2020 한국차세대컴퓨팅학회
하계학술대회

장　　소 : 제주 JDC(엘리트빌딩)

일　　시 : 2020. 8. 20(목) 14:00 ~ 8. 22(토) 12:00

주최 · 주관 : 한국차세대컴퓨팅학회, 제주드론산업협회

클라우드 환경을 위한 소프트웨어 정의 기반 MTD 프레임워크 대시보드 디자인 및 구현

Design and Implementation of a Software-Defined MTD Framework Dashboard for Cloud Environments

강기완[1], 박기웅[2,*)]

Ki-Wan Kang, Ki-Woong Park

[1](05006) 서울특별시 광진구 능동로, 세종대학교 시스템보안연구실

[2](05006) 서울특별시 광진구 능동로, 세종대학교 정보보호학과

kkwan0226@gmail.com, woongbak@sejong.ac.kr

요 약

기업 운영에 있어 효율성, 유연성, 경제성 등을 극대화하기 위해 클라우드를 도입하고 있지만 클라우드 도입에 따른 보안위협도 발생하고 있다. 이를 해결하고자 공격 과정에 있어 첫 단계인 정찰 단계를 어렵게 만들어 비대칭적 공방 관계를 역전 시킬 수 있는 네트워크 기반 MTD(Moving Target Defense) 연구가 활발하게 진행되고 있다. 그러나 네트워크 기반 MTD 연구를 실제 시스템에 적용하기에는 연구별로 상이한 소프트웨어 및 시스템 도입을 요구한다. 따라서 본 논문에서는 기존 네트워크 MTD 연구 및 향후 연구 개발 될 네트워크 기반 MTD 연구를 소프트웨어 정의 기술을 통해 용이하게 적용할 수 있게 3가지(Agility, Interoperability, Adaptiveness)의 프레임워크 요구사항을 도출하였다. 도출한 요구사항을 바탕으로 소프트웨어 정의 기반 MTD 프레임워크 대시보드를 디자인 및 구현하였다.

키워드: Cloud, Network-based Moving Target Defense, Software-Defined, Framework

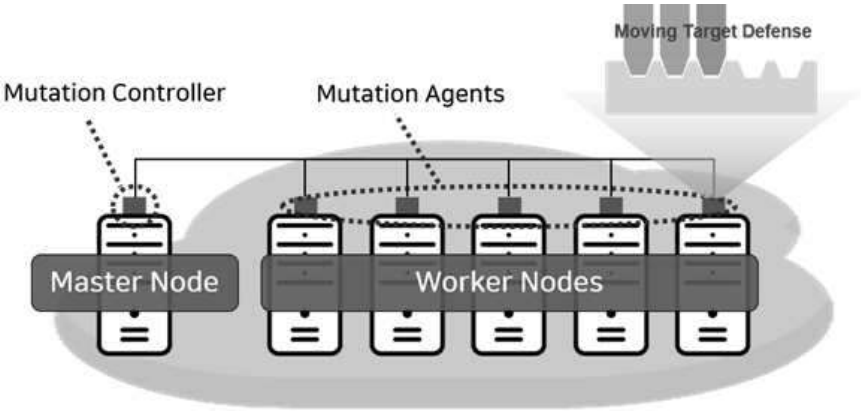
1. 서론

4차 산업혁명에 있어서 기반 인프라의 역할을 하고 있는 클라우드 컴퓨팅은 사용자가 요구하는 만큼의 컴퓨팅 자원을 활용할 수 있게 하는 컴퓨팅 방식이다[1]. 기업 운영에 있어 효율성, 유연성, 경제성 등을 극대화하기 위해 클라우드를 도입하고 있지만 시스템 취약점, APT(Advanced Persistent Threat), DoS(Denial of Service) 등 다양한 보안 위협들이 발생하고 있다[2].

