 변이 주소를 목적지 주소로 변경하여 네트워크 패킷을 송신한다. 분석 대상 환경은 주소 정책은 특정 시간에 네트워크 주소를 변경하는 정책을 사용하므로 주소변이 클라이언트와 주소변이 서버는 시간 동기화가 되어야 하는 환경이다.

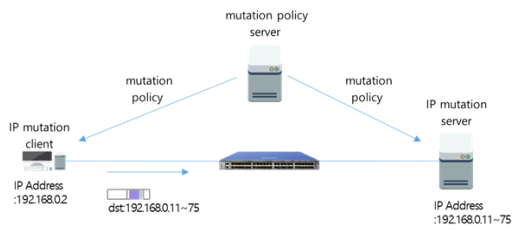

Fig. 1. IP mutation operating structure

3.2 네트워크 보호체계 주요 해당 시스템 분석

3.2.1 방화벽(Firewall)

방화벽은 네트워크 경계에서 불법적인 접근을 차단하는 시스템으로 일반적으로 인바운드, 아웃바운드 영역에 화이트리스트 기반으로 허용되는 IP를 설정하여 인가되지 않은 접속을 차단한다. 따라서 네트워크 주소변이 운용 환경에서 주소변이 클라이언트가 방화벽 내에 주소변이 서버와 같이 있으면 방화벽 정책 설정에 영향은 없으나 주소변이 클라이언트가 방화벽 외부에 위치한다면 방화벽 정책 설정 시 서버의 주소변이 대역을 허용해야 통신이 가능하다.

예를 들면 Fig. 2과 같이 주소변이 서버가 192.168.0.11~75 범위 내에서 임의값으로 변이한다고 하면 방화벽 정책을 설정할 때 인바운드 IP 허용 정책에 192.168.0.11~75의 IP을 설정해야 주소변이 클라이언트에서 송신하는 패킷이 방화벽을 통과할 수 있기 때문에 주소변이 서버와 통신이 가능하다. 기존 고정 IP 기반의 운용 환경에서는 서비스를 제공하는 서버의 IP 이외의 IP를 차단하고 실제 운용되는 IP 정보가 최대한 노출되지 않도록 하거나 노출 경로를 차단하려고 노력하였다. 따라서 고정 IP 운용환경에서 서버 주소가 192.168.0.11를 사용한다면 192.168.0.11이외의 IP를 차단하고 이 서버가 제공하는 포트만 허용하였다.

하지만, 방화벽 설정 정책이 노출되거나 방화벽 권한 탈취 등으로 방화벽 정책이 무력화되면 보안에 심각한 영향을 줄 수 있다. 반면에 주소변이 환경에서는 주소변이 서버의 IP가 계속 변이하는 구조로 공격자가 주소변이 정책을 모르는 한 주소변이 서버와 쉽게 통신할 수 없는 구조이다. 따라서 방화벽이 무력화 될 경우에도 공격자의 공격준비 및 시도를 무력화하는 효과가 있다.

