Moving Target Defense 이슈 및 평가인증 요구사항에 대한 연구

문서연*, 김재웅*, 박종혁**
*한국정보통신기술협회 융합기술표준단
**서울과학기술대학교 컴퓨터공학과
e-mail: moonsy0621@tta.or.kr

A Study on Moving Target Defense Issue and Certification Requirements

Seo Yeon Moon*, Jae Woong Kim*, Jong Hyuk Park**
*Dept of Convergence Technology Standardization, Telecommunications Technology Association(TTA)
**Dept of Computer Science and Engineering, Seoul National University of Science and Technology(Seoultech)

요 약

2011년 미국에서 최초로 소개된 후 기존 보안 기술과 다른 새로운 정보시스템 보호 기술로 Moving Target Defense(MTD)가 활발히 연구 되고 있다. MTD는 시스템의 구성 요소들을 불규칙적이고 동적으로 변화시켜 공격표면(Attack surface)을 줄임으로써 외부 공격에 대한 보안성을 높인다. 주로 시스템 정보를 수집 및 분석하여 공격하는 보안 위협들에 효과적이며 특히 지능형 지속 보안 위협(Advanced Persistent Threat), 킬 체인(Kill-Chain) 보안에 뛰어난 성능을 기대할 수 있다. 최근 MTD 시스템 구현 및 개발로 상용화가 시작되었으나 MTD 활용을 통해 어느 정도의 보안성 및 효율성을 가지는지에 대한 성능 평가인증, 시험지침 등이 표준화 되어있지 않아 기준이 모호한 실정이다. 본 논문에서는 이러한 최근 MTD 이슈에 대해 살펴보고 MTD와 연관 되어있는 각 분야에 어떤 평가인증 요구사항들이 있는지 분석한다. 이를 통해 MTD에 어떠한 평가인증 요구사항이 있는지 도출하여 앞으로 MTD 평가인증 표준화 참고 및 활용에 기여 할 수 있을 것으로 전망한다.

1. 서론

MTD 기술은 2011년 미국 백악관의 “연방정부의 사이버보안 R&D를 위한 전략적 계획” (Trustworthy Cyberspace: Strategic Plan for The Federal Cybersecurity Research and Development Program) 발표에서 처음 언급 되었으며, 국내에서는 2012년 한국인터넷진흥원에서 처음 소개 되었다. 2012년부터 시스템 구성요소(SW, Device 등)에서 MTD 기술을 활용 할 수 있는 요구사항 도출 연구로 시작하여 네트워크 기반(Router, Switch, SDN, Web) MTD 기술 연구가 주를 이루고 있다. 최근에는 스마트그리드, 커넥티드카, 클라우드 기반, 인공지능, 고도화된 랜덤알고리즘 등 융합기술 분야에서 MTD 서비스모델 및 강화된 보안 모델 연구가 활발하며 국내에서는 한국전자통신연구소, GIST, 국방부 등에서 네트워크, 인공지능 기반 MTD 개발이 진행되고 있다.

