Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.34, NO.1, Feb. 2024 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2024.34.1.53

위험 관리를 위한 MITRE ATT&CK 기반의 정량적 보안 지표*

김 해 린,[1†‡] 이 승 운,[2] 홍 수 연[3]
[1,2,3]LIG넥스원 (연구원, 선임연구원, 수석연구원)

A Quantitative Security Metric Based on MITRE ATT&CK for Risk Management*

Haerin Kim,[1†‡] Seungwoon Lee,[2] Su-Youn Hong[3]
[1,2,3]LIG Nex1 (Researcher, Senior Researcher, Chief Researcher)

요 약

안전한 네트워크를 위해 보안 평가는 필수불가결한 과정으로, 위험을 관리하기 위해서는 적절한 성능지표가 있어야 한다. 가장 널리 사용하고 있는 정량적 지표로는 CVSS가 있다. CVSS는 주관성과 해석의 복잡성, 보안 위험의 관점에서 맥락을 고려하지 못한다는 문제가 있다. 이러한 문제를 보완하기 위해 ISO/IEC 15408 문서의 보안 개념 및 관계도를 바탕으로 공격자, 위협, 대응, 자산의 4가지를 항목화하고 수치화 하는 지표를 제안한다. 네트워크 스캐닝을 통해 발견된 취약점은 약점, 공격패턴의 연결관계에 의해 MITRE ATT&CK의 기술과 매핑시킬 수 있다. 우리는 MITRE ATT&CK 의 Groups, Tactic, Mitigations을 이용하여 일관성을 가지며 직관적인 점수를 산출한다. 이에 따라 보안 평가 관리자가 다양한 관점의 보안지표 중 선택할 수 있는 폭을 넓히고, 사이버 네트워크의 보안을 강화하는데 긍정적인 영향을 기대한다.

ABSTRACT

Security assessment is an indispensable process for a secure network, and appropriate performance indicators must be present to manage risks. The most widely used quantitative indicator is CVSS. CVSS has a problem that it cannot consider context in terms of subjectivity, complexity of interpretation, and security risks. To compensate for these problems, we propose indicators that itemize and quantify four things: attackers, threats, responses, and assets, taking into account the security context of ISO/IEC 15408 documents. Vulnerabilities discovered through network scanning can be mapped to MITREATT&CK's technology by the connection between weaknesses and attack patterns (CAPEC). We use MITRE ATT&CK's Groups, Tactic, and Mitigations to produce consistent and intuitive scores. Accordingly, it is expected that security evaluation managers will have a positive impact on strengthening security such as corporate networks by expanding the range of choices among security indicators from various perspectives.

Keywords: Security metric, MITRE ATT&CK, Risk management

Received(10. 16. 2023), Modified(12. 18. 2023), Accepted(12. 18. 2023)

* 이 논문은 2021년 정부(방위사업청)의 재원으로 국방기술진흥연구소의 지원을 받아 수행된 연구임 (KRIT-CT-21-042)

† 주저자, haerin.kim@lignex1.com
‡ 교신저자, haerin.kim@lignex1.com(Corresponding author)