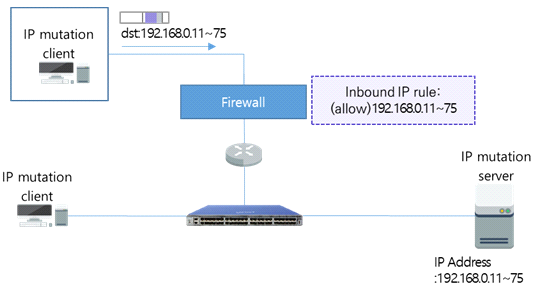

Fig. 2. firewall inbound rule

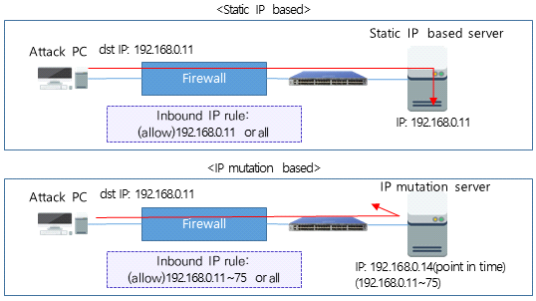

Fig. 3. disabled firewall comparison

3.2.2 IPS

IPS는 다양한 유해 트래픽에 대해 시그니처와 행위 규칙을 이용해 탐지하고 차단하는 시스템이다. 일반적으로 IPS는 패킷 헤더(packet header), 컨텐츠 필드(content field)를 검사하며 시그니처 정책에 따라 공격 및 유해 여부가 확실하면 차단하고, 아닌 경우는 알람으로 경고하거나 해당 트래픽 정보를 제공한다. 분석 대상 네트워크 주소변이 환경에서는 패킷의 목적지가 주소변이 서버의 주소이기 때문에 패킷헤더의 목적지 주소만 변이된다는 차이만 존재하므로 IPS의 시그니처 기반 탐지기능에 대해서는 영향을 주지 않는다. 왜냐하면 일반적으로 IPS의 차단 정책에는 목적지 주소가 포함되지 않기 때문이다. 또한 주소변이 클라이언트가 감염되어 유해 트래픽을 생성하는 경우라도 주소변이 클라이언트의 IP는 변이하지 않기 때문에 IPS가 해당 패킷을 차단할 때에도 기존의 고정 IP 기반 환경과 같이 주소변이 클라이언트의 패킷을 차단할 수 있다.

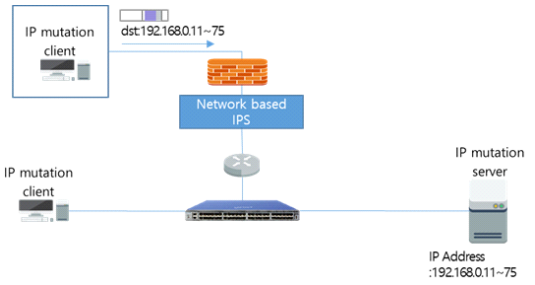

Fig. 4. IPS operating environment

3.2.3 NAC(Network Access Control)

NAC는 네트워크에 접근하는 엔드포인트(endpoint)의 보안성을 강화하기 위해 인가되지 않거나 감염된 단말기 등이 네트워크에 접속하는 것을 차단하는 시스템이다. NAC는 사용자 정보, 단말 정보, 트래픽 정보 등으로 클라이언트를 인증하며, NAC 운용환경은 NAC 에이전트 설치 유무에 따라 구분할 수 있다. 에이전트 기반 NAC은 클라이언트에 NAC 에이전트를 설치하여 클라이언트의 감염여부, 무결성 등을 검사하고 NAC 서버를 통해 인증정보 및 차단정책을 송수신하는 구조로 정책을 위반한 클라이언트를 차단한다. 비에이전트 기반의 NAC은 NAC 에이전트가 설치될 수 없는 환경이거나 성능 및 상호운용간 충돌로 인해 에이전트 설치 없이 클라이언트를 차단하는 방식으로 주로 IP, MAC 주소에 기반한 정책을 통해 정책에 맞지 않는 클라이언트가 네트워크에 접속하는 차단하는 방식이다. 에이전트 기반 NAC 환경에서 네트워크 주소변이 시스템을 적용한다면, 주소변이 클라이언트에 NAC 에이전트를 설치하여 운용해야 할 것이다. 이러한 경우 주소변이 클라어언트와 NAC 서버는 주소변이를 하지 않기 때문에 NAC 정책 송수신 및 차단정책에는 영향을 주지 않는다. 일반적으로 사용되지 않지만 클라이언트를 대상으로 하지 않고 서버에 NAC 에이전트를 설치하여 운용할 경우에는 NAC 클라이언트가 주소변이 서버에 설치되기 때문에 NAC 에이전트와 NAC 서버간의 정책 송수신 및 차단 정책에 문제가 된다. NAC 서버가 주소변이 서버의 주소변이 정책을 알 수 없기 때문이다. 상용 NAC 시스템은 linux 기반 클라이언트를 위해 linux용 NAC 에이전트가 제공되기 때문에 linux 서버에 NAC 에이전트를 설치하여 운용하는 것이 불가능한 것은 아니다. 하지만 일반적인 NAC 운용환경에서 서버에 NAC 에이전트를 설치 운용하지 않고 서버에 대해서는 비에이전트 기반의 NAC 정책을 적용한다.

