정 보 보 호 학 회 지
제28권 제2호, 2018. 4

네트워크 주소 변이 기반 Moving Target Defense 연구 동향

우 사 무 엘*, 박 경 민*, 문 대 성*, 김 익 균*

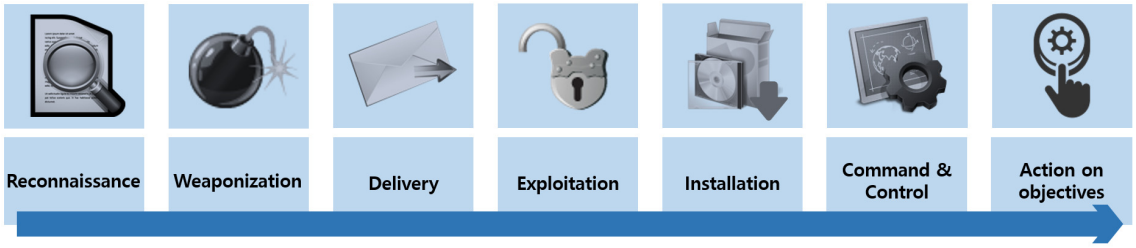
요 약

지능형 지속 위협(Advanced Persistent Threat) 공격은 Intrusion Kill Chain과 같은 일련의 단계로 구성되어 있기 때문에 특정 단계가 차단되면 공격은 실패하게 된다. Moving Target Defense(MTD)는 보호대상의 주요 속성(네트워크, 운영체제, 소프트웨어, 데이터)을 변화시켜 Intrusion Kill Chain을 구성하는 각 단계를 차단하는 능동적 사전 보안 기술이다. MTD 전략 중에서 네트워크 주소 변이(Network Address Mutation) 기술은 보호대상의 네트워크 주소(IP. Port)를 능동적으로 변이하는 기술로써, Intrusion Kill Chain의 첫 단계인 정찰(Reconnaissance) 행위에 소요되는 비용을 급격하게 증가시킬 수 있는 효율적인 보안 기술이다. 본 논문은 네트워크 주소 변이 기술 분야의 관련 연구들을 살펴보고 네트워크 주소 변이 기술 설계 시 고려해야하는 보안 요구사항과 기능 요구사항을 제안한다.

Ⅰ. 서 론

지능형 지속 위협 (Advanced Persistent Threat) 공격과 같은 고도화된 사이버 공격은 체계적인 단계로 구성되어 있으며 이 과정은 Intrusion Kill Chain으로 표현할 수 있다.[1] 그림 1은 Intrusion Kill Chain의 구성과 공격 수행 단계를 나타낸다. 일반적으로 Intrusion Kill Chain에서 어느 한 단계가 차단되면 해당 사이버 공격은 실패하게 된다. 기존의 정보보호 기술들을 사용하면 단기적으로는 Intrusion Kill Chain의 각 단계를 차단할 수 있다. 그러나 현 수준의 반응적/수동적 형태의 정보보호 기술들은 ICT(Information Communication Technology) 인프라의 보안 설정을 정적으로 유지하기 때문에 공격자들이 대상 시스템의 취약점을 분석할 수 있는 충분한 시간과 정보를 제공해 주는 결과를 초래하고 있다.[2] 이 때문에 단기적으로는 공격을 차단하는 것으로 보이지만 장기적으로는 공격자 우위의 비대칭적 공방관계를 형성시킨다.

최근, 공격자 우위의 비대칭적 공방관계를 역전시키기 위해 Moving Target Defense(MTD) 기술이 연구/개발 되고 있다.[3] MTD는 보호대상의 주요 속성을 능동적으로 변화시켜 각종 사이버 공격을 사전에 차단하는



〔그림 1〕 Intrusion Kill Chain의 구성과 공격 수행 단계〔1〕

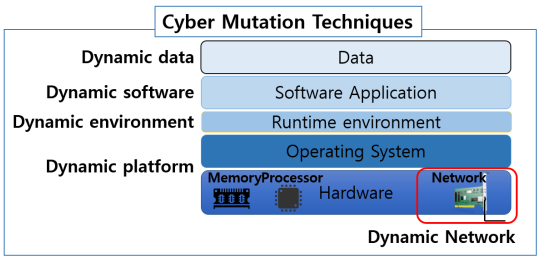
이 논문은 2018년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임(No.2017-0-00213, 능동적 사전보안을 위한 사이버 자가변이 기술 개발)
* 한국전자통신연구원 초연결통신연구소 정보보호연구본부 지능보안연구그룹 (samuelwoo@etri.re.kr, kmpark@etri.re.kr, daesung@etri.re.kr, ikkim21@etri.re.kr)