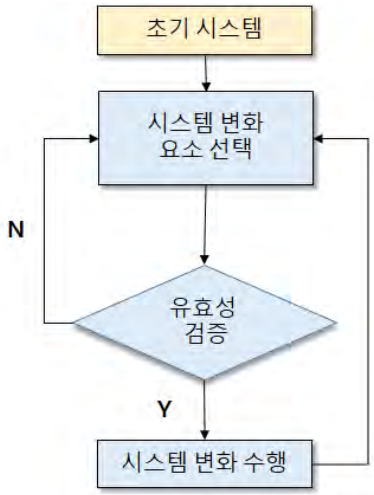
MTD는 시스템 구성요소를 동적으로 배치 및 운영하여 공격에 대한 비용을 크게 높이고 결정적 공격 방법 수를 줄이며, 시스템 정적 및 동질성을 약화시키는 것을 의미한다. 즉, 공격자의 복잡성과 비용을 높이고 취약성과 공격 기회를 제한하며 시스템 탄력성을 높이기 위해 시간의 흐름에 따라 지속적으로 정보를 변경하는 것이다 [1]. MT는 기존 정보보안의 탐지, 대응, 분석 등의 틀을 벗어나 시스템의 공격표면을 줄이는 또 다른 보안 방법으로 낮은 비용 대비 높은 효율을 기대할 수 있다 [2]. 하지만 해당 분야의 연구가 채 10년이 되지 않아 이슈가 많이 존재하며 그 중 시스템 영향보고서, 평가인증, 시험지침 등에 대한 연구가 시급하다. 본 논문에서는 이러한 최근 MTD 이슈에 대해 살펴보고 MTD와 연관되어있는 각 분야의 어떤 평가인증 요구사항들이 있는지 분석한다. 이를 통해 MTD 평가인증 요구사항 도출하여 표준화 활용 및 연구 방향에 대해 논의한다.

2. 관련연구

본 장에서는 MTD 기술 및 이슈에 대해 설명보고 MTD 평가인증 요구사항을 도출하기 위해 관련 분야의 평가는 어떠한 것들이 있는지 살펴본다.

2.1 MTD 기술

MTD는 공격자가 악용할 수 있는 광범위한 공격 표면을 줄이기 위해 시스템을 지속적으로 변화 시키는 것을 의미한다. 일반적으로 시스템의 공격 가능한 영역은 공격자가 접근할 수 있는 모든 리소스를(예: 소프트웨어, 열린 포트, 구성 요소 취약점을 통해 제공되는 기타 리소스 등) 포함한다. MTD 시스템의 기본 프로세스는 그림 1과 같다 [3-5].



(그림 1) MTD 기본 프로세스

첫 번째 단계는 운영 환경에서 시스템의 초기 배치를 의미하며 시스템이 실행될 때 MTD 시스템은 시스템 변화를 수행하기 위한 요소를(Adaptation) 선택한다. 선택이 가능한 요소로는 네트워크, 소프트웨어, 보안에서 사용되는 정보가 있다. 시스템 변화의 수행의 시점은 고정적이거나, 임의적이거나, 혹은 시스템에 공급되는 외부 정보에 의해 결정될 수 있다. 모든 운영 시스템에는 자원의 제한이 있으므로, 선택된 구성에 대한 배치의 결과는 현재 시스템에서 적합한지 유효성에 대해 점검되어야 한다. 적합하지 않다면, 시스템 변화를 주지 않고 새로운 요소들을 선택 한다.

2.2 MTD 이슈

MTD는 2012년부터 연구가 진행되어 아직 연구 초기단계라 볼 수 있으며 발전하기 위한 많은 이슈들이 존재한다. 먼저 현재 상용화된 MTD 기술은 네트워크 환경 요소들로 한정적이며 일반적으로 보안 솔루션에서 추가기능으로 활용되고 있다. 특정 도메인이나 큰 규모의 시스템에서 활용하기 위해서는 단일로 활용 할 수 있는 모델과 이를 위한 복원력 있는 관리 및 제어 메커니즘 개발 등이 함께 연구되어야 한다.

또 다른 이슈로는 MTD의 성능 및 효율성의 과학적 추론에 대한 평가 및 방법 개발이 있다. MTD를 통해 시스템에 주는 영향력에 대한 보고서가 아직 정립되지 않았으며 불규칙성에 따른 효율성 입증 및 가치에 대한 연구가 필요한 실정이다. 따라서 MTD 성능 평가 기준, 지침, 시험 운용 모델 등에 대한 연구 등이 필요하다.

2.3 MTD 관련 분야 평가

MTD 기술에서 상용화 및 활용 가능성이 제기된 분야는 네트워크, 소프트웨어, 보안이 있으며 본 절에서는 각 분야별 평가 및 시험 요소들이 어떤 것들이 있는지에 대해 살펴본다.