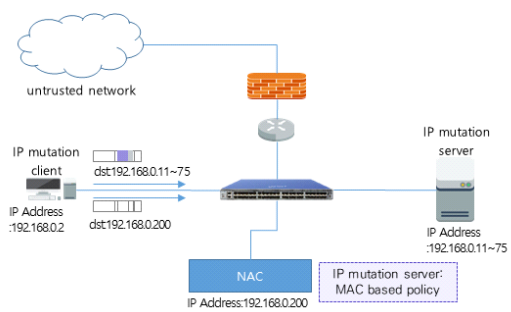

Fig. 5. NAC operating environment

따라서 주소변이 환경에서 일반적인 NAC 설정 정책과 같이 주소변이 서버에 대해서 비에이전트 기반의 정책을 사용하면 영향을 주지 않는다. 다만 비에이전트 기반의 정책에서 IP-MAC 일치, 허용 IP 및 MAC 이외 차단 정책을 설정할 수 있는데 이런 경우 주소변이 서버의 주소변이 대역을 설정해야 하거나 변이하지 않는 주소변이 서버의 MAC 주소로 정책을 설정하면 기존 시스템에서와 차이는 없다.

3.2.4 네트워크 분석시스템

네트워크 정보 수집은 공격자만 하는 것이 아니라 정보보호체계 내에서도 정보보호를 위해 네트워크 데이터를 수집하고 저장한다. 수집된 데이터는 네트워크 상태분석, 통계정보 제공, 이상탐지, 사고 발생 시 조사분석에 활용된다. 이렇게 수집된 데이터를 분석하는 시스템에서는 네트워크 변이환경은 목적지 주소가 변이되기 때문에 기존 고정 IP 환경과 차이가 있다. 예를 들면 네트워크 정보 분석 시 목적지 기반의 통계정보가 필요한 경우 네트워크 변이환경에서는 실제 동일한 서버와 통신하였지만 목적지 주소로만 보면 각각 다른 서버로 분석된다. 또한 주소변이 대역을 여러 대의 서버가 공유하여 사용할 경우에는 원래 접속하지 않은 서버와 통신했다는 잘못된 결과를 초래할 수 있다. 다른 예로서 보안사고 발생 시 그동안 수집된 로그정보 및 네트워트 패킷 캡처 정보를 분석하게 되는데 주소변이 환경에서는 목적지 주소가 변이된 정보이므로 실제 통신한 서버를 알기 어렵다. 따라서 네트워크 주소변이 기술에서는 네트워크 분석시스템이 수집한 정보를 이용하여 실제 통신한 서버가 무엇이였는지 알 수 있도록 하는 정보를 관리해야 한다. 이러한 관리 정보는 주소변이 정책에 따라 관리 정보가 달라질 수 있으나 3.1장에 설명한 분석 대상 네트워크 주소변이 환경을 기준으로 관리되야 할 정보에 대해 설명한다. 네트워크 분석시스템에서 주로 분석하는 데이터는 로그 및 네트워크 패킷 캡처 데이터 등이 있으며 기본으로 포함되는 데이터 요소로는 타임스탬프가 있다. 주소변이 환경에서도 주소 정책에 의해 시간에 따라 주소가 변이되기 때문에 시간 정보가 필수 요소로 활용된다. Fig. 6와 같이 분석 대상 네트워크 주소변이 환경은 주소변이 클라이언트, 주소변이 서버, 변이정책 서버가 시간 동기화가 되어있고 주소변이 클라이언트와 주소변이 서버간 통신하는 구조이다. 네트워크 분석시스템이 해당 통