현재 클라우드 컴퓨팅 시스템은 초기 지정한 속성에 대해 정적으로 유지하기 때문에 공격자들에게 대상 시스템의 취약점을 분석할 수 있는 충분한 시간과 정보를 제공할 수 있다. 이러한 공격자 우위의 비대칭적 공방 관계를 역전시키기 위해 보호대상의 주요 속성(네트워크, 플랫폼, 실제환경, 소프트웨어, 데이터 등)을 능동적으로 변화시켜 다양한 보안 위협을 사전에 차단하는 연구인 MTD(Moving Target Defense) 연구 개발이 활발하게 진행되고 있다[3]. 다양한 MTD 기술 중 공격 과정에 있어 첫 단계인 정찰 단계를 어렵게 만들어 비대칭적 공방 관계를 역전 시킬 수 있는 네트워크 기반 MTD는 매우 효율적인 방어 방법으로 꼽힌다[4]. 그러나 네트워크 기반 MTD 연구는 각 연구별 상이한 소프트웨어 및 시스템 도입을 요구한다.

따라서 본 논문에서는 기존 네트워크 MTD 연

* 교신저자



(그림 1) Overview of Software-Defined MTD

구 및 향후 연구 개발 될 네트워크 기반 MTD 연구를 소프트웨어 정의 기술을 통해 용이하게 적용할 수 있는 프레임워크 요구사항을 도출하였다. 도출한 요구사항을 바탕으로 도출한 요구사항을 바탕으로 소프트웨어 정의 기반 MTD 프레임워크 대시보드를 디자인 및 구현하였다.

본 논문의 구성은 다음과 같다. 2장에서는 기존 네트워크 기반 MTD 연구 분석을 통해 각 연구별 요구사항을 분석하고, 3장에서는 기존 네트워크 기반 MTD 연구 및 향후 연구 개발 될 네트워크 기반 MTD 연구를 용이하게 적용할 수 있는 프레임워크의 필요성 및 요구사항을 도출하고, 4장에서는 소프트웨어 정의 기반 MTD 프레임워크의 대시보드를 디자인 및 구현하였다. 마지막으로 5장에서는 본 논문의 결론 및 향후 연구방향에 대해 기술한다.

2. 관련 연구

본 장에서는 기존 네트워크 기반 MTD 연구 분석을 통해 각 연구별 실제 시스템에 적용함에 있어 추가적으로 요구되는 사항을 도출하였다.

- RPAH(Random Port and Address Hopping)

Yue-Bin Luo, et.al[5]는 IP 주소와 통신 포트를 지속적으로 그리고 예측 불가능하게 하는 메커니즘을 제안하였다. 해당 메커니즘을 시스템에 적용하기 위해서는 보호하고자 하는 대상 시스템의 Gateway에 추가적으로 해당 기능을 구현해야한다.

- RHM(Random Host Mutation)

Al-Shaer, et.al[6]는 보호하고자 하는 대상 시스템이 사용할 수 있는 가상 IP 주소의 범위를 변경하는 역할을 수행하는 LFM(Low Frequency Mutation)과 LFM에서 지정한 IP 범위 내에 있는 IP 주소를 할당하는 역할을 하는 HFM(High Frequency Mutation)을 통해 가상 IP를 할당하는 메커니즘을 제안하였다. 해당 메커니즘을 시스템에 적용하기 위해서는 스위치와 라우터 사이에 MTG(Mutation Gateway)를 배치해야 한다.

- Decoy-Based MTD

Andrew Clark, et.al[7]는 공격자가 실제 시스템을 타겟팅 하는 것을 방지하기 위해 다수의 디코이 시스템을 도입한다. 또한 시스템의 네트워크 주소뿐만 아니라 디코이 시스템의 네트워크 주소도 함께 변이시키는 것을 제안하였다. 해당 메커니즘을 시스템에 적용하기 위해서는 디코이 시스템을 추가적으로 운용해야 한다.

- HIDE(Host IDEntify Anonymization)

Jafarian, et.al[8]는 Al-Shaer, et.al[6]이 제안한 RHM 모델에 허니팟 클라우드를 도입하여 공격자가 대상 시스템의 네트워크 속성을 탐색하지 못하도록 하는 메커니즘을 제안하였다. 허니팟 클라우드는 공격자의 대상 시스템과 다른 네트워크에 위치하고 있으며, 외부망에 존재하는 MTG를 통해 의심스러운 트래픽의 경우 허니팟 클라우드로 리다이렉션 한다. 해당 메커니즘을 시스템에 적용하기 위해서는 허니팟 클라우드를 추가적으로 운용해야 한다.