능동적 사전 보안 기술이다. MTD 기술은 변이(Moving, Mutation)하는 속성에 따라 표 1과 같이 분류된다. 그림 2는 각 요소 기술의 적용 예를 나타내고 있다. 5가지 주요 요소 기술 중 Network Based Moving Target Defense(NMTD)는 보호대상의 네트워크 속성을 변화시켜 Intrusion Kill Chain의 첫 단계인 정찰(reconnaissance)을 어렵게 만드는 매우 효율적인 방어 방법이다. 실제 공격에 앞서 공격자들은 목표 시스템의 취약점을 확보하기 위해 정찰 단계를 수행한다.[4] 공격자들은 수동적으로 네트워크 트래픽을 수집하여 분석하는 스니핑(sniffing) 기술과 능동적으로 다양한 스캐닝 툴을 사용한 프로빙(probing) 기술을 활용하여 목표 시스템의 주요 정보를 획득하게 된다.

NMTD 연구 분야 중 네트워크 주소 변이(Network Address Mutation) 기술은 공격자들의 수동적/능동적 분석 시도 자체를 차단시킬 수 있는 매우 효율적인 보안 기법 중 하나이다. 본 논문에서는 NMTD 기술 중 가장 활발하게 연구되고 있는 네트워크 주소 변이 기술의 동향을 살펴보고 기존 연구들의 한계점을 분석 한다. 그리고 안전하고 효율적인 네트워크 주소 변이 기술 설계를 위해 필수적으로 고려해야 하는 설계 요구 사항을 제안한다.

〔표 1〕 MTD 관련 주요 기술 분류〔3〕

적용 분야(계층)	주요 기술	기술 목표
Network	Moving	Network Mutation
Platform	Multi-variant	Topology Mutation
SW	Multi-variant	Execution Diversification
	Obfuscation	Code Self Randomization
Data	Distribution	Mutated Distributed Data



〔그림 2〕 MTD 요소기술 개념도〔3〕

본 논문은 다음과 같은 순서로 구성된다. 2장에서 네트워크 주소 변이 기술을 정의하고 3장에서 주요 관련 연구들의 특징을 살펴본다. 마지막으로 4장에서 안전하고 효율적인 네트워크주소 변이 기술 설계를 위한 요구 사항을 정의한다.

Ⅱ. 네트워크 주소 변이 기술의 정의

MTD 연구는 연구의 목적에 따라 다음과 같이 3가지 분야로 분류 할 수 있다.[2]

1. MTD Theory: 효과적인 MTD 전략을 수립하는 방법을 연구한다. 보호 대상에서 어떤 속성을 언제 이동시킬지에 대한 설계 원리를 연구한다.
2. MTD Strategy: MTD Strategy는 이동시킬 속성(예, 운영체제, 소프트웨어, 네트워크 구성 및 주소)을 선정하고 해당 속성에 적합한 이동/변이 기술을 설계하는 연구 분야이다.
3. MTD Evaluation: MTD Evaluation은 MTD Strategy 평가에 사용되는 객관적 지표와 정보를 제공하기 위한 방법을 연구한다. 새롭게 설계/개발되는 MTD Strategy 기법들을 평가하는 척도를 마련하는 연구 분야이다.

네트워크 주소 변이 기술은 MTD Strategy 연구 분야 중 하나인 네트워크 동적 변이 기술의 세부 기술이다. 네트워크 주소 변이는 보호대상의 네트워크 주소(IP, Port)를 능동적으로 변이하여 공격자의 정찰 행위를 사전에 차단하는 기술이다.

네트워크 주소 변이 기술은 네트워크 주소를 생성하고 동기화 시키는 방법에 따라 크게 두 가지 분야로 구분할 수 있다.

