Journal of The Korea Society of Computer and Information
Vol. 23 No. 12, pp. 95-105, December 2018

www.ksci.re.kr
https://doi.org/10.9708/jksci.2018.23.12.095

Survey on the use of security metrics on attack graph

Gyung-Min Lee *, Huy-Kang Kim*

Abstract

As the IT industry developed, the information held by the company soon became a corporate asset. As this information has value as an asset, the number and scale of various cyber attacks which targeting enterprises and institutions is increasing day by day. Therefore, research are being carried out to protect the assets from cyber attacks by using the attack graph to identify the possibility and risk of various attacks in advance and prepare countermeasures against the attacks. In the attack graph, security metric is used as a measure for determining the importance of each asset or the risk of an attack. This is a key element of the attack graph used as a criterion for determining which assets should be protected first or which attack path should be removed first. In this survey, we research trends of various security metrics used in attack graphs and classify the research according to application viewpoints, use of CVSS(Common Vulnerability Scoring System), and detail metrics. Furthermore, we discussed how to graft the latest security technologies, such as MTD(Moving Target Defense) or SDN(Software Defined Network), onto the attack graphs.

▸Keyword: Attack Graph, CVSS, Security Metric, Moving Target Defense, Survey

I. Introduction

1. Background & Motivation

과학기술정보통신부의 2018년 4월 통계[1]에 의하면 국내 기업을 대상으로 하는 침해사고 신고접수는 2015년 225건, 2016년 247건, 2017년 287건으로 꾸준히 증가하고 있다. 이는 2010년 기준 연 53건의 침해사고가 접수된 것에 비해 약 5배 이상 증가한 수치이며, 하루에 한 번꼴로 침해사고가 발생하고 있다는 것을 의미한다. 공격자들은 공격 대상의 시스템에 존재하는 취약점을 이용하여 시스템 내로 침투한다. 시스템 내에 존재하는 취약점이 많을수록 공격자가 이용할 수 있는 공격 경로가 다양해질 수 있으며 공격의 성공 가능성도 증가하게 된다. 다양한 공격으로부터 자산을 안전하게 보호하기 위해서는 공격자가 사용 가능한 경로와 취약점을 확인하고 분석할 수 있어야 한다. 공격 그래프(attack graph)[2]는 네트워크 토폴로지 상에 존재하는 다양한 취약점 및 네트워크 토폴로지의 특성들을 분석하여 존재할 수 있는 다양한 공격 경로들을 확인하는 방법이다. 공격 그래프는 이처럼 시스템 내에 존재하는 취약점들을 이용하여 공격자의 침투 경로를 사전에 확인하고 각각의 공격 경로를 평가하는 데 의의를 두고 있다. 과거에는 공격 그래프에서 추출한 공격 경로의 길이와 같이 직관적으로 확인할 수 있는 지표를 이용해 각 공격 경로를 평가하였다[3]. 그러나 기업 및 기관에서 사용하는 시스템이 복잡해지고 비교적 더 중요한 자산들이 생겨나면서 이전의 지표들의 효용성이 떨어지기 시작했다. 이러한 상황에서 기존의 단순 정보만을 이용하는 것이 아닌 자산의 중요도, 공격의 성공 가능성, 공격의 영향력 등 다양한 기준을 이용하여 공격 경로를 평가하는 기술들이 등장하기

• First Author: Gyung-Min Lee, Corresponding Author: Huy-Kang Kim
*Gyung-Min Lee (pinjk123@korea.ac.kr), Graduate School of Information Security, Korea University
*Huy-Kang Kim (cenda@korea.ac.kr), Graduate School of Information Security, Korea University
• Received: 2018. 08. 27, Revised: 2018. 10. 30, Accepted: 2018. 11. 26.
• This work was supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIT) (No.2017-0-00213, Development of Cyber Self Mutation Technologies for Proactive Cyber Defense)

시작하였다. 공격 그래프는 이러한 지표들을 적극적으로 연구하고 이용하여 더욱 정확한 공격 경로를 예측하고 공격 경로의 우선순위와 같은 중요한 정보들을 추출하고자 하였다.

공격 그래프에서 사용하는 지표들은 보안 메트릭(security metric)이라고 일컬어지며 각각의 취약점이 지니는 위험도를 측정하거나 자산에 끼치는 영향력 및 자산의 중요도 등을 평가한다. 보안 메트릭은 그 자체로도 각 취약점 및 자산에 대한 정보를 얻을 수 있다는 점에서 중요한 정보가 될 수 있다. 공격 그래프를 이용해 얻어낸 공격 경로에 대한 정보와 함께 사용하는 경우, 각각의 공격 경로가 지니는 잠재적인 위험성과 우선시 보호해야 할 호스트 등과 같은 유용한 정보를 획득할 수 있다. 더욱 정확한 공격 경로의 판별 및 취약성 판단의 필요성이 증가함에 따라 다양한 보안 메트릭 및 공격 그래프 생성 도구에 대한 연구가 이루어지고 있다.

2. Contribution

본 논문에서는 공격 그래프에서 사용하는 보안 메트릭들의 특성을 확인하기 위해 앞서 존재한 다양한 공격 그래프 논문들의 보안 메트릭에 대한 조사 및 분류를 진행하였다. 분류한 보안 메트릭에 대해 공격 그래프에서 사용되는 보안 메트릭별 적용 관점을 확인하였다. 적용된 보안 메트릭별 특징을 분석하여 특정 상황에 알맞은 보안 메트릭을 사용할 수 있도록 메트릭별 특성을 표로 정리하였다. 더불어 최근 연구되기 시작한 MTD(Moving Target Defense)와 SDN(Software Defined Network)기반의 동적 네트워크 환경에 도입된 보안 메트릭을 조사하였다. 또한 위 조사를 통해 MTD 및 SDN 환경에 도입된 보안 메트릭의 보완점을 확인하고 적절한 도입을 위해 고려해야 할 점에 대해 논의하였다.

II. Preliminaries

1. Vulnerability

보안 취약점이란, 정보 시스템 혹은 구현된 소프트웨어 내에 존재하는 약점으로 공격자가 시스템에 침입하기 위한 주요 경로로 사용되는 것을 의미한다[4]. 보안 취약점은 주로 프로그램을 본래의 기능과는 다른 방향으로 작동하도록 유도하거나 비인가 사용자에게 권한을 부여하는 등의 임무를 수행한다. 이러한 보안 취약점들은 많은 유저들이 사용하는 다양한 프로그램 내에 존재하며 주기적인 보안 패치를 통해 수정된다. 공격자들은 프로그램 내에 존재하는 다양한 보안 취약점을 확인하고 분석하여 시스템 내에 침투한다. 침투한 이후 공격자들은 시스템의 오작동을 유도하거나 중요 자산들을 유출하고자 한다. 이러한 이유로 보안 취약점들은 시스템의 안정성을 확보하기 위해 반드시 고려해야 할 사항 중 하나이다.

2. CVSS

1999년 미국의 비영리 회사인 MITRE 사에서 공개적으로 알려진 소프트웨어의 보안 취약점에 대한 고유 표기인 CVE(Common Vulnerabilities and Exposure) [5]를 체계화하였다. CVSS(Common Vulnerability Scoring System) [6]는 이러한 고유한 CVE에 부여된 점수로 각 취약점에 대해 기밀성, 무결성, 가용성, 위험성 등 다양한 관점의 점수를 계산하는 점수화 체계이다. Fig. 1.과 같이 CVSS는 크게 기본 메트릭 그룹(base metric group), 시계열성 메트릭 그룹(temporal metric group), 환경 메트릭 그룹(environmental metric group)으로 나뉘며 세 그룹의 점수를 조합하여 취약점에 대한 평가를 진행한다. 각 메트릭 그룹에 대한 점수는 다양한 분야의 보안 전문가들의 판단에 의해 부여된다. 또한 추가적인 공격 방안 등의 발견으로 인해 주기적으로 갱신되어 보안 관리자들이 비교적 객관적인 평가 지표로 사용할 수 있다는 장점이 있다. 게다가 다양한 평가 지표 중 하나인 공격 가능성(exploitability) 점수 등을 이용해 공격의 성공 확률들을 계산하여 더욱 정량적으로 공격을 평가할 수도 있다.