I. 서 론

디지털 시대에 클라우드 전환에 따라 비대면 원격 근무 환경 변화, 우크라이나 사태가 장기화됨에 따라 시대적, 기술적, 국가적으로 사이버 보안 위협이 증가하고 있다 [14]. Griffths [13]가 조사한 사이버 범죄 통계 기사에 따르면, 2022년 데이터 유출로 인해 기업은 평균 435만 달러의 손실을 입었고, 영국 기업의 39%가 사이버 공격을 당했다고 보고했다. 정보보안과 개인정보보호는 사고가 발생할 경우 경제적 손실과 개인 사생활, 국가적 안보에도 큰 영향을 미치기 때문에 선제적으로 위험관리를 하는 것이 필요하다. 위험 관리에 있어서 정량적 보안지표는 IT 자산을 파악하고 위협을 모델링하면서 보안 수준을 파악하기 위한 중요한 도구이다. 하지만 널리 사용되는 Common Vulnerability Scoring System (CVSS) 점수와 정성적 전문가의 평가만으로는 일관적이고 최신화된 보안 성능을 측정하기가 어렵다. 따라서 우리는 국제 표준화 기구에서 제안한 보안 개념과 관계 도식 [15]에 따라 위험에 직접적으로 영향을 미치는 1) 위험을 발생시키는 잠재적 위협, 2) 위협을 일으키는 위협원, 3) 위험을 유발하는 취약점에 대한 자산 소유자의 대응, 4) 위험에 처하는 대상 자산으로 위험을 다각도로 고려한 4가지 요소를 MITRE ATT&CK 프레임워크에서 식별하였다. 취약점인 CVE에 대해 CWE, CAPEC 연결관계를 추론하여 MITRE ATT&CK 의 위협 기술을 도출한다. 위협 기술에 초점을 두고 방어 기술, 공격자 그룹, 자산의 보안에 해당하는 각 관계를 이용하여 그 개수를 기반으로 보안 점수를 산출하였다. 우리가 제안하는 보안지표는 MITRE ATT&CK를 기반으로 CVSS의 단점을 보완하여 일관성과 공격의 맥락 파악, 최신화가 가능하도록 설계하였고 직접 가상의 네트워크를 구성하여 보안 성능을 계산한다. 마지막으로 대규모 인프라에 적용할 경우 활용하는 방법을 기술하였고 제안하는 지표는 CVSS에 비해 보안의 위험을 다각도로 분석할 수 있다는 점에서 장점이 있다.

II. 문헌 연구

2.1 MITRE ATT&CK

MITRE ATT&CK [1]는 실제 세계의 관찰 기반으로 공격자의 전술과 기술 및 절차(TTP, Tactics, Techniques, and Procedures)를 정리해 둔 지식 베이스 프레임워크이다. 인터넷 상에 공개되어 있어 전 세계 누구나 무료로 사용 가능하며 사이버 보안과 관련하여 위협 모델링이나 방법론 개발을 위해 널리 사용되고 있다. Ahn 등[3]은 사이버 공격에 대한 의사결정을 지원하는데 있어 공격그래프와 MITRE ATT&CK 매트릭스를 이용하여 그 효과를 평가했다. Ahmed 등[4]은 지능형 사이버 위협으로부터 위험을 평가하기 위해 MITRE ATT&CK를 활용하여 공격 확률과 공격 성공 가능성을 판단하였다. Kwon 등[5]은 MITRE ATT&CK 매트릭스를 NIST 사이버 보안 프레임워크에 매핑시켜 위협에 대한 대응방법을 사이버 위협 사전으로 제안하였다. MITRE ATT&CK는 공신력 있는 프레임워크로 우리는 본 프레임워크에 기술되어 있는 전술, 방어 기술, 공격자 그룹을 사용한다.

2.2 CVSS

제한된 보안 자원을 현명하게 배분하기 위해 시스템의 전반적인 위험을 정량화 할 수 있는 보안 지표는 오래전부터 연구되어 왔다 [6]. Doynikova 등[8]은 보안 데이터 소스, 보안 정보, 보안 관리 주체와 지표를 정리하여 온톨로지를 제안하였다. 가장 널리 사용되는 정량적 보안 지표로는 CVSS (Common Vulnerability Scoring System) [9]가 있다. 이 지표는 NVD (National Vulnerability Database) [10]에서 제공하는 것으로, 소프트웨어 취약점의 특성과 심각도를 파악할 수 있는 공개 프레임워크이다. 점수는 기본, 시제, 환경 3가지 종류의 지표를 기준으로 정량화하며 각 관점에서 보안 취약점의 특성을 산출한다. Spring 등[11]은 CVSS가 가진 문제들을 분석했다. 그들이 주장하는 주된 문제는 주관성과 해석의 복잡성이다. CVSS의 지표는 여러 가지 기준으로 구성되어 있으며 사용자와 환경에 따라 다르게 해석될 여지가 있다는 것이다. 그리고 CVSS 점수는 심각도에 대한 지표이고 보안 위험도를 나타내지 않는다. 예를 들어 보안 사고를 유발하는 맥락이나 피해에 대해 고려하지 않는다는 것이다. 따라서 CVSS는 주관성, 복잡성, 맥락성 부분에서 보완이 필요하다.