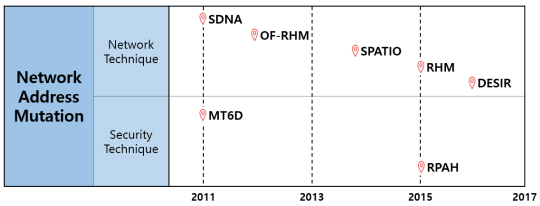
- (네트워크 기술 기반) 실제 IP와 가상 IP 변환을 이용한 NAT(Network Address Translation) 관점의 네트워크 주소 변이 연구로써 가장 활발하게 연구되고 있는 분야이다.
- (정보보호 기술 기반) 암호학적 hash function을 기반으로 네트워크 주소를 생성하고 이를 이용하여 네트워크 주소 변이 기술을 설계하는 연구로써

연구가 시작되는 추세이다.

Ⅲ. 네트워크 주소 이동 기술 동향

본 장에서는 네트워크 주소 변이 기술 관련 주요 연구들의 특징을 살펴본다. 그림 3은 주요 연구 현황을 간단하게 나타낸 것이다. 각 연구들의 주요 특징은 다음과 같다.

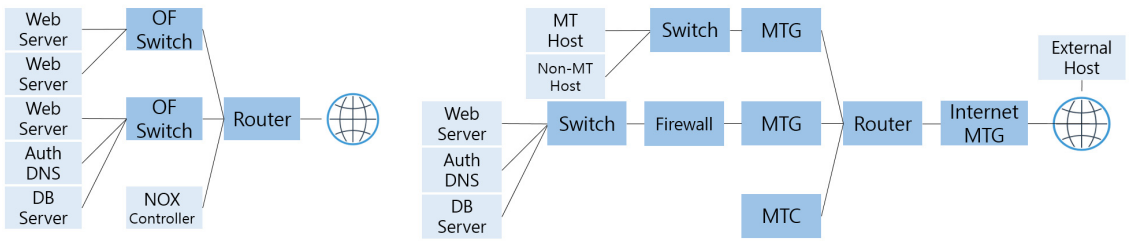
1. (Self-shielding Dynamic Network Architecture) SDNA는 특정 그룹 내부에 소속된 보호대상 호스트들이 IP정보를 노출하지 않고 패킷을 송-수신 하는 기법이다.[5] SDAN Entity가 Token IP를 생성하여 이를 기반으로 익명 통신을 수행한다. 공격자는 보호대상 호스트들의 실제 IP를 분석할 수 없다. 그러나 익명 통신을 수행하기 위해 사용하는 비밀 키를 유지/관리하는 오버헤드가 발생한다. End To End 통신을 수행하는 경우, 송신노드와 수신노드 사이의 경유 노드들까지 비밀 키를 공유해야한다. 이 과정에서 노드간 상호인증과 키 교환 오버헤드가 발생한다. 또한 Token IP를 생성하고 유지/관리 하는 방법에 대해서는 구체적인 기법을제안하고 있지 않다.
2. (OpenFlow-Random Host Mutation) OF-RHM은 보호대상 호스트들에게 가상 IP를 할당하고, 그것을 주기적으로 변환시키는 대표적인 네트워크 주소 변이 연구이다.[6] OF-Switch는 보호대상 호스트의 실제 IP와 가상 IP를 맵핑시켜서 외부에는 실제 IP를 은닉하고, 가상 IP만 공개하도록 한다. OF-RHM은 가상 IP를 주기적으로 변환시켜 네트워크 스캐닝 공격에 소요되는 비용을 증가시킨다. OF-RHM은 SDN에서만 적용 가능한 기술로서 확장성이 부족하다. 이와 함께 가상 IP를 생성하고 관리하는 기법을 제안하고 있지 않다. 그림 4-A는 OF-RHM의 시스템 아키텍처이다.