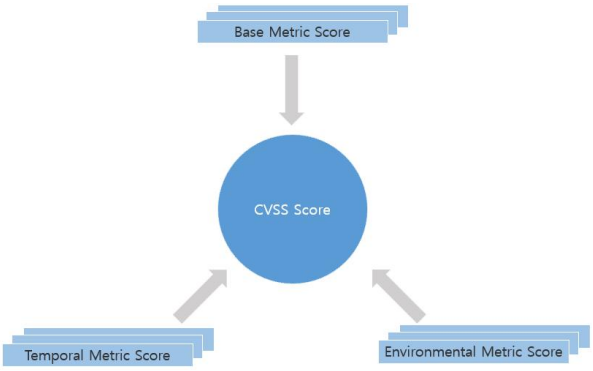

Fig. 1. CVSS scoring process

3. Attack graph

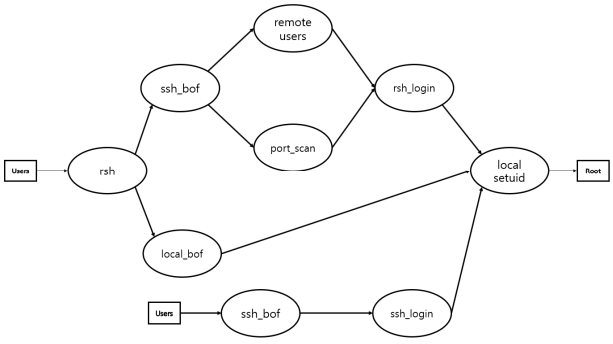

Fig. 2. Example of attack graph

공격 그래프란 시스템 내에 존재하는 호스트, 프로세스에 대해 모든 연결 정보를 그래프로 표현하여 공격의 경로가 될 수 있는 지점들을 파악하기 위한 기법이다. 공격 그래프는 공격자가 시스템에 침입하기 위한 경로를 모두 나타낼 수 있으며 공격의 목표를 한눈에 파악하는 데 알맞은 분석 방법이다. 또한

공격 경로를 시각적으로 나타낸다는 데 있어 관리자가 보다 빠르고 명확한 판단을 내리는 데에도 큰 도움을 준다. 그러나 시스템 내의 모든 호스트에 대해 가능한 경로를 모두 그래프로 나타내는 것은 더욱 완벽한 경로 파악에는 도움이 되지만, 연산량이 기하급수적으로 늘어난다는 단점이 있다. 이러한 이유로 공격 그래프를 보다 효율적으로 생성하는 다양한 도구들에 대한 연구를 지속하여 왔으며 그 예시는 다음과 같다.

Xinming Ou 등[7]은 ICAT와 같이 알려진 취약점에 대한 정보를 보유하고 있는 데이터베이스를 바탕으로 소프트웨어와 네트워크 내의 호스트별 보유 취약점, 네트워크 환경 설정 등의 정보를 이용하여 공격 그래프를 생성하고 각 취약점 및 공격 경로의 위험성을 판단하는 도구인 MulVAL을 제시하였다.

Kyle Ingols 등[8]은 네트워크의 reachability, 공격의 사전 조건 등을 고려하는 그래프인 MP 그래프(Multiple-Prerequisite Graph)를 제안하면서 네트워크 내의 취약점 및 네트워크 정보를 수집하는 도구인 Nessus 등을 이용하여 네트워크 내의 공격 경로를 확인하고 평가하는 도구인 NetSPA를 제시하였다.

III. Classification According to Metric Application Point of View

공격 그래프상에서 사용하는 다양한 보안 메트릭의 경우 고려하는 대상에 따라 이용하는 정보가 다르기 때문에 메트릭별 관점을 기준으로 분류할 수 있다. 공격 그래프에서 사용하는 보안 메트릭들의 관점은 크게 두 분류로, 위상(topology)의 관점과 취약점(vulnerability)의 관점으로 나눌 수 있다. Table 1.은 사용된 보안 메트릭들을 위상의 관점, 취약점의 관점으로 분류한 것이다.

과거에는 네트워크에 대해 얻을 수 있는 정보가 매우 한정적이었으며 취약점에 대한 정보를 얻기가 힘들어 개별 취약점에 대해 고려하기보다는 공격 그래프상에서 나타나는 여러 공격 경로의 특성 및 모양을 중심으로 공격 경로를 분석하였다. 공격 경로의 길이, 공격 경로의 개수, 가장 짧은 공격 경로와 같이 구조를 분석하여 얻을 수 있는 정보들을 공격 경로 분석의 지표로 이용하였다.

Cynthia Phillips 등[2]은 최단 경로(shortest path)를 찾는 알고리즘을 이용하여 공격 그래프상에 존재하는 다양한 공격 경로 중 길이가 가장 짧은 공격 경로를 판별하였다. 이는 공격 그래프를 이용하여 공격의 잠재적 위험성을 판별하는 기준을 제안한 초창기의 연구로, 이후 해당 공격 경로가 가장 높은 성공 확률을 보인다는 것을 확률 계산을 기반으로 증명하였다.

Rodolphe Ortalo 등[9]은 METF(Mean Effort To security Failure)라는 기준을 제안하여 해당 값이 클수록 네트워크가 안전하다는 것을 주장하였다. 공격에 필요한 최소 노력을 산정하기 위해 확률 계산을 이용하며 공격 경로의 개수(number of path)가 늘어날수록 해당 값이 작아져 네트워크가 안전해지지 않다는 것을 실험을 통해 증명하였다.

Vaibhav Mehta 등[10]은 공격자의 정보, 시스템의 정보, 시스템 내의 방어 정책 등을 바탕으로 전체 시스템의 상태(state)를 구성하였다. 구성한 상태를 바탕으로 Google 사의 페이지 랭크(pagerank) 알고리즘을 응용하여 상태의 등수를 매기는 방안을 제안하였으며 임의의 시뮬레이션에서 도달 가능성 등을 이용해 각 상태의 등수를 매겼다. 이후 보안성이 충분히 갖춰지지 않은 상태들인 오류 상태(error state)의 도달 가능 확률이 높은 경우 해당 시스템은 안전하지 않다고 판단하였다.

Nwokedi Idika 등[11]은 기존 연구들에서 제안한 최단 공격 경로의 길이(shortest path), 공격 경로의 개수(number of path) 등의 비교적 단순한 보안 메트릭들을 보완하여 공격 경로들의 길이의 정규 평균(normalized mean of attack path), 공격 경로들의 길이의 표준편차(standard deviation of path lengths), 공격 경로들의 길이의 모드(mode of path lengths), 공격 경로들의 길이의 중앙값(median of path lengths) 등과 같은 추가적인 보안 메트릭을 제안하고 적용하였다.

이처럼 네트워크 위상에서 얻을 수 있는 다양한 정보를 바탕으로 하는 보안 메트릭들이 연구되었으며 기존의 메트릭들을 보완하는 연구도 활발하게 진행되었다. 반면 미국 국립표준기술연구소(NIST)[12]에서 각종 취약점에 대한 데이터베이스를 구축하기 시작하면서, 네트워크 위상이 아닌 네트워크 내 취약점을 이용하여 공격 경로를 분석하고 평가하는 방법에 대한 연구도 활발히 진행되었다.

Davide Balzarotti 등[13]은 개별 취약점의 성공 가능성(exploitability)과 공격의 재생산성(reproducibility)을 고려하여 취약점 의존 그래프(vulnerability dependency graph)를 그리는 방안에 대해 제안하였으며 이를 이용해 자산 평가에 이용할 수 있도록 기준을 제시하였다.