III. 제안하는 보안 지표

CVSS의 한계를 극복하기 위해 우리가 제안하는 정량적 보안지표는 네트워크의 전반적인 위험관리를 포함한다. 네트워크에 있는 개별 자산의 취약점을 바탕으로 위험을 수치화하여 평가한다. Fig. 1의 가운데 그림에서 나타낸 것과 같이 위험에 영향을 주는 요소들을 항목화하였다.

3.1 취약점과 MITRE ATT&CK의 연계

우리는 BRON [12]을 이용하여 발견된 취약점을 ATT&CK [1]의 Technique과 연결한다. 그 과정에는 3가지 연결성이 존재하는데, 먼저 Common Vulnerability Enumerations (CVE) 취약점은 Common Weakness Enumerations (CWE) 약점과 대응관계가 존재한다. 두 번째로 약점이 존재하면 이를 악용하는 공격이 가능하므로 CWE 약점은 Common Attack Pattern Enumeration and Classification (CAPEC) 공격패턴과 상관관계가 있다. 마지막으로 CAPEC 공격패턴은 ATT&CK의 Technique과 연결된다.

3.2 위험 관련 수치화 항목 식별

최종적으로 취약점에 매핑되는 위협 기술을 이용하여 ISO/IEC 15408-1 표준화 문서[15]에서 나타낸 위험 개념도에서 위험과 직접적으로 관련 있는 대응, 위협원, 위협, 자산을 ATT&CK의 Mitigation, Group, Tactic, Asset과 연결시킨다. Fig. 1의 오른쪽에 있는 보안 맥락을 나타내는 도식은 자산 소유자, 보안 대책, 취약점, 위협원, 위협, 위험, 자산으로 구성되어 상호간의 연결 관계를 가지고 있다. 위험을 중심으로 자산 소유자는 자산에 가치를 부여하고 위험을 최소화하고자 한다. 그러나 위협원에서 발생시키는 위협은 위험을 증가시킨다. 이 위험은 곧 자산으로 이어지기 때문에 소유자는 보안대책을 통해 위험을 감소시키려고 한다. 위험에 직접적인 영향을 주는 요소로는 위협, 보안대책, 자산이 있다. 더불어 위협을 가하는 근원이 위협원이기 때문에, 위협원인 공격자의 목적이나 기술이 상당히 중요하다.

3.3 점수 산출 방법

우리는 공격자, 보안대책, 위협, 자산인 총 4가지에 대한 지표를 위협모델링에서 자주 사용되는 ATT&CK에 기반하여 제안하였고 발견된 취약점에 대해 매핑되는 기술은 아래 식 (1)을 통한 점수로 산출한다. 하나의 취약점에 대한 점수는 기술 당 점수의 합산으로 측정한다.

$$Score(T) = \frac{N_G}{Total_G} + \left(1 - \frac{N_M}{Total_M}\right) + \frac{TA_n}{Total_{TA} \times N_{TA}} + \frac{N_{C.I.A}}{Tatal_{TA(Impact)}} \quad (1)$$