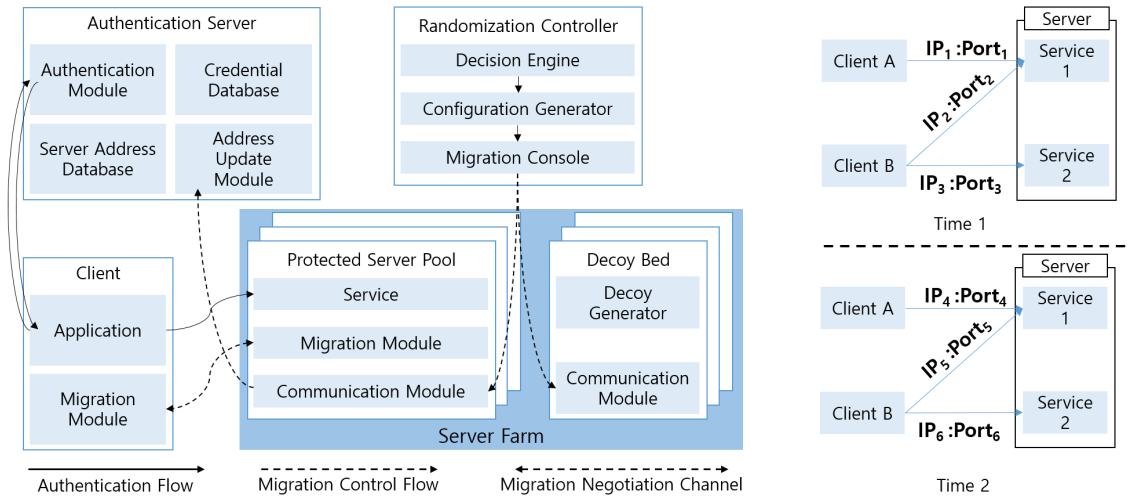
〔그림 3〕 네트워크 주소 변이 기술 연구 흐름

3. (Spatio-temporal Address Mutation for Proactive Cyber Agility against Sophisticated Attackers) SPATIO는 DNS 기반의 IP 주소 변경 기법으로, 아래와 같이 두 가지 방법으로 구성된다.[7]
   - Temporal mutation: 시간단위로 IP 주소 변경
   - Spatial mutation: 주어진 시간에도 복수개의 IP 주소가 할당되어 주소를 변이.

   제어 시스템에서는 주소 변이 전략 및 접근 제어 정책에 따라 실제 IP 주소로의 접근을 제어하고, Gateway는 실제 IP와 가상 IP 간의 변환을 수행한다.
4. (Random Host Mutation: RHM) RHM은 SDN 없이 Legacy 네트워크에 IP 변이 기능을 제공한다.[8] 가상 IP 할당 방식에 있어서 LFM(Low Frequency Mutation)과 HFM(High Frequency Mutation)을 사용한다. LFM은 각 보호대상 호스트에 할당될 수 있는 IP 주소의 범위를 변경하는 기능이다. HFM은 LFM에서 할당된 IP 주소의 범위에 속하는 IP 주소 하나를 각 보호대상 호스트에 가상 IP로 할당하는 주소 변이 기법이다. 그림 4-B는 RHM의 시스템 아키텍처이다.
5. (Decoy-enhanced seamless IP randomization) DESIR는 가상 IP를 사용하는 기존의 연구들과는 다르게 보호대상 호스트의 실제 IP를 랜덤하게 변경하



〔그림 4〕 OF-RHM과 RHM의 시스템 아키텍처 개요



〔그림 5〕 DESIR와 RPAH의 시스템 아키텍처 개요

는 기법을 제안했다.[9] 기존 연구들은 가상 IP를 생성한 후 NAT 또는 SDN을 이용하여 실제 IP와 가상 IP를 변환해 주는 기능을 제안했다.

DESIR에서는 실제 IP와 가상 IP의 변환을 보호대상 호스트에서 수행하는 End-Point-Mutation 개념을 제안했다. End-Point-Mutation으로 인해 외부에서 바라보는 주소 변이의 형태는 보호대상 호스트의 실제 IP주소가 변하는 것으로 보인다. 그러나 DESIR 또한 주소 변이에 사용할 IP를 생성하고 관리하는 방법은 구체적으로 제안하지 않았다, 또한 보호대상 호스트에 접속한 Client의 수가 증가할수록 서비스 지연이 발생하는 심각한 문제점을 내포하고 있다. 그림 5-A는 DESIR의 시스템 아키텍처이다.