Lingyu Wang 등[14]은 각각의 취약점이 성공할 확률을 계산하기 위해 각 취약점의 사전 조건이 성사될 확률을 확인하고 공격 경로별 누적확률을 계산하였다. 해당 논문에서는 확률을 계산하기 위한 사전 정보를 NIST의 CVSS를 이용해 얻을 수 있다고 언급하였다. 또한 누적 확률을 연산하는 것의 어려움을 줄이기

Table 1. Metrics classification based on application perspective

Category	References	Representative researches
Topological	[3], [9], [10], [11]	“Experimenting with Quantitative Evaluation Tools for Monitoring Operational Security”[9] “Extending Attack Graph-Based Security Metrics and Aggregating Their Application”[11]
Vulnerability	[13], [14], [15], [20-36]	“Assessing the Risk of Using Vulnerable Components”[13] “Using CVSS in Attack Graphs”[15]
Both	[16], [17], [19], [37]	“Measuring the Overall Security of Network Configurations Using Attack Graphs”[16] “Quantifying Security Risk by Measuring Network Risk Conditions”[17]

위해 공격 경로 내의 순환(cycle)을 줄이려는 방안도 제시하였다.

Laurent Gallon 등[15]은 NIST에서 제공하는 CVSS의 보안 메트릭들을 이용하여 다단계 공격(multi-stage attack)에 대한 보안 평가를 진행하였다. 해당 논문은 CVSS에서 제공하는 기본 메트릭(base metric)과 영향력 메트릭(impact metric)을 이용해 취약점에 의해 전체 네트워크 및 각 호스트가 받는 영향을 계산하는 정량적인 평가 방법에 대해 제시하였다.

취약점 기반의 보안 메트릭에 대한 연구가 진행되면서, 취약점과 함께 네트워크 위상에 대한 분석이 수반되어야 한다는 의견을 제시하였다. Lingyu Wang 등[16]은 네트워크 내에 존재하는 각 취약점에 대해 네트워크가 지니는 저항성(resistance) 및 네트워크의 초기 설정에 의한 공격에 대한 저항성을 고려하여 취약점과 네트워크 위상 모두를 고려하는 보안 메트릭을 제안하였다.

Candace Suh-Lee 등[17]은 내부 네트워크를 기준으로 공격의 성공 가능성에 영향을 미치는 요소들을 확인하였다. 외부 인터넷과 같이 신뢰할 수 없는 네트워크와 내부 호스트간의 근접성을 측정하여 보안 메트릭으로 이용하며 각 호스트의 이웃 호스트가 가진 취약점 정보를 이용한 보안 메트릭을 제안하였다.

전반적으로 네트워크 위상을 고려한 보안 메트릭의 경우 비교적 제한된 정보와 알기 쉬운 정보를 이용하여 네트워크의 안정성을 판단하는 연구가 다수 존재하였으며 공격 그래프의 연구 초기에 주로 사용되었다. 각 자산 내에 존재하는 취약점의 중요성이 강조되기 시작하면서, 네트워크 위상보다는 취약점을 이용한 보안 메트릭의 연구가 활발히 진행되기 시작하였으며 그 추세는 지금까지 이어지고 있다. 또한 둘 모두를 고려하는 연구들은 그 연구가 매우 활발히 이루어진 편은 아니지만 네트워크의 전반적인 안정성과 더불어 개별 자산의 안정성도 함께 고려한다는 장점으로 인해 비교적 최근 다시 연구가 이루어지고 있다.

IV. Classification According to Use of CVSS

MITRE 사가 알려진 취약점에 대한 데이터베이스를 구축한 이후, NIST는 CVSS를 이용하여 더욱 체계화된 데이터베이스인 NVD(National Vulnerability Database)[18]를 구축하기 시작했다. NVD가 구축된 이후, 공격 그래프에 관한 연구들은 더욱 정확하고 객관적인 기준을 제안하기 위해 NVD에 작성되어있는 CVSS 점수를 기반으로 하는 보안 메트릭에 대한 연구를 진행해왔다.

CVSS는 취약점의 심각성에 대한 점수 외에도 주요 특성에 대한 세부 정보를 카테고리로 나누어 점수를 부여한다. CVSS는 지난 1999년 이후 CVSS v2.0이라는 점수 평가 기준을 이용해 모든 취약점에 대한 평가를 진행하였으며 지난 2015년 변경된 평가 기준인 CVSS v3.0을 이용해 취약점들을 평가한다. CVSS는 크게 기본 메트릭 그룹(base metric group), 시계열성 메트릭 그룹(temporal metric group), 환경 메트릭 그룹(environmental metric group)으로 세부 메트릭을 구분하고 있다. 각각은 취약점의 공통적인 특성, 시계열적인 특성, 환경적인 특성을 반영하고 있으며 대표적인 메트릭으로는 AC(Attack Complexity), AV(Attack Vector), 악용 가능성(exploitability) 등이 있다. 세 메트릭은 각각 공격의 어려움, 공격자가 자산에 공격을 수행할 때 필요한 논리적, 물리적인 거리, 공격 성공 가능성 등을 나타내는 세부 메트릭이다.

반면 공격 그래프가 적용되는 네트워크의 특성, 혹은 보안 메트릭의 기준에 따라 CVSS 점수가 아닌 별도의 메트릭을 제안하는 연구들도 다수 존재한다. 이러한 관점을 바탕으로 공격 그래프상에서 사용되는 보안 메트릭을 CVSS 사용 여부에 따라 분류할 수 있다. Table 2.는 사용된 보안 메트릭들을 CVSS 사용 여부를 기준으로 분류한 것이다.

CVSS를 사용하지 않는 보안 메트릭은 단순히 CVSS를 사용하지 않는 것과 더불어 CVSS에 기반을 둔 취약점 위험성 기준이 아닌 새로운 기준을 수립하는 방안을 제안한다. Joseph Pamula 등[19]은 네트워크의 보안 안전성은 해당 네트워크에 공격을 성공시킬 수 있는 가장 약한 공격자의 능력에 따라 결정된다고 주장하였다. 가장 약한 공격자란 최소한의 노력으로 목표 자산에 침투할 수 있는 공격자를 의미한다. 이러한 주장을 바탕으로 공격 목표에 도달하기 위해 필요한 네트워크의 초기 설정의 최소 집합(minimal set of initial attributes)을 계산하여 해당 네트워크의 안전성을 평가하는 방안을 제시하였다.

Steven Noel 등[20]은 각 네트워크 환경에 따라 다른 확률을 적용하고자 이벤트 발생 횟수에 따른 확률을 이용한 보안 메트릭을 제안하였다. 각각의 보안 위협 이벤트가 얼마나 자주 관측되는지 등의 정보를 이용해 해당 취약점의 발생 확률을 계산하였으며 이를 이용한 누적 확률에 근거한 보안 메트릭을 제시하였다.

반면 다수의 연구는 제시하는 보안 메트릭의 명확한 근거를 위해 혹은 비교적 정확한 확률 계산을 위해 CVSS를 사용하기도 한다. 이러한 경향은 최근 몇 년간 증가하는 모습을 보이며 시간이 지날수록 다양한 관점에서의 CVSS 이용이 이루어지고 있다.

Melanie Tupper 등[21]은 취약성(vulnerability), 악용 가능성(exploitability), 공격 가능성(attackability) 라는 세 관점에서의 보안 메트릭을 제안하였다. 취약성 계산에는 CVSS의 영향력 점수(impact score), 시계열 점수(temporal score)를

Table 2. Metrics classification based on CVSS usage

CVSS usage	References	Representative researches
Without CVSS	[3], [9], [10], [11], [13], [14], [16], [19], [20], [25]	“A Weakest-Adversary Security Metric for Network Configuration Security Analysis”[19] “Measuring Security Risk of Networks Using Attack Graphs”[20]
With CVSS	[15], [17]. [21], [22], [23], [24], [26-37]	“VEA-bility Security Metric: A Network Security Analysis Tool”[21] “CVSS-based Security Metrics for Quantitative Analysis of Attack Graphs”[22]

이용하였고 악용 가능성 계산을 위해 네트워크에서 동작중인 서비스의 수와 CVSS의 악용 가능성 점수(exploitability score)를 이용하였으며 공격 가능성 계산에는 네트워크 내의 가능한 공격 경로의 개수를 이용하였다.