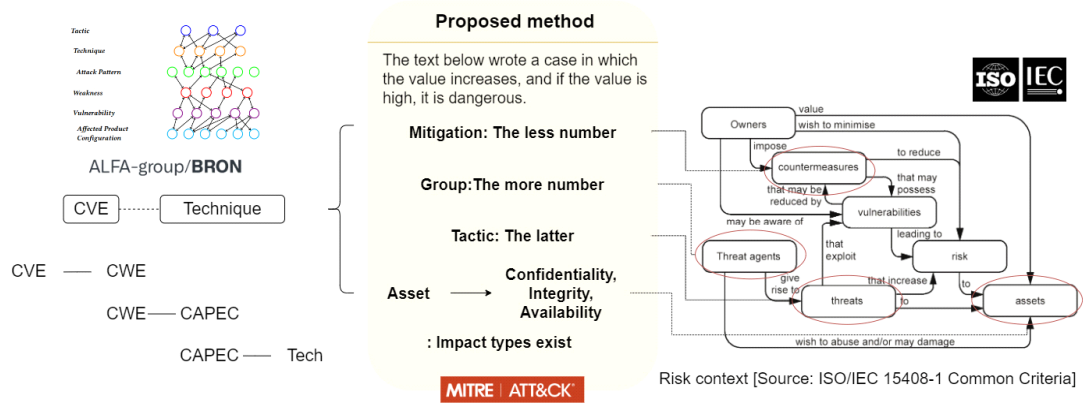


Fig. 1. The proposed security metric link vulnerabilities with threat technique and measure higher score with fewer mitigations to the technique, more attack groups using the technique, the later the tactical stages belonging to the technique, and the impact of asset confidentiality, integrity, and availability. Each element refers to the security concept and relationship diagram of the ISO/IEC 15408-1.

제안하는 점수는 각 기술에 대해 산출되므로 Score(T)의 T는 Technique의 약자이다. $\frac{N_G}{Tatal_G}$의 G는 ATT&CK의 공격자 그룹을 설명하고 있는 Groups의 약자로, 취약점과 매핑되는 기술을 사용했던 공격자 수를 이용하여 전체 공격자 수로 나누고 합이 1이 되도록 나타낸다. 대응을 고려하기 위한 $\frac{N_M}{Tatal_M}$에서 M은 ATT&CK의 방어 기술을 나타내는 Mitigations의 약자이며 기술에 매핑되는 방어 기술의 수를 전체 방어의 수로 나누는데, 이 값은 방어 기술의 수가 많을수록 위협을 조치하기 위한 방법의 수가 많다고 판단하여 위험도가 낮다고 가정한다. 따라서 식 (1)에서 계산된 값을 뺀다. $\frac{TA_n}{Total_{TA} \times N_{TA}}$에서 TA는 ATT&CK의 Tactic의 약자이다. 우리는 위협에 대한 점수를 기술이 속한 전술의 단계를 총 전술의 단계와 전술의 개수의 곱으로 나누어 산출한다. 초기에 사용되는 전술일수록 낮은 위험도를 가지고 후기에 사용되는 전술일수록 공격이 진행중인 상태일 확률이 높으며 가능한 대응이 많지 않으므로 높은 값을 가지도록 한다. 자산은 정보보안의 3요소인 기밀성, 무결성, 가용성을 보존함으로써 달성된다. $\frac{N_{C.I.A}}{Tatal_{TA(Impact)}}$에서 C.I.A는 기밀성(Confidentiality), 무결성(Integrity) , 가용성(Availability)을 나타내며, ATT&CK의 TA0040(impact) 전술에서 impact type으로 정의된 기밀성, 무결성, 가용성의 값을 이용한다. 즉, 발견된 취약점과 매핑된 기술이 impact 전술에 속한 기술이며 impact type이 존재한다면 점수를 부여한다. 해당 항에 대한 결과값을 0과 1사이로 제한하기 위해 impact type에 대한 개수를 impact 전술에 속한 기술의 총 개수로 나눈다.

3.4 가상 환경 설정 및 실험

우리가 제안하는 보안지표를 사용하여 하나의 네트워크에서 사이버 보안 관점의 위험을 관리하는 전반적인 과정은 Fig. 2와 같다. 자산모델링과 취약점 스캐닝은 예시를 바탕으로 하여 MITRE 버전 13.1, BRON v3을 기준으로 Table 3을 나타낼 수 있다. 각 자산에 대하여 발견된 취약점인 CVE를

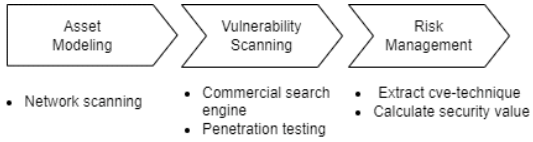


Fig. 2. Risk management process utilizing proposed security metric.