2.3.1 네트워크 평가

네트워크 성능 평가로는 IEEE.802.11 문서를 기준으로 국내에서 평가 지침 및 시험 항목을 준용하고 있으며 주로 네트워크 기능. 서비스, 성능 시험으로 구분된다. 평가으로는 SSID 적용여부, 인증, 데이터 페이로드, WEP키 설정, RTS 및 CTS, IBSS, WPA 등 13가지 항목이 있다 [6]. 이를 참고 하여 홈 게이트웨이, 무선접속 성능평가 방법, 무선랜 시험규격, 차량 LAN 시험 규격 등 각 분야 환경 및 국내 ICT 서비스 등을 고려하여 활용되고 있다 [7-9]. 이 외에 TTA 네트워크 보안장비에 대한 성능 측정 방법에서 패킷, 트래픽에 따른 처리율과 지연시간 측정 및 기준에 대해 설명하고 있으며 테스트 환경 및 방법을 다루고 있다 [10].

2.3.2 소프트웨어 평가

소프트웨어의 경우 다양한 실행 환경, 장치, 목적 등으로 개발되기 때문에 타 평가보다 상대적으로 더 광범위한 평가인증 지침들이 있다. 각 응용계층 서비스에 적절히 운용 될 수 있는 지침, 일반적인 시스템의 소프트웨어 기능 평가 및 운용 지침, 소프트웨어 자체 성능 시험 등 이 있으며 각 평가인증 문서에서 운영체제, 하드웨어성능, 버전, 소프트웨어 언어별로 분류되어있다. 국내에서 GS 시험인증, CC평가, 확인 및 검증시험, 벤치마크테스트 등이 있으며 일반적으로 기능성, 사용성, 이식성, 성능효율성, 유지보수성, 신뢰성, 공급업체지원 항목을 기준으로 평가 한다. 국내 평가의 주요 준용 문서로는 국가표준(KS) 정보기술-소프트웨어공학-제품 품질 요구사항, 정보기술-소프트웨어 프로세스 평가, 컴퓨터 기반 소프트웨어시스템 측정과 등급평가 등이 있다 [11-13].

2.3.1 보안 평가

보안 평가의 경우 2018년 4월 18일부터 과학기술정보통신부와 협력으로 한국인터넷진흥원(KISA)이 지정한 6

개 기관에서 정보보호제품 성능평가 제도를 진행하고 있다. KISA는 2013년 정보보호제품 성능 시험에 대한 연구를 진행 하였으며 국내외 정보보호제품 성능 시험 연구 사례 분석을 기반으로 성능시험 항목 및 방법을 제시하였다. 이를 통해 CC평가인증, 보안적합성검증의 현황 및 국외 성능시험 항목을 국내 평가와 비교하여 국내 환경에 적합한 보안 성능시험 검증체계 수립 방향을 논의하였다 [14]. TTA는 정보보호제품 표준 적합성 시험 방법을 표준안으로 채택하였다 [15]. 위 표준은 사용자입장, 생산자 입장, 시험평가자 입장 등을 고려하여 융통성, 확장성, 정확성, 일관성, 적응성,효용성으로 항목을 분류하여 정보보호 표준적합성 시험 방법론(Advanced Security Conformance Test, ASCT)을 제안하여 정보보호제품 시험기준 및 절차 표준에 대해 제시하였다. KS로는 정보기술-보안 기술- 보 기술 보안 평가 방법론, 정보기술-보안기술-정보기술보안 평가기준 시리즈에서 보안기술 필수 요구사항 및 항목별 평가 방법, 절차, 평가 기준 등을 소개하고 있다 [16, 17].

3. MTD 평가인증 요구사항

본 장에서는 2.3절에서 살펴본 각 분야별 평가들의 요구사항 중에 MTD와 연관되어있는 평가 항목이 어떤 것들이 있는지 도출한다. MTD는 시스템의 환경요소를 변화시키디 때문에 성능과 밀접한 요소가 요구된다. 따라서 표 1과 같이 지연시간, 응답속도, 사용율, 처리율 등을 기준으로 MTD 평가인증을 마련해야 한다.