3. 소프트웨어 정의 기반 MTD 프레임워크 요구사항 도출

본 장에서는 소프트웨어 정의 기반 MTD 프레임워크의 필요성을 제시하고, 그에 따른 요구사항을 도출한다.

3.1 소프트웨어 정의 기반 MTD 프레임워크의 필요성

본 논문에서는 소프트웨어 정의 기반 MTD 프레임워크의 필요성을 크게 두 가지로 구분하였다.

• 추가적인 기능 구현

Yue-Bin Luo, et.al[5], Al-Shaer, et.al[6]이 제안한 RPAH, RHM은 보호하고자 하는 대상 시스템의 IP 주소 및 통신 포트를 변경하여 대상 시스템의 공격 복잡도를 높이는 연구이다. 그러나 해당 메커니즘은 추가적으로 기존에 존재하던 게이트웨이에 기능을 구현하거나, 새로운 게이트웨이 추가를 요구한다.

• 추가적인 시스템 도입

Andrew Clark, et.al[7], Jafarian, et.al[8]이 제안한 Decoy-based MTD, HIDE는 보호하고자 하는 대상 시스템의 네트워크 속성의 변경뿐만 아니라 추가적으로 시스템을 도입하여 공격 복잡도를 높이는 연구이다. 그러나 해당 메커니즘은 RPAH, RHM 등과 같은 연구에 추가적으로 Decoy 시스템 및 허니팟 클라우드를 도입하는 것을 요구한다.

3.2 소프트웨어 정의 기반 MTD 프레임워크 요구사항 도출

본 논문에서는 소프트웨어 정의 기반 MTD 프레임워크의 요구사항에 대해 도출하였다.

• Agility

기존의 네트워크 기반 MTD 연구 및 향후 연구 개발 될 네트워크 기반 MTD 연구들을 수용할 수 있어야 한다. 이를 통해 다양한 네트워크 속성(IP/MAC 주소, 포트, 라우팅 경로 등)을 동적으로 변경시키고, 다양성을 제공하여 높은 공격 복잡도를 제공할 수 있어야 한다.

• Interoperability

다양한 네트워크 속성을 동적으로 변경시키고, 다양성을 제공하기 위해선 특정 환경(운영체제, 네트워크 장비 등)에 종속되지 않고, 상호 운용성을 보장할 수 있어야 한다.

• Adaptiveness

특정 조건 및 환경에 따라 동적으로 변경하고자 하는 네트워크 속성을 관리하여 유효한 범위 내에 보호하고자 하는 대상 시스템이 위치할 수 있도록 해야 한다.

4. 소프트웨어 정의 기반 MTD 프레임워크 대시보드 디자인 및 구현

본 장에서는 앞서 도출한 소프트웨어 정의 기반 MTD 프레임워크의 요구사항을 바탕으로 프레임워크의 대시보드 디자인 및 구현에 대해 다룬다. 소프트웨어 정의 기반 MTD 프레임워크 대시보드는 크게 세 부분으로 분류하였으며, 각 부분의 역할은 다음과 같다.

• MTD Mechanism

기존 네트워크 기반 MTD 연구 및 향후 연구 개발 되는 네트워크 기반 MTD 연구를 소프트웨어화하여 상황에 맞는 메커니즘을 적용하는 부분

• Management

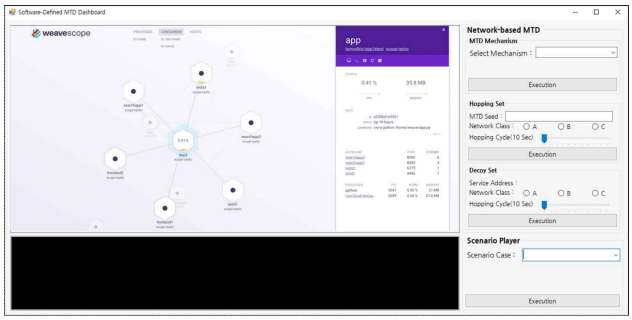
네트워크 기반 MTD 연구에 있어 주된 변이 요소인 네트워크 주소 변이 속성(Seed, Network Class, Hopping Cycle)을 설정하는 부분