Marjan Keramati 등[22]은 각 취약점의 위험도와 취약점별 자산에 끼치는 영향력을 CVSS를 바탕으로 계산하였으며 공격 경로의 길이를 함께 고려해 공격 경로별 위험도를 계산하는 방법을 제시하였다. 저자는 해당 방법이 공격 그래프상에서 공격 경로에 대한 정량적 평가가 가능하며 자산에 끼치는 영향력을 함께 고려하였기 때문에 네트워크 전체의 보안 손실(security loss)도 계산할 수 있다고 주장하였다.

Fangfang Dai 등[23]은 네트워크 내의 위험(risk)을 기반으로 하는 공격 그래프인 RFAG(Risk Flow Attack Graph)를 제안하였다. 해당 공격 그래프는 네트워크에서 최대 유량을 구하는 용도로 사용되는 최대 유량(maximum flow) 알고리즘을 사용하여 네트워크 내에 발생할 수 있는 최대 위험을 계산하였다. 각 위험의 계산은 CVSS 점수를 기반으로 이루어졌으며, 알고리즘을 이용해 위험의 최대치를 계산하는 방식을 이용하였다.

CVSS를 사용하지 않는 보안 메트릭들에 대한 연구는 네트워크의 초기 설정, 특성 등을 이용하는 연구와 통계를 기반으로 한 공격 확률과 같이 새로운 기준을 이용한 연구로 나뉘게 된다. 그러나 CVSS가 이전보다 명확한 지표를 수립하고 다양한 취약점의 정보를 수집하기 시작하면서, CVSS를 보안 메트릭에 이용하여 더욱 객관적이며 다양한 취약점을 고려할 수 있는 보안 메트릭들에 대한 연구가 활발히 이루어지고 있다.

V. Classification According to Detailed Metric

본 단원에서는 공격 그래프상에서 사용된 보안 메트릭을 보다 세부적으로 분류하였으며 Table 3.은 분류한 내용을 정리한 표이다. 세부 분류는 확률을 이용한 메트릭, 베이지안 네트워크(bayesian network) 등 네트워크 혹은 시스템 모델을 이용한 메트릭, CVSS 메트릭을 이용한 메트릭, 알고리즘을 응용한 메트릭 등 다양한 분류로 이루어져 있다.

Table 3.의 (a)는 확률을 기반으로 한 보안 메트릭에 관한 연구들을 정리한 것이다. 공격 그래프는 어떤 공격 경로가 가장 높은 확률로 사용될 것인지 판별하기 위해 공격자가 사용한 취약점이 성공적으로 작동할 확률 등을 계산하여 실제 침입이 일어날 가능성에 대해 고려해야 한다. Anoop Singhal 등[24]은 공격 그래프와 CVSS 메트릭을 이용해 확률을 기반으로 하는 보안 메트릭을 연구하였다. CVSS 메트릭을 바탕으로 하는 확률을 이용해 공격 확률뿐만 아니라 위험에 대한 확률도 연산할 수 있다는 것을 주장하였다.

Lixia Xie 등[25]은 다수의 에이전트에 기반을 둔 모델인 MRAMBAG(Multi-Agents Risk Assessment Model Based on Attack Graph)를 제안하였다. 해당 연구는 확률을 기반으로 하여 공격 경로별 위험성의 순위를 평가하였으며 각 자산의 위험을 평가하여 가장 먼저 조치를 취해야 할 자산을 확인하는 데에 초점을 맞추었다.

John Homer 등[26]은 공격 성공 가능성의 누적 확률을 이용하여 공격 경로별 위험도를 평가하는 방안을 제시하였다. 또한 공격 그래프상에서 연산 비용이 늘어나는 주된 원인인 경로 순환 문제를 해결하는 알고리즘을 제시하여 공격 그래프 생성의 복잡도를 줄이는 방안에 대해 연구하였다.

(b)는 다른 네트워크 혹은 시스템에 적용되던 네트워크 모델들을 보안 메트릭으로 활용한 연구들을 정리한 것이다. 공격 그래프는 기업 및 기관의 네트워크를 구조화하여 발생할 수 있는 공격 경로를 확인하기 때문에 네트워크 모델에 적용할 수 있는 다양한 모델을 이용한 연구를 진행할 수 있다. Marcel Frigault 등[27]은 베이지안 네트워크 모델을 이용하여 개별 공격 경로의 성공 확률을 계산하는 방법을 제안하였다. 베이지안 네트워크를 생성하는 데 사용한 확률값은 CVSS 메트릭을 이용하였으며 이를 통해 각 공격 경로가 가지는 누적 확률을 계산하여 공격 경로의 위험성을 산정하였다.

Table 3. Metrics classification based on detailed metric

Class	Category	References	Representative researches
(a)	Probability	[9], [10], [13], [14], [20], [24], [25], [26], [27], [28], [29], [31], [34], [36]	- “Security Risk Analysis of Enterprise Networks Using Probabilistic Attack Graph”[24] - “Network Security Risk Assessment Based on Attack Graph”[25]
(b)	Using network or system model	[27], [28], [29], [31]	- “Dynamic Security Risk Management Using Bayesian Attack Graphs”[28] - “Network Security Risk Assessment Method Based on HMM and Attack Graph Model”[29]
(c)	Using algorithm	[3], [10], [23], [30]	“Identifying Critical Attack Assets in Dependency Attack Graphs”[30]
(d)	CVSS score	[15], [21], [22], [23], [31], [32], [33], [35], [36], [37]	“An Approach of Security Risk Evaluation Based on the Bayesian Attack Graph”[31] “Metrics Suite for Network Attack Graph Analytics”[32]
(e)	Network attributes	[3], [9], [11], [16], [17], [19], [22], [34], [35]	“An Approach for Security Assessment of Network Configurations Using Attack Graph”[34] “Evaluating Security and Availability of Multiple Redundancy Designs when Applying Security Patches”[35]
(f)	Resistance or safetiness to attack of network	[16], [19], [34], [36], [37]	“Quantifying Security Risk by Critical Network Vulnerabilities Assessment”[36] “Network Diversity: A Security Metric for Evaluating the Resilience of Network Against Zero-Day Attacks”[37]

Nayot Poolsappasit 등[28]은 베이지안 네트워크 모델을 이용한 공격 그래프인 BAG(Bayesian Attack Graph)를 제안하였으며 베이지안 네트워크를 이용해 네트워크의 보안성을 확인하고 측정한 확률 기반의 보안성을 바탕으로 네트워크의 위험 평가에 이용하는 방법을 제안하였다.

Si-chao Liu 등[29]은 HMM(Hidden Markov Model)을 이용하여 네트워크의 보안성을 평가하는 방안에 대해 연구하였다. 해당 논문은 CVSS를 기반으로 취약점별 가중치 값을 산정하고 네트워크 내의 상태 변화를 측정한 뒤 가장 발생 확률이 높은 상태 변화를 산정하였다. 이를 이용해 네트워크 내에서 가장 일어날 확률이 높은 공격 경로를 확인하여 사전에 방지하는 방법을 제시하였다.

(c)는 공격 그래프에 기존에 연구되어온 알고리즘을 도입한 보안 메트릭에 관한 연구들을 정리한 것이다. 기존 알고리즘들은 대부분 그 성능이나 효용성이 검증된 것들이기 때문에 이를 알맞은 방법으로 적용한다면 공격 경로를 확인하는데 있어 매우 유용한 분석 방법이 될 수 있다. Reginald E. Sawilla 등[30]은 구글(Google) 사에서 개발하고 이용한 페이지랭크(pagerank) 알고리즘을 응용하여 공격 그래프에 적용하였다. 자산랭크(Assetrank)라 명명한 이 알고리즘은 공격 그래프에서 각 자산에 대해 순위를 매기며 높은 순위가 매겨진 자산일수록 공격자에게 유용한 공격 수단이 된다는 것을 의미한다. 해당 논문은 이러한 정보를 이용해 공격자로부터 가장 먼저 방어해야 할 자산이 무엇인지 확인할 수 있다고 주장하였다.