6. (Moving Target IPv6 Defense) MT6D는 IPv6환경에서 64bit 크기의 Interface Identifier 값을 동적으로 변환하여 공격자의 분석을 방해하는 익명 주소 사용 기법이다.[10] 송신자와 수신자 사이에 동기화되는 값(시간 정보 등)을 One-way Hash function의 입력 값으로 사용하여 상호간에 동기화된 익명 주소를 생성한다. 다수의 IPv6 address를 저장하기 때문에 메모리 오버헤드가 상승하고, routing update비용이 발생하게 된다.
7. (Random port and address hopping) RPAH는 Hopping interval을 사전에 정의하고, interval마다 보호대상의 IP 와 Port를 변이하는 기법을 제안했다.[11] 이들은 가상 주소를 생성하기 위해 pseudo-random function을 사용했다. 이들의 기법을 실제 환경에 적용하기 위해서는 보호대상의 기존 Gateway에 주소 변이 기능을 추가해야 한다. 또한 pseudo-random function을 사용하여 IP와 Port를 생성하는 경우 발생 가능한 주소 충돌 문제를 고려하지 않았다. 5-B는 RPAH의 시스템 아키텍처이다.

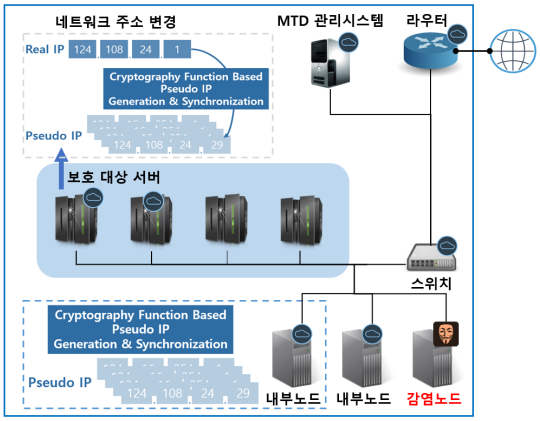
앞에서 살펴본 7가지 기존 연구들 외에도 다양한 네트워크 주소 변이 기법들이 발표되었다.[15][16][17] 기존 연구들은 네트워크 주소 생성과 변이를 위해 NAT 형태의 주소 변이 방법과 암호알고리즘을 이용한 주소 생성 방법을 사용하고 있다.

그러나 NAT 형태의 주소 변이의 경우 주소 변이 행위가 보호대상 호스트에서 수행되지 않는다면 보호대상 호스트와 동일한 서브네트워크에 위치한 내부 공격자에게 보호대상 호스트의 실제 주소가 노출될 가능성을 내포하고 있고, 암호알고리즘을 사용하여 네트워크 주소를 생성하는 경우 서로 다른 입력에 대한 동일한 출력값이 발생하는 주소 충돌 문제가 발생할 수 있다. 또한 대부분의 기법의 경우 정해진 시간마다 주소 변이를 수행하는 주기적 주소 변이 방식을 사용하고 있으나, 침입탐지시스템이나 관리시스템의 요청에 따라 비 주기적으로 주소 변이를 수행 할 수 있는 비 주기적 주소 변이 프로세스도 고려해야 한다. 이처럼 기존 연구들은 크고 작은 문제점들을 내포하고 있다. 3장에서 분석한 기존

연구들의 특성을 기반으로 4장에서는 네트워크 주소 변이 기법을 설계할 때 고려해야하는 요구 사항을 제안한다.

Ⅳ. 네트워크 주소 변이 기술 설계 고려사항

DESIR를 제외한 대부분의 연구들은 가상 IP와 실제 IP를 변환해주는 NAT방식을 기반으로 네트워크 주소 변이 기법을 설계하였다. 이 경우 그림 6과 같은 환경에서 내부 공격자에게 보호대상 호스트의 실제 IP가 노출되는 문제점이 발생한다.[11] 또한 대부분의 기법들은 네트워크 주소 변이에 사용할 주소를 생성하고 관리하는 기법을 제안하고 있지 않다. 다음 4가지 사항을 고려하여 네트워크 주소 변이 기술을 설계한다면 안전성과 효율성이 강화된 네트워크 주소 변이 기술을 설계할 수 있을 것으로 사료된다.



〔그림 6〕 네트워크 주소 변이 적용 환경

4.1. 네트워크 주소 변이 시스템 아키텍처

네트워크 주소 변이는 주기적/비주기적으로 수행될 수 있다. 주기적 주소 변이의 경우 보호대상 호스트와 클라이언트들이 정해진 주기마다 주소를 변경한다. 이 때 네트워크 주소 생성 및 동기화 기능은 각 각의 호스트에서 수행 될 수 있으므로 관리시스템의 제어를 최소화한 분산형 구조의 주소 변이 시스템을 운영할 수 있다. 분산형 구조의 경우 주소 변이를 위해 발생되는 제어 패킷의 오버헤드를 감소시킬 수 있다.