<표 1> MTD 평가 분야별 요구사항

분 류	평가 항목
네트워크	- 패킷 크기 변화에 따른 처리율과 지연시간 - IPv4/IPv6, TCP/UDP, 응용 프로토콜 등 트래픽에 대한 처리율과 지연시간
소프트웨어	- 시간 효율성(실행 반응 및 수행시간 또는 처리율, 응답 시간 등) - 자원 효율성(평균 프로세서/메모리/장치/대역폭 사용률 등)
보안	- 액세스 제어 리스트 수에 따른 비트, 패킷 처리율/전송률과 지연시간 - 패턴 매칭 규칙 수에 따른 비트/패킷전송률 과 지연시간 - 시간에 따라 설정된 터널 수, 터널 생성률, 해지율 - 시간에 따른 HTTP 트랜잭션 개수 및 생성률

네트워크 성능 평가로는 패킷 크기 변화와 IPv4, IPv6, TCP, UDP, 응용계층 트래픽에 대한 처리율과 지연 시간이 있다. 패킷 크기 변화의 경우 각 패킷 크기별 측정된 패킷, 비트전송률로 평가할 수 있고 주요 성능 측정 변수는 단일 IPv4, IPv6, 듀얼 스택 설정 등이 있다. IPv4, IPv6 트래픽은 구성비에 따른 패킷, 비트 전송률과 지연시간을 측정하고 패킷 크기 변화, 듀얼 스택 등을 고려한다. TCP, UDP, 응용프로토콜 또한 구성비에 따른 패킷, 비트 전송률과 지연시간으로 평가하며 응용계층 트래픽의 경우 HTTP, FTP, UDP의 구성비를 고려한다. 이외에 MTD 적용 전과 후의 QoS, 라우팅 프로토콜과 인접 요소 상태 및 인접성 변화율 등을 검토 할 수 있다.

소프트웨어의 경우, 평가 항목 중 MTD 시스템 운용에서 가장 눈여겨볼 항목은 성능 효율성이며 시간 효율성과 자원 효율성으로 구분한다. 시간 효율성은 시스템에서 요구되는 기능을 프로그램이 수행 할 때의 수행시간과 처리율의 정도, 응답 시단 등을 평가하는 특성을 의미한다. 시간 효율성 항목에는 평균응답시간, 응답시간 적합성, 평균왕복시간, 왕복 시간 적합성, 평균처리량이 있다. 자원 효율성은 시스템에서 요구되는 기능을 프로그램이 수행 할 때 필요한 프로세서 수행 시간 비율을 의미하며 프로세서, 메모리, 장치, 대역폭 등의 평균 사용률을 측정한다.

MTD 운용에서 활용할 수 있는 시스템 보안평가는 솔루션에 사용되는 비밀번호, 키, 토큰, 난수 발생기, 난수 엔트로피 선택(예: 시간) 등의 변화에 따른 보안성능 및 효율성 검증과 밀접하다. 처리율, 지연시간, 해지율, 생성률 등 MTD로 변화된 요소에 따른 보안 솔루션 영향은 기존 보안 평가와 관련된 항목을 통해 점검이 가능하다. 하지만 외부 공격에 얼마나 MTD가 보안성을 보이는지에 대해서는 신뢰성 있는 모집단과 과학적 추론을 고려한 연구 및 실험 결과가 필요하며, 결과를 통해 MTD 보안 성능 시험 방법 및 지침 등으로 평가인증 요구사항에 추가할 수 있다.