(d)는 CVSS 메트릭을 이용하여 공격 경로의 성공 가능성, 위험도 등을 계산한 보안 메트릭에 관한 연구들을 정리한 것이다. 공격 그래프는 개별 공격에 대해 보다 정확한 분석을 진행해야 하기 때문에 공격의 위험성 등에 대한 명확한 기준이 필요하다. Wang Hui 등[31]은 BAG(Bayesian Attack Graph)에서 각 공격의 확률을 계산하기 위해 CVSS 메트릭을 이용하였다. CVSS 메트릭의 AC(Access Complexity)와 같은 값을 이용해 공격의 어려움을 공격 성공 확률에 빗대어 이용하였다.

Steven Noel 등[32]은 자산들을 하나의 그룹으로 묶어 보안성을 평가하였다. 각 그룹 내의 자산들의 CVSS 메트릭을 합산하여 하나의 가족 점수(family score)를 산정하고 그룹별 가족 점수를 합산한 네트워크 점수(network score)를 산정하여 그룹별 그리고 네트워크 전체의 보안성을 평가하는 방안을 제시하였다.

Young Hoon Moon 등[33]은 네트워크 내의 각 자산별 CVSS 점수를 이용한 평가와 더불어 각 기업별, 소프트웨어별 평판 점수를 산정하고 보안 조치에 따른 점수를 산정하여 종합적인 공격 경로 평가 방안을 제시하였다. 평판 점수의 경우, OS와 서비스별 평판 점수로 나뉘며 각각은 OS, 서비스에 존재하는 취약점 정보 및 개수에 따른 가중치를 바탕으로 산정된다. OS의 경우 OS에 존재하는 취약점의 개수에 따라 가중치가 부여되며 서비스의 경우 서비스에 존재하는 취약점의 개수 및 CVSS 점수에 따라 가중치가 부여된다. 마지막으로 보안 조치에 따른 점수의 경우, 보안 인증에서 사용하는 인증 방안 혹은 암호 알고리즘에 따라 점수를 부여하고 이를 종합하여 안전성을 평가한다.

(e)는 네트워크 구성에 대한 정보를 이용하여 네트워크의 보안성을 평가하는 보안 메트릭에 관한 연구를 정리한 것이다. 네트워크의 경로 길이, 방화벽 정책, 시스템별 보안 패치 등과 같이 네트워크의 구성에 대한 정보는 시스템에 가해진 공격에 대한 저항성, 공격자가 공격을 성공시키는데 필요한 노력 등을 계산하는 데 적합해 이를 이용해 네트워크의 보안성을 평가하는 연구가 필요하다. Nirnay Ghosh 등[34]은 네트워크 정책이 다단계 공격에 얼마나 저항할 수 있게 설정되어 있는지를 이용해 보안성을 평가할 수 있다고 주장하였다. 이를 바탕으로 저자는 공격자의 네트워크의 정책에 따른 공격 성공 확률을 계산하여 네트워크의 공격 저항성을 확인하는 방안을 제시하였다.

Mengmeng Ge 등[35]은 네트워크 내의 시스템이 가진 보안 취약점에 대해 보안 패치를 진행하는 경우 네트워크 전반적인 보안성이 얼마나 증가하는지를 보안 메트릭을 이용하여 측정하였다. 또한 보안 패치로 인해 시스템에 가해지는 가용성의 변화를 측정하여 평가하기 위한 다양한 기준을 제안하였으며 위의 두 기준을 토대로 시스템 보안 패치로 인한 가용성을 증가시키기 위해 시스템의 복제품을 두는 것이 보안성 패치로 인한 보안성 증가에는 악영향을 끼친다는 점을 확인하였다.

(f)는 네트워크 전체가 공격에 대해 지니는 저항성 혹은 안전성을 평가하는 보안 메트릭에 관한 연구를 정리한 것이다. 각 자산이 공격에 대해 지니는 저항성을 확인하는 것도 중요하지만 네트워크 전체에 대한 전반적인 안전성을 평가하는 것은 보안 관리자의 입장에서 보다 명확하게 네트워크의 상태를 확인할 수 있다는 장점이 있기 때문에 해당 관점에 대한 지속적인 연구가 필요하다. Umesh Kumar Singh 등[36]은 네트워크 환경을 고려한 보안 메트릭인 위험(hazard) 메트릭을 제안하였다. 해당 메트릭은 CVSS 점수, 공격의 빈도 등을 이용하여 확률을 계산하고 이를 바탕으로 공격에 대해 네트워크가 지니는 저항성을 계산하는 방안에 대해 제시하였다.

Mengyuan Zhang 등[37]은 제로데이 공격에 대해 네트워크가 지니는 보안성을 평가하기 위한 메트릭을 제안하였다. 저자는 네트워크의 보안성을 다양성에 기반을 둔 세 가지 기준인 자원의 다양성의 풍부함(richness of resource), 공격에 필요한 최소 노력(least attacking effort), 확률 기반의 네트워크 다양성(probabilistic network diversity)으로 나누어 평가를 진행하는 방안을 제시하였다.

이처럼 매우 다양한 관점의 보안 메트릭에 대한 연구가 활발히 진행되어왔으며 연구의 관점도 확대되어가는 추세이다. 확률을 이용하는 보안 메트릭의 경우, 시스템의 보안성과 공격의 위험성을 판단하기 때문에 효율적이며 베이지안 네트워크, CVSS 점수와 같이 확률을 계산할 수 있는 다양한 지표들을 이용한 연구가 활발하게 이루어지고 있다. 다른 연구 관점들도 마찬가지로 단순히 하나의 관점으로만 공격의 위험성을 판단하는

것이 아닌 다양한 관점을 도입하여 더욱 네트워크에 적합한 보안 메트릭을 수립하기 위한 연구가 지속되고 있다.

VI. Discussion about grafting Attack Graph onto MTD and SDN

최근에는 SDN 혹은 MTD 등과 같은 최신 기술들을 바탕으로 한 보안 기법들을 이용하여 네트워크의 보안성을 증진하는 연구 및 적용이 이루어지고 있다[38]. SDN이란 네트워크 내의 트래픽 전달 동작을 소프트웨어 기반 컨트롤러에서 제어 및 관리하는 접근 방식으로, 네트워크 내 개별 시스템의 종류에 구애받지 않고 다수의 시스템을 관리할 수 있는 기술이다. MTD는 공격 대상이 되는 시스템 혹은 네트워크의 구성 및 세부 설정을 능동적이고 지속해서 변화시켜 공격자가 공격 대상의 취약점을 확인하기 어렵게 하는 기술이다. 이러한 과정에서 MTD는 정보를 수집하고 시스템의 구성을 변경하는 등 일련의 작업을 SDN 기술을 이용하여 구현하게 된다. 이러한 최신 보안 기술을 이용하는 기업 및 기관이 늘어남에 따라 공격 그래프는 위와 같은 기술들을 반영하여 공격 경로 및 위험성을 판단할 수 있는 능력을 함양해야 할 필요가 있다.

Rui Zhuang 등[39]은 MTD 기술의 효용성을 분석하기 위해 CAG(Conservative Attack Graph)를 제안하였다. 해당 공격 그래프는 기존의 확률 기반 공격 그래프와 달리 사전 조건을 만족하여 공격이 성사되는 경우 상태 전이가 발생한다는 가정하에 공격 그래프를 생성하는 방식을 이용하였다. 상태 전이가 발생할 확률을 이용해 공격자의 공격 성공 확률을 계산하였으며 MTD가 적용되는 시간 간격을 기반으로 해당 MTD 기술이 공격자의 공격으로부터 얼마나 안전한지를 평가하였다.