비주기적 네트워크 주소 변이의 경우 관리시스템의 판단에 따라 보호대상 호스트의 주소를 변경하는 중앙 집중형 구조의 주소 변이 시스템을 운영할 수 있다. 이 경우 주소 생성 및 분배를 관리시스템에서 수행하는 것이 보다 효율적이다. 다만 주소 변이를 위한 제어 패킷이 부가적으로 발생한다. 이처럼 분산형 구조와 중앙 집중형 구조는 각각의 장점과 단점이 존재한다. 네트워크 주소 변이 기술을 적용하는 인프라의 특성에 따라 분산형 구조와 중앙 집중형 구조를 고려하여 네트워크 주소 변이 기술을 설계해야 한다.

4.2. 네트워크 주소 생성, 동기화 및 충돌회피

공격자가 유추 할 수 없는 네트워크 주소를 생성하기 위하여 MT6D와 같은 기법에서는 암호학적 hash function을 사용했다. 보호대상 호스트와 클라이언트 사이에서 비밀키만 잘 관리한다면 효율적으로 익명 주소를 생성할 수 있다. 다만 다음 두 가지 사항은 필수적으로 고려해야 한다. 첫째, 특정 서브네트워크 안에서 하나 이상의 보호대상 호스트를 운영하는 환경의 경우 네트워크 주소 변이 시 마다 서로 다른 네트워크 주소를 각 각의 보호대상 호스트에게 할당해야한다. hash function의 경우 서로 다른 입력에 대해 동일한 출력이 발생할 수 있으므로 충돌회피 기능을 고려해야 한다. 둘째, 보호대상 호스트와 클라이언트가 주소변이를 동기화하기 위해서는 동기화가 가능한 입력 파라메터(시간 동기화, 카운터 등)를 사용하여 주소 생성에 사용해야 한다.

4.3. 네트워크 주소 변이 기능 수행 위치

가상 IP와 실제 IP를 변환해주는 방식의 네트워크 주소 이동 기술은 보호대상 호스트의 실제 네트워크 주소를 변경하는 것이 아니라, 외부에 공개된 가상 주소를 실제 주소로 맵핑 시켜주는 기술이다. 해당 기술은 그림 6과 같이 공격자가 보호대상과 동일한 내부망에 위치하는 공격 모델에서는 실제 IP가 공격자에게 노출되는 문제가 발생한다. 이를 해결하기 위해서는 보호대상 호스트의 실제 IP를 변경하는 관점의 End Point Address Mutation을 고려해야 한다.

4.4. 개체 인증 및 키 관리

네트워크 주소 변이에 사용되는 주소를 생성하고 안전하게 관리하기 위해서는 개체 인증과 키 관리 기능이 필요하다. 특히 암호학적 hash function을 사용하여 네트워크 주소를 생성하는 기법의 경우 안전한 키 관리는 필수적으로 고려되어야한다.

Ⅴ. 결 론

본 논문에서는 네트워크 주소 변이 기술과 관련된 기존 연구들의 동작원리를 간단히 요약한 뒤, 이들 기술들이 실제 네트워크에 적용되기 위해 해결해야할 문제점들을 분석하였다. 또한, 공격자의 공격 위치 및 네트워크 주소 변이 기술 적용 환경을 기준으로 내부 공격자 위협 모델에 대하여 서술한 후 이를 극복하기 위한 요구사항들을 제안하였다. 안전하고 효율적인 네트워크 주소 변이 기법을 설계하기 위해서는 본 논문이 제안한 기술 설계 고려사항을 만족해야 한다. 물론 네트워크 주소 변이 기술 자체만으로는 공격자의 취약점 분석 행위를 완벽하게 차단할 수 없다.[13] 향후 네트워크 Fingerprinting Mutation[14] 기술과 Decoy Operation 기술을 네트워크 주소 변이 기술과 함께 융합한다면 안전성이 강화된 네트워크 동적 변이 기술을 설계할 수 있을 것으로 사료된다.