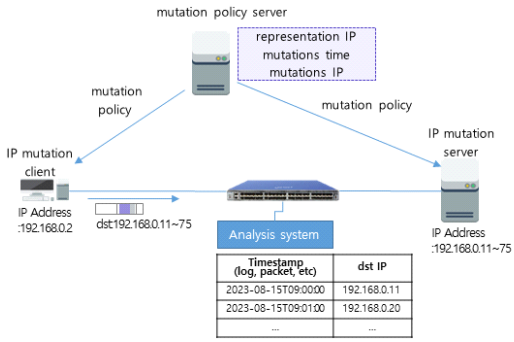

Fig. 6. information for analysis system

신망에서 시간동기화 하여 네트워크 정보를 수집하면 네트워크 분석시스템이 수집된 데이터와 주소변이 정책에 의해 수행된 정책 정보는 동일한 시간 정보를 갖게 된다.

따라서 네트워크 분석시스템이 수집한 데이터가 주소변이 된 데이터라 하더라도 시간 따라 변이한 정책 정보를 알 수 있으면 원래 통신하였던 서버를 알 수 있게 된다. 네트워크 분석시스템이 수집한 주소변이 데이터를 실제 통신한 서버 정보로 변환하기 위해 네트워크 주소변이 기술에서 관리해야 할 정보는 주소변이 서버를 유일하게 식별할 수 있는 대표 IP 주소 값과 시간에 따른 주소변이 이력이다. 예를 들면 대표 IP가 192.168.0.11인 서버가 UTC 2023-08-15T09:01:00에 192.168.0.12로 2023-08-15T09:02:00에 192.168.0.20으로 변경하는 정책이 수행되었으면 네트워크 분석시스템이 수집한 데이터 중에 2023-08-15T09:01:00와 2023-08-15T09:01:59 사이에 시작된 세션 데이터 중에서 목적지가 192.168.0.12인 데이터를 192.168.0.11로 변경해주면 수집된 통신 데이터들이 유일한 대표 IP로 매핑되기 때문에 주소변이가 안 된 환경에서와 같이 수집데이터를 분석할 수 있게 된다.

IV. 결 론

공격자가 활용될 수 있는 공격표면을 능동적으로 변이하여 사이버 공격을 원천적으로 방어하기 위한 방법으로 MTD(Moving Target Defense) 기술이 연구되고 있으며 MTD 분야의 하나로써 네트워크 주소를 물리적으로 변이하며 통신하는 네트워크 주소변이 기술이 있다. 네트워크 주소는 시스템의 주

요 속성으로 기존 운용 시스템에서 중요하게 활용되고 있다. 따라서 기존 시스템과 네트워크 주소 변이 기술이 어떠한 영향이 있는지 검토가 필요하며, 본 논문에서는 기존 네트워크 보호체계 내에서 주요시스템인 방화벽, IPS, NAC과 사이버 대응체계 내의 네트워크 분석시스템과 영향성을 분석하였다. 분석결과 방화벽은 주소변이 대역을 허용을 해야한다는 점에서 기존 정책설정 방식과 차이가 있을 수 있으나 공격표면을 변이하는 네트워크 주소변이 기술로 인해 방화벽 정책이 노출되거나 방화벽 권한 탈취 등에 의해 방화벽 기능이 무력화 될 경우에도 공격자가 쉽게 보호대상 서버와 쉽게 통신할 수 없는 장점이 있다. 또한 네트워크 주소변이 기술이 주소변이 서버의 IP를 변경함에 따라 시그니처 기반의 트패픽 분석 및 행위 규칙을 이용해 탐지하고 차단하는 IPS의 주요 기능에는 영향이 없는 것으로 분석되었다. NAC인 경우 NAC의 주요 대상인 엔드포인트를 대상으로 하지 않고 서버에 NAC 에이전트를 설치하는 예외적인 상황을 제외하면 네트워크 주소변이 기술은 NAC을 운영하는데 영향을 주지 않는다. 마지막으로 네트워크 분석시스템이 수집한 네트워크 데이터 중에 목적지 주소기반으로 데이터를 분석하는 경우가 있는데 이는 목적지 주소변이 환경에서는 문제가 될 수 있으나, 주소변이 기술 적용 시 대표 IP 할당 및 주소변이 이력 정보를 관리하면 네트워크 분석시스템이 이 정보를 활용하여 기존 고정 IP 환경에서와 같이 데이터를 분석할 수 있다. 결론적으로 주소변이 기술은 기존 네트워크 보호체계 내에서 적용되었을 때 주요 시스템에 따라 약간의 차이는 있지만 운용 기능 및 보안정책 상에 배타적이지 않고 상호운용이 가능한 것으로 판단되었으며 사이버 대응체계 내의 네트워크 분석 시스템과의 연동성을 위해 네트워크 주소변이 기술에서 관리해야 할 정보를 제안하였다. 향후 연구 내용로는 정보보호체계의 다른 정보보호 체계에 대한 분석와 기존 운용되는 네트워크 보호체계에 적용하여 다양한 보안시스템과의 상호 연동성 및 주소변이 기술에 적용에 대한 성능적 대한 오버헤드를 비교할 계획이다.