Jin B. Hong 등[40]에 의하면, MTD 기술은 크게 세 기준으로 분류될 수 있다고 한다. MTD 기술은 네트워크 내의 시스템의 연결성, 위치한 정책 그룹 등을 변경하는 shuffle 기술로 나눌 수 있다. 또한 네트워크 전체 혹은 각 시스템의 구성 및 세부 설정을 변경하는 다양성 기반의 기술로도 구분 지을 수 있다. 마지막으로 DDoS(Distributed Denial of Service) 공격 등을 방지하기 위해 다수의 복제 시스템을 만들어 대비하는 가용성 관점에서의 기술들이 있다. 저자는 세 기준의 MTD 기술을 평가하기 위해 공격 그래프와 공격 트리(attack tree)를 함께 이용하는 방법에 대해 제안하였다.

Ankur Chowdhary 등[41]은 SDN 기반의 DAC(Detect-Analyze-Countermeasure) 구조를 이용하며 대응 방안을 만들기 위해 공격 그래프를 사용하는 프레임워크를 제안하였다. 저자는 침입이 발생했을 때 이에 대응하기 위해 공격 그래프를 이용하여 MTD 기술을 적합하게 적용하는 방안을 연구하였다. 공격 그래프를 생성하는데 필요한 시간을 줄이기 위해 네트워크 내의 시스템들을 수 개의 그룹으로 묶는 방법을 제안하였으며 자산 랭크 알고리즘을 기반으로 자산의 중요도를 평가해 가장 먼저 방어해야 할 자산에 대한 대응책을 마련하는 방안을 제시하였다.

Simon Enoch Yusuf 등[42]은 T-HARM(Temporal-Hierarchical Attack Representation Model)을 제안하여 동적 네트워크의 보안성을 평가하고 취약점이 새로이 등장하거나 취약점을 패치한 경우 네트워크의 위험도 변화를 측정하였다. 취약점이 새로 발견되거나 기존의 취약점을 패치한 경우 기존의 보안 메트릭들의 값은 변경된다. 이를 확인하기 위해 해당 논문에서는 시계열성 그래프(temporal graph)를 이용하여 동적 네트워크의 변화를 확인하는 방안을 제안하였으며 네트워크에 존재하는 취약점 개수가 적은 경우와 많은 경우에 동적 네트워크의 보안성을 평가하기 위한 메트릭들을 구분하였다.

Joo Yeon Moon 등[43]은 MTD 및 SDN이 적용된 네트워크에서 네트워크 내의 변경사항을 탐지하여 공격 그래프를 생성하고 갱신하는 알고리즘 및 프레임워크를 제안하였다. 해당 논문에서는 네트워크 내의 변경사항이 탐지될 때마다 연산의 효율성을 위해 기존 공격 그래프를 수정하는 방법을 통해 MTD 기술이 접목된 네트워크에서 공격 그래프를 효율적으로 생성하였다. 그러나 MTD 환경에 알맞은 별도의 보안 메트릭이 구체적으로 제안되지 않아 네트워크 내에서 탐지되는 변경사항을 반영할 수 없다는 단점이 있다.

위의 네 연구는 모두 MTD 기술과 기존의 공격 그래프를 접목한 연구로 볼 수 있다. 각각은 MTD 기술의 효용성 분석 및 공격 그래프 기반의 MTD 적용 방안에 대해 제안하고 있다. 그러나 MTD 와 SDN 기술이 비교적 최근 등장한 기술이기 때문에 이를 적용한 연구가 충분히 이루어지지 않은 한계점이 있다. [39]의 경우, 호스트 수의 증가에 따른 MTD 공격 그래프의 크기가 급격히 증가하여 연산량의 문제가 있다. 또한 실험을 진행하는 데 있어 임의의 확률값을 이용하여 더욱 명확한 보안 메트릭이 제시되지 않은 문제점이 있다. [40]은 네트워크 환경을 모델링하는 기술과 취약점의 위험성 등을 연산하는 기술이 부족하다는 한계가 있다는 것을 기술하고 있다. [31]와 [42] 및 [43]의 경우, 연구에서 제안하는 별도의 메트릭이 없으며 MTD 기술이 적용될 때 메트릭의 변화를 고려하지 않은 한계가 있다. 이처럼 지금까지의 연구들은 MTD 기술을 공격 그래프에 적절하게 적용하였다는 장점이 있다. 그러나 세부 메트릭을 이용하여 위험성을 보다 객관적으로 판단하고 그래프를 효율적으로 생성하는 방안이 없다는 한계가 존재한다.

최신 기술에 발맞추어 공격 그래프를 생성하기 위해 크게 두 가지 연구가 필요하다. 첫째, MTD 기술의 적용에 따른 경량화된 공격 그래프 생성 및 갱신 알고리즘이 필요하다. MTD 기술 중 시간 간격마다 네트워크 구성을 변경하는 기술 혹은 decoy 시스템을 이용하는 기술 등과 같이 주기적인 공격 그래프의 재구성이 필요한 경우, 공격 그래프를 빠르게 생성할 필요가 있다. 둘째, MTD 기술 적용에 따른 새로운 보안 메트릭의 개발이

필요하다. 기존의 보안 메트릭은 MTD 기술이 도입된 네트워크에서 공격 경로의 위험성 및 자산의 안전성을 평가하는 데 부족한 점이 있다. 예를 들어 CVSS 기반의 보안 메트릭의 경우, 시스템의 포트 및 IP주소의 변경에 따른 효과를 반영하지 못해 충분한 안전성 평가가 불가능한 단점이 있다. 이처럼 경량화된 공격 그래프 생성 기법과 더불어 MTD 기술의 적용을 고려한 새로운 보안 메트릭에 대한 연구가 필요하다. 네트워크 전체의 설정에 대한 엔트로피(entropy)를 계산하여 설정 변경 전후의 변화량을 측정한 후 네트워크의 안전성을 평가하는 방식 등이 하나의 예라고 볼 수 있다.

VII. Analysis

앞서 조사한 공격 그래프상의 보안 메트릭들은 각 메트릭이 적용되는 관점에 따른 쟁점이 존재한다. 생성하고자 하는 공격 그래프와 네트워크가 적용된 상황에 따라 고려할 수 있는 요소가 각기 다르기 때문에 알맞은 보안 메트릭을 도입하는 것에는 어려움이 따른다. 이러한 결정을 돕기 위해 본 논문에서는 각 보안 메트릭 세부 메트릭 관점별 주요 쟁점을 크게 다섯 가지 측면에서 분류하였으며 그 결과는 Table 4.와 같다. 위상 및 취약점의 관점, CVSS 사용 여부의 관점은 세부 메트릭 관점의 분류에 따라 그 특성이 잘 녹아들어 있어 별도로 분류하지 않았다. 각각의 측면에 대해 보안 메트릭이 지니는 강점을 크게 H(high), M(medium), L(low)로 표현하였다.

객관성(objectivity)은 사용한 보안 메트릭의 평가 방식이 얼마나 객관적인지에 대해 검증이 가능한지를 나타내는 지표이다. **정량성(quantitative)**은 보안 메트릭이 사용한 관점이 정량적으로 표현될 수 있는지에 대한 지표이다. **공격자의 입장에 대한 고려 여부(attacker's side)**는 해당 보안 메트릭이 시스템을 방어하는 것과 더불어 공격에 필요한 노력 등의 공격자 측면에서의 고려사항이 있었는지에 대한 지표이다. **확장성(scalability)**의 경우 제안한 보안 메트릭이 한정된 시스템이 아닌 다양한 종류의 시스템에서 원활하게 동작할 수 있는지 여부이다. 마지막으로 **적용성(applicability)**은 해당 보안 메트릭이 네트워크 내에 발생하는 변화에 대해 적응하는 데 필요한 연산량 등을 고려한 지표이다.