참 고 문 헌

[1] Martin, Lockheed. “Cyber Kill Chain.” Available: http://cyber.lockheedmartin.com/hubfs/Gaining the Advantage Cyber Kill Chain.pdf, 2014

[2] Cai, Gui-lin, et al, “Moving target defense: state of the art and characteristics,” Frontiers of Information Technology & Elec-tronic Engineering, pp. 1122-1153, 2016.

[3] Hamed, et al. “Finding focus in the blur of moving-target techniques.” IEEE Security & Privacy pp. 16-26, 2014.

[4] D. Kewley, R. Fink, J. Lowry and M. Dean, “Dynamic Aproaches to Thwart Adversary Inteligence Gathering,” Procedings of the DARPA Information Survivabilty Conference and Expositon, p. 176-185, 2001.

[5] Yackoski, Justin, et al. "A self-shielding dynamic network architecture." Military communications conference, 2011-MILCOM 2011. IEEE, 2011.

[6] Jafarian, Jafar Haadi, Ehab Al-Shaer, and Qi Duan. "Openflow random host mutation: transparent moving target defense using software defined networking." Workshop on Hot topics in software defined networks. ACM, 2012.

[7] Jafarian, Jafar Haadi H., Ehab Al-Shaer, and Qi Duan. "Spatio-temporal address mutation for proactive cyber agility against sophisticated attackers." Proceedings of the First ACM Workshop on Moving Target Defense. ACM, 2014.

[8] 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.

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

[10] Dunlop, Matthew, et al, “Mt6d: A moving target ipv6 defense,”IEEE Military Communications Conference, 2011.

[11] Luo, Yue-Bin, et al. “RPAH: Random port and address hopping for thwarting internal and external adversaries.” Trustcom/BigDataSE/ISPA, Vol. 1, 2015.

[12] K.M.Park, S.Woo, D.S.Moon, and I.K.Kim, “Trends in Network Address Moving Technology,” ETRI Electronics and Telecommunication Trends, Vol 32, 2017

[13] K.M.Park, S.Woo, D.S.Moon, and H. Choi, “Secure Cyber Deception Architecture and Decoy Injection to Mitigate the Insider Threat”, Symmetry, 2018

[14] Zhao, Zheng, Fenlin Liu, and Daofu Gong, “An SDN-Based Fingerprint Hopping Method to Prevent Fingerprinting At-tacks,” Security and

Communication Networks, 2017.
[15] M. Atighetchi, P. Pal, F. Webber, and C. Jones, “Adaptive Use of Network-Centric Mechanisms in Cyber-Defense,” In Object-Oriented Real-Time Distributed Computing, Sixth IEEE International Symposium on (pp. 183-192). 2003
[16] S. Antonatos, P. Akritidis, E.P. Markatos, and K.G. Anagnostakis, “Defending against hitlist worms using network address space randomization,” Computer Networks, 51 (pp. 3471-3490) 2007.
[17] J. H. Jafarian, A. Niakanlahiji, E. Al-Shaer, and Q. Duan, “Multi-dimensional Host Identity Anonymization for Defeating Skilled Attackers,” Proceedings of the 2016 ACM Workshop on Moving Target Defense, (pp. 47-58) 2016

〈저 자 소 개〉

우 사 무 엘 (Woo Samuel)
2016년 8월 : 고려대학교 정보보호대학원 정보보호학 박사
2016년 10월~현재 : 한국전자통신연구원 정보보호연구본부
관심분야 : 정보보호, 네트워크보안, 자동차보안

박 경 민 (Park Kyungmin)
2013년 2월 : 충남대학교 컴퓨터공학과 석사
2017년 2월~현재 : 한국전자통신연구원 정보보호연구본부
관심분야 : 정보보호, 네트워크보안, 분산시스템

문 대 성 (Moon Daesung)
정회원
2007년 2월 : 고려대학교 전산학과 박사
2000년 12월~현재 : 한국전자통신연구원 정보보호연구본부
관심분야 : 정보보호, 네트워크보안, 영상처리, 바이오인식

김 익 균 (Kim Ikkyun)
정회원
2009년 2월 : 경북대학교 컴퓨터공학과 박사
2001년~현재 : 한국전자통신연구원 정보보호연구본부
관심분야 : 정보보호, 네트워크보안, 클라우드 컴퓨팅