하나씩 무작위로 선정하였다. 그리고 BRON을 통해 CVE와 매핑된 Technique을 구할 수 있고 ATT&CK를 이용하여 Technique에 매핑된 Group, Mitigation, Tactic, 기밀성, 무결성, 가용성을 찾을 수 있다.

예시로 보안지표를 산출하는 과정을 보여주기 위해, 위협 모델링에서 학술적으로 자주 사용되는 공격 그래프 프레임워크 MulVAL [16]의 논문에서 샘플 네트워크를 인용하였다. Fig. 3에는 웹서버와 파일서버, 워크스테이션으로 크게 3개의 호스트가 존재하며 방화벽, 인터넷 환경이 네트워크를 구성하고 있다. 공격자 그룹의 전체 수는 136, 방어 기술의 전체 수는 43, 전술의 총 단계 수는 14, Impact 전술의 총 기술의 수는 26개이다. 따라서 식 (1)에 의해 Fig. 3 네트워크의 파일서버 자산의 보안점수는 T1027.006, T1027.009, T1564.009에 대한 점수의 합산인 4.44점으로 산출할 수 있으며, 각각의 산출식은 다음과 같다.

- $Score(T1027.006) = \frac{1}{136} + \left(1 - \frac{0}{43}\right) + \frac{7}{14 \times 1} + 0 = 1.51$
- $Score(T1027.009) = \frac{0}{136} + \left(1 - \frac{2}{43}\right) + \frac{7}{14 \times 1} + 0 = 1.45,$

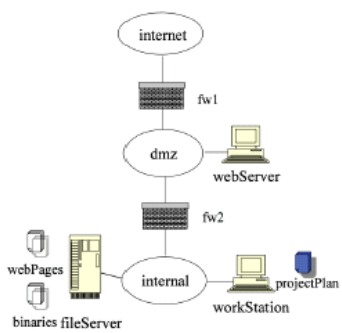


Fig. 3. Example network [16]

- $Score(T1564.009)$
$$= \frac{1}{136} + \left(1 - \frac{1}{43}\right) + \frac{7}{14 \times 1} + 0 = 1.48$$

자산에는 여러개의 취약점이 존재할 수 있다. 그리고 하나의 취약점에는 해당 약점을 이용하는 다양한 방법의 공격패턴에 의해 한 개 이상의 공격 기술들이 매핑된다. 우리가 제안하는 방법론은 하나의 공격 기술에 대해 ATT&CK라는 공개 매트릭스 기반의 일관적이고 최신화가 가능한 0에서 1사이의 점수

Table 1. Technique was mapped using BRON for randomly selected CVE, and then Technique was mapped to Group, Mitigation, Tactic, Asset(impact type) by MITRE ATT&CK.

	CVE	Technique	Group	Mitigation	Tactic	Asset
webserver	CVE-2022-31813	T1557.002	G0003 G1014	M1042 M1041 M1037 M1035 M1031 M1017	collection credential access	-
		T1584.002	-	M1056	resource development	-
		T1491	-	M1053	impact	integrity
		T1211	G0007	M1048 M1050 M1019 M1051	defense evasion	-
		T1542.002	G0020	M1051	defense evasion persistence	-
		T1556	-	M1047 M1032 M1028 M1027 M1026 M1025 M1022 M1024 M1018	credential access defense evasion persistence	-
fileserver	CVE-2014-6278	T1027.006	G0016	M1047 M1037 M1028 M1027 M1026 M1025 M1022 M1024 M1018	defense evasion	-
		T1027.009	-	M1049 M1040	defense evasion	-
		T1564.009	-	M1013	defense evasion	-
workstation	CVE-2023-20854	T1548	-	M1047 M1038 M1028 M1026 M1022 M1052	defense evasion privilege escalation	-

를 구하는 것이다. 따라서 네트워크 관점에서는 자산이 많을수록, 자산의 관점에서는 취약점이 많고 취약점에 매핑되는 위협 기술이 많을수록 점수가 높게 측정된다. 이는 보안의 맥락 상 이해하기에 매우 직관적이며 타 네트워크와 비교에 있어서 적합하다.