4. 결론

정적 시스템의 보안 방안으로 제안된 MTD 기술은 공격자가 악용할 수 있는 광범위한 공격 영역을 줄이기 위해 시스템을 지속적으로 변경하는 것을 의미한다. 주 공격 표적을 가지는 보안위협의 특정 도메인, 시스템에 효과적인 보안성을 지닌 MTD는 아직 연구 초기단계에 불과하지만 2017년에 상용화 되는 등 개발 활발히 진행되고 있다. 하지만 아직 MTD 기술 평가에 대한 연구는 이슈로 남아있으며 이에 대한 연구가 필요하다.

본 논문에서는 MTD 기술 개요 및 이슈, 그리고 관련 분야의 평가들을 살펴보고 분석하여 MTD 평가인증 요구사항을 도출 하였다. MTD는 공격표면을 유동적으로 만들기 위해 환경요소를 변경시키므로 각 요소의 변화에 따른 시스템 및 보안 영향에 따른 평가 요소를 고려해야 한다. 국내 평가 기준 표준 문서를 기반으로 도출 된 요구사항을 통해 MTD 평가인증 기준 마련에 기여 할 수 있을 것으로 기대하며, 관련 국제표준 조사 및 분석으로 더 신뢰성 있고 개선된 기준으로 보완 할 수 있을 것으로 전망한다.

Acknowledgement

이 논문은 2018년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (No.2017-0-00061, 국내 ICT표준 제개정 연구)

참고문헌

[1] Kang, Koo-Hong, Tae-Keun Park, and Dae-Sung Moon. "Analysis of Threat Model and Requirements in Network-based Moving Target Defense." 한국컴퓨터정보학회논문지, 2017

[2] Tian, Jue, Tan, Guan, "Enhanced Hidden Moving Target Defense in Smart Grids." IEEE Transactions on Smart Grid, 2018

[3] Zhang, Hong-qi, Cheng Leiab, De-xian Changab, Ying-jie Yangab,. "Network moving target defense technique based on collaborative mutation." Computers & Security, 2017

[4] Carvalho, Marco, Richard Ford. "Moving-target defenses for computer networks." IEEE Security & Privacy. 2014

[5] Tang, Sun, Yang, Long, "A Network Coding and DES Based Dynamic Encryption Scheme for Moving Target Defense", IEEE Access, 2018

[6] IEEE 802 Working Group, "IEEE 802.11 WIRELESS LOCAL AREA NETWORKS", IEEE Standards Association, 2014

[7] TTA, 홈게이트웨이 기능 및 성능 평가기준, TTAK.KO-04.0123, 2010

[8] TTA, "휴대인터넷(IEEE 802.16m 와이브로)의 무선접속 규격에 대한 성능평가방법 (EMD)", TTAE.IE - 802.16mEMD, 2010

[9] TTA, "차량이동환경을 위한 무선LAN(IEEE802.11p) 물리계층 시험규격", TTAK.KO-06.0440, 2016

[10] TTA, "네트워크 보안 장비에 대한 성능 측정 방법", TTAS.KO-12.0044, 2006

[11] 국가표준(KS), "정보 기술-소프트웨어 공학-제품 품질 요구사항 및 평가(SQuaRE)-품질 요구사항", KS X ISO/IEC 25030, 2014

[12] 국가표준(KS), "정보기술-소프트웨어 프로세스 평가" 시리즈, KS X ISO/IEC 15504-X, 2013

[13] 국가표준(KS), "정보기술-컴퓨터 기반 소프트웨어 시스템의 성능의 측정과 등급평가", KS X ISO/IEC 14756, 2014

[14] 이상걸, 이정희, 장병련, 안해림, "국내외 정보보호제품 성능시험 연구 사례 분석", KISA, 2013

[15] TTA, "네트워크 보안 장비에 대한 성능 측정 방법", TTAS.KO-12.0044, 2006

[16] 국가표준(KS), "정보 기술-보안 기술-정보 기술 보안 평가 방법론", KS X ISO/IEC 18045, 2017

[17] 국가표준(KS), "정보기술-보안기술-정보기술보안 평가기준" 시리즈, KS X ISO/IEC 15408-X, 2014