References

[1] K.M.Park, S.Woo, D.S Moon and I.K. Kim, "Trends in Network Address Moving Technology," Electronics and Telecommunications Trends, vol.32, no.6, pp. 73-82, Dec. 2017.

[2] Se-Han Lee and Ki-Woong Park, "A Method for Derivation of Software-Defined MTD Research Direction for secure IoT Device through Analysis of MTD Strategy Research Result," JDCA, vol.5, no.2, pp. 147-158, May 2022.

[3] Luo, Yue-Bin, et al. "RPAH: Random port and address hopping for thwarting internal and external adversaries," Trustcom/BigDataSE/ISPA, vol. 1, pp. 263-270, Aug, 2015.

[4] S. Antonatos, P. Akritidis, E. P. Markatos, and K. G. Anagnostakis, "Defending against histlist worms using network address space randomization," CACM Conference on Computer and Communications Security 2005, pp. 30-40, Nov. 2005.

[5] 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, Oct. 2016.

[6] J. Sun and K. Sun, "DESIR: Decoy-enhanced seamless IP randomization," The 35th Annual IEEE International Conference on Computer Communications, pp. 1-9, Jul. 2016.

[7] Tae-Keun Park, Kyung-Min Park and Dae-Sung Moon, "Attack Surface Expansion through Decoy Trap for Protected Servers in Moving Target Defense" JKSCI, Vol. 24 No. 10, pp. 25-32, Oct. 2019.

[8] Ministry of Government Legislation Korean Law Information Center, "Defense Information Service Order," https://www.law.go.kr/LSW//admRulLsInfoP.do?chrClsCd=&admRulSeq=2100000229796#J2656015, 2023.09.01.

〈저자소개〉

이 수 원 (Suwon Lee) 정회원
2005년 8월: 충남대학교 컴퓨터공학과 졸업
2007년 8월: 충남대학교 컴퓨터공학과 석사
2007년 12월~현재: 한화시스템 수석연구원
〈관심분야〉 사이버 능동방어, 정보보호 정책, 사이버리스크 평가

황 세 영 (Seyoung Hwang) 정회원
2007년 2월: 성균관대학교 전자전기공학과 졸업
2006년 12월~현재: 한화시스템 전문연구원
〈관심분야〉 사이버 능동방어, 정보보호, 해상 사이버보안

홍 석 규 (SeukGue Hong) 정회원
2018년 8월: 국가평생교육진흥원 컴퓨터 공학과 학사
2023년 8월: 국민대학교 일반 대학원 컴퓨터 공학과 석사
2023년~현재: 한화시스템 연구원
〈관심분야〉 정보보호, 컴퓨터공학, 네트워크 보안, 이상탐지