IV. 지표의 활용

제안하는 보안지표는 학교, 기업, 군 등 대규모 인프라에 적용할 수 있다. 먼저 각 기관에서는 보안을 측정할 자산을 정의해야한다. 정보를 보호할 호스트인 서버나 프린트기와 같은 장비를 식별하고 자산의 경계를 설정한다. 그리고 취약점 스캐닝 도구, 모의 침투 테스트를 함으로써 CVE를 도출한다. 취약점 CVE는 CWE, CAPEC 연결관계에 의해 MITRE ATT&CK의 Techniques 정보를 얻을 수 있다. MITRE ATT&CK는 Techniques에 대응하는 Mitigations, Groups, Tactic 을 함께 제공하기 때문에 제안하는 보안 공식에 대입할 변수는 모두 구하였다. 마지막으로 식 (1)을 이용하여 보안 위험도를 정량적으로 산출할 수 있다. 일반적으로 많이 사용되는 CVSS는 자산의 취약점에 초점을 두어 위험성을 나타내는데, 제안하는 지표는 사이버 보안에서의 위험을 다차원적으로 고려하기 위해 보안 개념과 그 관계를 파악하였기 때문에 위험 관리에 있어서 다각도의 시선이 포함된 수치를 확인할 수 있다.

V. 결 론

우리가 제안하는 지표는 ATT&CK를 기반으로 공격자 그룹의 수, 방어 기술의 수, 전술의 수가 정해져 있고 모두에게 공개되어 있다. 이는 일관성을 제공할 뿐만아니라 ATT&CK 버전 업데이트에 따라, 지표 또한 최신화가 가능하다. 추가적으로 우리는 자산에 대한 중요도를 지표에 포함하였다. 정보자산에 대해서는 보안의 중요한 3요소인 기밀성, 무결성, 가용성을 바탕으로 산정할 수 있다. Marcus 등 [7]이 제시한 보안 수준의 측정을 위한 지표의 기준에서와 같이, 본 논문에서 제안하는 지표는 보안의 관점에서 위험관리에 대한 개념 및 관계도를 참고하여 직관적으로 지표의 항목을 구성하고 수치로써 정량화하였다. 또한 ATT&CK 기반으로 일관성을 가지고 누구에게나 명확한 기준을 설정하였으므로 서로 다른 시스템 간의 비교가 가능하다. 향후 연구로는 CVSS 뿐만 아니라 다양한 보안지표들을 같은 대상의 인프라를 두고 값을 산출하여 비교 분석해본다면, 위험관리에 있어서 각 지표들의 특징과 장단점을 더 명확하게 파악할 수 있을것이라 예상한다.

본 논문에서 제시하는 보안지표는 MITRE ATT&CK를 기준으로 발견한 취약점과 대응하는 기술에 대해 매핑된 방어 기술이 적을수록, 공격 그룹이 많을수록, 전술단계의 후반에 있는 기술일수록, Impact 전술에 속하여 자산의 기밀성, 무결성, 가용성에 영향을 미치는 기술일수록 점수가 높게 측정되므로 분석한 네트워크에 대한 값이 크면 위험하게 나오도록 구성하였고, 이를 이용하여 보안 전문가가 다양한 보안지표 중 하나로 선택할 수 있는 폭을 넓히고, 기업이나 학교 네트워크의 보안을 강화할 것으로 기대한다.

References

[1] The MITRE Corporation, “MITRE ATT&CK.” [Online]. Available: https://attack.mitre.org, 2023.10

[2] Ahn, G., Lee, S. A., & Park, W. H. (2021, October). Changes of Cyber Hacking Attack Aspect of North Korea Cyber-Attack Groups Applying MITRE ATT&CK. Research Briefs on Information and Communication Technology Evolution, 7, 75-88.