• Situation Visualization

현재 구동 중인 서비스들의 상황 및 상태 파악을 위함

• Terminal

시나리오 실행에 따른 결과 및 관련 로그들을 확인하기 위함



(그림 2) Software-Defined MTD Dashboard

5. 결론 및 향후 연구 방향

본 논문에서는 클라우드 환경을 위한 소프트웨어 정의 기반 MTD 프레임워크 설계 및 구현에 앞서 해당 프레임워크의 필요성 및 요구사항을 제시한다.

현재 클라우드 컴퓨팅 시스템의 정적인 보안 설정으로 인해 공격자들이 대상 시스템의 취약점을 분석할 수 있는 충분한 시간과 정보를 제공한다. 이러한 공격자 우위의 비대칭적 공방 관계를 역전

시키기 위해 MTD 연구 개발이 활발하게 진행되고 있다. 그러나 관련 연구 분석을 통해 활발히 연구되고 있는 네트워크 기반 MTD 연구는 각 연구 별 상이한 소프트웨어 및 시스템 도입을 요구한다. 따라서 본 논문에서는 소프트웨어 정의 기반 MTD 프레임워크를 통해 기존 네트워크 기반 MTD 연구 및 향후 연구 개발 될 네트워크 기반 MTD 연구를 용이하게 적용할 수 있도록 하는 것을 목표로 한다.

이러한 소프트웨어 정의 기반 MTD 프레임워크 설계 및 구현에 앞서 본 논문에서는 소프트웨어 정의 기반 MTD 프레임워크의 요구사항으로 3가지 항목(Agility, Interoperability, Adaptiveness)을 제시한다. 더 나아가 본 논문에서는 해당 요구사항을 바탕으로 소프트웨어 정의 기반 MTD 프레임워크의 대시보드에 대해 디자인 및 구현하였다.

향후 도출된 요구 사항에 따라 소프트웨어 정의 기반 MTD 프레임워크 설계 및 구현하는 연구를 수행한다면 다양한 MTD 연구들을 용이하게 적용할 수 있을 것으로 사료된다.

Acknowledgement

본 연구는 2019년도 과학기술정보통신부의 재원으로 정보통신기획평가원(No.2018-0-00420)의 지원 및 한국연구재단 연구과제(NRF-2020R1A2C4002737)의 지원을 받아 수행된 연구임.

참고문헌

[1] 이아름, “클라우드컴퓨팅 시장 및 정책동향”, 융합연구정책센터, vol 111, 2018. 3.

[2] 정성재, 배유미, 클라우드 보안 위협요소와 기술 동향 분석“, 보안공학연구논문지, 제 10권 제 2호, pp.199-212, 2013. 4.

[3] “Moving Target Defense 기반 능동형 서비스 보안 지침”, 한국정보통신기술협회, 2019

[4] 우사무엘, 박경민, 문대성, 김익균, “네트워크 주소 변이 기반 Moving Target Defense 연구 동향”, 정보보호학회지, 제 28권 제 2호, 2018. 4.

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

[6] Al-Shaer, Ehab, Qi Duan, and Jafar Haadi Jafarian. "Random host mutation for moving target defense." International Conference on Security and Privacy in Communication Systems. Springer, Berlin, Heidelberg, 2012.

[7] Clark, Andrew, Kun Sun, and Radha Poovendran. "Effectiveness of IP address randomization in decoy-based moving target defense." 52nd IEEE Conference on Decision and Control. IEEE, 2013.

[8] Jafarian, Jafar Haadi, et al. "Multi-dimensional host identity anonymization for defeating skilled attackers." Proceedings of the 2016 ACM Workshop on Moving Target Defense. 2016.