확률 기반의 보안 메트릭은 공격 성공 확률 등을 계산하는 데 있어 비교적 객관적인 지표를 얻기가 어려워 낮은 객관성을 보인다. 그러나 확률이 수치로 표현되며 공격자의 입장에서 성공률을 계산하는 측면, 어떠한 시스템에서라도 수학적 연산인 확률 연산이 가능한 측면 등을 고려하여 Table 4.와 같은 평가를 할 수 있다. **네트워크 및 시스템 모델을 이용하는 보안 메트릭**은 수학적으로 검증된 모델을 평가에 사용하기 때문에 높은 객관성을 가질 수 있다. 그러나 사용한 모델에 따라 정량적인 평가가 불가능할 수 있으며 네트워크가 변화할 때마다 모델을 새로 적용해야 하는 단점 등으로 인해 낮은 정량성 및 적용성을 보인다. **기존에 연구되어온 알고리즘을 도입한 보안 메트릭**은 앞선 메트릭과 마찬가지로 수학적으로 검증된 알고리즘을 사용하였기 때문에 높은 객관성을 가질 수 있다. 그러나 사용하는 시스템에 따라 적용할 수 없는 경우가 발생할 수 있으며 네트워크 변화에 따라 새로운 계산이 필요하다는 점에서 낮은 확장성 및 적용성을 보인다. **CVSS 점수를 사용하는 보안 메트릭**의 경우, 보안 전문가들의 판단에 의해 매겨진 점수를 이용하기 때문에 비교적 적당한 객관성을 가질 수 있다. 또한 각 평가를 점수로 구체화하여 높은 정량성을 보일 수 있으며 공격의 어려움 등을 고려하는 데 있어서 공격자의 입장도 잘 고려할 수 있다. 마찬가지로 시스템 내에 존재하는 취약점에 따라 점수를 부여할 수 있기 때문에 높은 확장성을 보이며 네트워크의 변화에 대해 변화한 취약점을 확인하고 즉각적인 대처를 할 수 있어 높은 적용성을 보인다. **네트워크 구성을 이용하는 보안 메트릭**은 네트워크의 구성이라는 객관적인 정보를 이용한 평가 방법이기 때문에 높은 객관성을 보이나, 이를 정량화하는 데에는 적합한 기준이 부족하여 낮은 정량성을 보인다. 그러나 네트워크의 구성에 대한 변경점을 즉각적으로 확인하고 반영할 수 있으며 네트워크 환경이 다양하더라도 구성을 확인하는 데에는 어려움이 적어 비교적 높은 적용성 점수를 부여할 수 있다. 마지막으로 **공격에 대한 저항성을 이용한 보안 메트릭**은 안정성을 평가하는 지표인 네트워크의 다양성, 저항성 등이 네트워크 관리자의 의견을 바탕으로 수립되기에 비교적 낮은 객관성을 보인다. 또한 이러한 지표들이 정량적으로 표기되어 수식으로 연산할 방안이 명확하지 않아 비교적 낮은 정량성을 보인다. 그러나 공격에 대한 저항성을 계산하는 데 있어 공격자의 노력 등을 고려하기에 이 점에서 높은 점수를 부여할 수 있다.

총 다섯 가지의 보안 메트릭 평가 관점 중 MTD 및 SDN이 도입된 네트워크에서 보안 메트릭을 사용하기 위해서는 주로 확

Table 4. Evaluation of 5 aspects in security metrics

Metrics	Objectivity	Quantitative	Attacker's side	Scalability	Applicability
Probability	L	H	H	H	M
Using network or system model	H	L	L	L	L
Using algorithm	H	L	L	L	L
CVSS score	M	H	H	H	H
Network attributes	H	L	M	H	H
Resistance or safetiness to attack of network	L	L	H	H	L

장성과 적용성을 고려할 필요가 있다. SDN이 도입된 네트워크는 중앙 컨트롤러 및 정보 스위칭 기기와 같은 기존 공격 그래프에서 제안하는 네트워크 시스템과는 다른 구성을 보인다. 이러한 환경에서 보안 메트릭을 보다 적절하게 적용하기 위해서는 메트릭의 확장성을 고려해야 한다. 또한 MTD 환경은 지속해서 네트워크의 정보가 변경되는 특성을 보이고 있기 때문에 이를 반영할 수 있도록 높은 적용성을 보이는 메트릭을 이용해야 한다. 메트릭을 더욱 명확하게 표현하고 관리자가 한눈에 알아보기 쉽게 하기 위해 객관성 및 정량성이 부가적으로 고려되어야 한다. 이러한 점으로 미루어 보아 총 6가지의 보안 메트릭 중 CVSS 점수, 네트워크 구성, 확률을 이용한 보안 메트릭이 비교적 MTD 및 SDN 환경에서 적합할 것으로 기대된다.

VIII. Conclusions

기업 및 기관이 가진 정보 자산의 중요성이 날이 갈수록 늘어나면서 다양한 방어 기법과 더불어 보안성 및 안전성을 평가하기 위한 보안 메트릭에 대한 연구가 이뤄지고 있다. 공격자의 예상 침입 경로를 도식화하여 관리자가 빠른 의사결정을 내리도록 돕는 공격 그래프는 일련의 보안 메트릭을 이용해 네트워크의 보안성을 정량적으로 평가한다. 그러나 네트워크의 설정 및 환경과 같은 요소들이 매우 다양하기 때문에 이를 고려하기 위한 다양한 관점의 보안 메트릭에 대한 연구가 이루어져야 한다.

본 논문에서는 공격 그래프상에서 이용하는 보안 메트릭에 대한 연구들을 조사하였으며 이를 메트릭 적용 관점, CVSS 사용 여부, 세부 메트릭이라는 3가지 기준으로 분류하였다. 또한 세부 메트릭에 따른 분류에 대해 각 메트릭이 지니는 특성을 크게 다섯 가지 관점에서 정리하였다. 더 나아가 정리한 관점을 이용하여 새로이 도입되는 기술을 기존 공격 그래프에 적용하기 위해 고려해야 할 사항에 대해 논의하였다. 본 연구를 통해 다양한 보안 메트릭에 대한 연구들을 공격 그래프의 생성 관점에 맞추어 적절히 적용할 수 있을 것으로 기대된다. 더 나아가 새로운 기술들을 도입한 네트워크에서의 공격 그래프 생성 방안 및 보안 메트릭 연구에 있어 중점적으로 고려해야 할 점이 무엇인지에 대해서도 도움을 줄 수 있으리라 기대된다.

REFERENCES

[1] Ministry of Science and ICT, *http://www.index.go.kr/potal/main/EachDtlPageDetail.do?idx_cd=1363*

[2] Schneier, Bruce. "Attack trees." Dr. Dobb's journal 24.12 (1999): 21-29.

[3] Phillips, Cynthia, and Laura Painton Swiler. "A graph-based system for network-vulnerability analysis," Proceedings of the 1998 workshop on New security paradigms. pp. 71-79, Charlottesville, Virginia, USA, September, 1998.

[4] National Institute of Standards and Technology Glossary, *https://csrc.nist.gov/glossary/term/vulnerability*

[5] CVE, *https://cve.mitre.org/*

[6] CVSS, *https://www.first.org/cvss*

[7] Ou, Xinming, Sudhakar Govindavajhala, and Andrew W. Appel. "MulVAL: A Logic-based Network Security Analyzer," USENIX Security Symposium. Vol. 8, 2005.

[8] Ingols, Kyle, Richard Lippmann, and Keith Piwowarski. "Practical attack graph generation for network defense," Computer Security Applications Conference, pp. 121-130, December, 2006.

[9] Ortalo, Rodolphe, Yves Deswarte, and Mohamed Kaâniche. "Experimenting with quantitative evaluation tools for monitoring operational security," IEEE Transactions on Software Engineering Vol. 25, No. 5, pp. 633-650, September, 1999

[10] Mehta, Vaibhav, et al. "Ranking attack graphs," International Workshop on Recent Advances in Intrusion Detection. pp. 127-144, 2006.

[11] Idika, Nwokedi, and Bharat Bhargava. "Extending attack graph-based security metrics and aggregating their application," IEEE Transactions on Dependable and Secure Computing Vol. 9, No. 1, pp. 75-85, January, 2012.

[12] National Institute of Standards and Technology, *https://www.nist.gov*

[13] Balzarotti, Davide, Mattia Monga, and Sabrina Sicari. "Assessing the risk of using vulnerable components," Quality of Protection, pp. 65-77, 2006.

[14] Wang, Lingyu, et al. "An attack graph-based probabilistic security metric," IFIP Annual Conference on Data and Applications Security and Privacy, Vol. 5094. pp. 283-296, 2008.

[15] Gallon, Laurent, and Jean Jacques Bascou. "Using CVSS in attack graphs," Availability, Reliability and Security, 2011 Sixth International Conference on. IEEE, pp. 59-66, 2011.

[16] Wang, Lingyu, Anoop Singhal, and Sushil Jajodia. "Measuring the overall security of network configurations using attack graphs," IFIP Annual Conference on Data and Applications Security and Privacy, Vol. 4602, pp. 98-112, 2007.

[17] Suh-Lee, Candace, and Juyeon Jo. "Quantifying security risk by measuring network risk conditions," Computer and Information Science (ICIS), 2015 IEEE/ACIS 14th International Conference on. IEEE, pp. 9-14, July, 2015.

[18] National Vulnerability Database, *https://nvd.nist.gov*

[19] Pamula, Joseph, et al. "A weakest-adversary security

metric for network configuration security analysis," Proceedings of the 2nd ACM workshop on Quality of protection. ACM, pp. 31-38, October, 2006.

[20] Noel, Steven, et al. "Measuring security risk of networks using attack graphs," International Journal of Next-Generation Computing, Vol. 1, No. 1, pp. 135-147, July, 2010.

[21] Tupper, Melanie, and A. Nur Zincir-Heywood. "VEA-bility security metric: A network security analysis tool," Availability, Reliability and Security, 2008. ARES 08. Third International Conference on. IEEE, pp. 950-957, March, 2008.

[22] Keramati, Marjan, Ahmad Akbari, and Mahsa Keramati. "CVSS-based security metrics for quantitative analysis of attack graphs," Computer and Knowledge Engineering (ICCKE), 2013 3th International eConference on. IEEE, pp. 178-183, November, 2013.

[23] Dai, Fangfang, et al. "Exploring risk flow attack graph for security risk assessment," IET Information Security Vol. 9, No. 6, pp. 344-353, November, 2015.

[24] Singhal, Anoop, and Xinming Ou. "Security risk analysis of enterprise networks using probabilistic attack graphs," Network Security Metrics, pp.53-73, November, 2017.

[25] Xie, Lixia, Xiao Zhang, and Jiyong Zhang. "Network Security Risk Assessment Based on Attack Graph," Journal of Computers Vol. 8, No. 9, pp. 2339-2347, September, 2013.

[26] Homer, John, et al. "Aggregating vulnerability metrics in enterprise networks using attack graphs," Journal of Computer Security Vol. 21, No. 4, pp. 561-597, September, 2013.

[27] Frigault, Marcel, and Lingyu Wang. "Measuring network security using bayesian network-based attack graphs," Annual IEEE International Computer Software and Applications Conference. IEEE, pp. 698-703, August, 2008.

[28] Poolsappasit, Nayot, Rinku Dewri, and Indrajit Ray. "Dynamic security risk management using bayesian attack graphs," IEEE Transactions on Dependable and Secure Computing, Vol. 9, No. 1, pp. 61-74, June, 2012.

[29] Liu, Si-chao, and Yuan Liu. "Network security risk assessment method based on HMM and attack graph model," 2016 17th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD). IEEE, pp. 517-522, June, 2016.

[30] Sawilla, Reginald E., and Xinming Ou. "Identifying critical attack assets in dependency attack graphs," European Symposium on Research in Computer Security, Vol. 5283, pp. 18-34, 2008.

[31] Hui, Wang, Chen Fuwang, and Wang Yunfeng. "An Approach of Security Risk Evaluation Based on the Bayesian Attack Graph," Open Cybernetics & Systemics Journal, Vol. 9, pp. 953-960, 2015.

[32] Noel, Steven, and Sushil Jajodia. "Metrics suite for network attack graph analytics," Proceedings of the 9th Annual Cyber and Information Security Research Conference. ACM, pp. 5-8, April, 2014.

[33] Moon, Young Hoon, et al. "Hybrid Attack Path Enumeration System Based on Reputation Scores," Computer and Information Technology (CIT), 2016 IEEE International Conference on. IEEE, pp. 241-248, December, 2016.

[34] Ghosh, Nirnay, and Soumya K. Ghosh. "An approach for security assessment of network configurations using attack graph," Networks and Communications, 2009. NETCOM'09. First International Conference on. IEEE, pp. 283-288, December, 2009.

[35] Ge, Mengmeng, Huy Kang Kim, and Dong Seong Kim. "Evaluating Security and Availability of Multiple Redundancy Designs when Applying Security Patches." Dependable Systems and Networks Workshop (DSN-W), 2017 47th Annual IEEE/IFIP International Conference on. IEEE, pp. 53-60, June, 2017.

[36] Singh, Umesh Kumar, and Chanchala Joshi. "Quantifying security risk by critical network vulnerabilities assessm ent," International Journal of Computer Applications, Vol. 156, No. 13, pp. 26-33, December, 2016.

[37] Zhang, Mengyuan, et al. "Network diversity: a security metric for evaluating the resilience of networks against zero-day attacks," IEEE Transactions on Information Forensics and Security, Vol. 11, No. 5, pp. 1071-1086, January, 2016.

[38] Jessica Steinberger et al. "DDoS defense using MTD and SDN," IEEE Network Operations and Management Symposium 2018 on. IEEE, April, 2018.

[39] Zhuang, Rui, et al. "Investigating the application of moving target defenses to network security," Resilient Control Systems (ISRCS), 2013 6th International Symposium on. IEEE, pp. 162-169, August, 2013.

[40] Hong, Jin Bum, and Dong Seong Kim. "Assessing the effectiveness of moving target defenses using security models," IEEE Transactions on Dependable and Secure Computing, Vol. 13, No. 2, pp. 163-177, April, 2016.

[41] Chowdhary, Ankur, Sandeep Pisharody, and Dijiang Huang. "Sdn based scalable mtd solution in cloud network," Proceedings of the 2016 ACM Workshop on Moving Target Defense. ACM, pp. 27-36, October, 2016.

[42] Yusuf, Simon Enoch, et al. "Security Modelling and Analysis of Dynamic Enterprise Networks." Computer and Information Technology (CIT), 2016 IEEE International Conference on. IEEE, pp.249-256, December, 2016.

[43] Joo Yeon Moon, Taekyu Kim, Insung Kim, and Huy Kang Kim. “An attack graph model for dynamic network environment,” Journal of The Korea Institute of Information Security & Cryptology, Vol. 28, No. 2, pp. 485-500, April, 2018.

Authors

Gyung-Min Lee received the B.S. degrees in Computer Science from Korea University, Korea, in 2018. He is currently a M.S. student studying the major of Information Security at Korea University. His research interests are in the areas of information security, online game security and system security.

Huy-Kang Kim received his B.S. degree in Industrial Management in 1998, M.S. and Ph.D degrees in industrial and systems engineering from KAIST in 2000 and 2009, respectively. He founded A3 Security Consulting, the first information security consulting company in Korea in 1999. Currently he is an associate professor in Graduate School of Information Security, Korea University. Before joining Korea University, he was a technical director (TD) and a head of information security department of NCSOFT (2004~2010). His research interests include solving security problems in online games based on the user behavior analysis and data mining.