[3] Pirca, A. M., & Lallie, H. S. (2023, April). An empirical evaluation of the effectiveness of attack graphs and MITRE ATT&CK matrices in aiding cyber attack perception amongst decision-makers. Computers & Security, 130, 103254.

[4] Ahmed, M., Panda, S., Xenakis, C., & Panaousis, E. (2022, A ugust). MITRE ATT&CK-driven cyber risk assessment. In Proceedings of the 17th International Conference on Availability, Reliability and Security (pp. 1-10).

[5] [Kwon, R., Ashley, T., Castleberry, J., Mckenzie, P., & Gourisetti, S. N.

G. (2020, October). Cyber threat dictionary using mitre att&ck matrix and nist cybersecurity framework mapping. In 2020 Resilience Week (RWS) (pp. 106-112). IEEE.

〔6〕 Singhal, A., & Ou, X. (2009, April). Techniques for enterprise network security metrics. In Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies (pp. 1-4).

〔7〕 Pendleton, M., Garcia-Lebron, R., Cho, J. H., & Xu, S. (2016, December). A survey on systems security metrics. ACM Computing Surveys (CSUR), 49(4), 1-35.

〔8〕 Doynikova, E., Fedorchenko, A., & Kotenko, I. (2019, August). Ontology of metrics for cyber security assessment. In Proceedings of the 14th International Conference on Availability, Reliability and Security (pp. 1-8).

〔9〕 F. of Incident Response and S. Teams, "CVSS." [Online]. Available: https://www.first.org/cvss, 2023.10.15

〔10〕 National Institute of Standards and Technology, [Online]. Available: https://nvd.nist.gov/, 2023.10

〔11〕 Spring, J., Hatleback, E., Householder, A., Manion, A., & Shick, D. (2021, Match). Time to Change the CVSS?. IEEE Security & Privacy, 19(2), 74-78.

〔12〕 Hemberg, E., Kelly, J., Shlapentokh-Rothman, M., Reinstadler, B., Xu, K., Rutar, N., & O'Reilly, U.M. (2020, October). Linking threat tactics, techniques, and patterns with defensive weaknesses, vulnerabilities and affected platform configurations for cyber hunting. arXiv preprint arXiv:2010.00533.

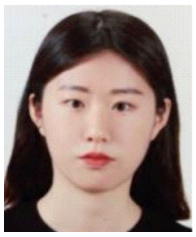
〔13〕 https://aag-it.com/the-latest-cyber-crime-statistics/, 2023.08, Charles Griffiths

〔14〕 https://www.concert.or.kr/bbs/board.php?bo_table=newsletter&wr_id=515&page=3, 2023.01, CONSERT (CONsortium of CERT)

〔15〕 International Organization for Standardization. (2005). Information Technology: Security Techniques: Evaluation Criteria for IT Security: Part 1: Introduction and General Model. International Organization for Standardization.

〔16〕 Ou, X., Govindavajhala, S., & Appel, A. W. (2005, August). MulVAL: A logic-based network security analyzer. In USENIX security symposium (Vol. 8, pp. 113-128)

〈저자소개〉



김 해 린 (Haerin Kim) 정회원
2021년 2월: 세종대학교 지능기전공학부 졸업
2023년 2월: 고려대학교 대학원 정보보안학과 석사
2023년 1월~현재: LIG넥스원 연구원
〈관심분야〉 data-driven security, 사이버전 훈련

이 승 운 (Seungwoon Lee) 정회원
2015년 2월: 아주대학교 정보컴퓨터공학부 졸업
2017년 2월: 아주대학교 소프트웨어학 석사
2022년 2월: 아주대학교 컴퓨터공학 및 보안 박사
2022년 1월~현재: LIG넥스원 선임연구원
〈관심분야〉 사이버보안 훈련, 사이버 전투모의

홍 수 연 (Su-Youn Hong) 정회원
2002년 2월: KAIST 전기 및 전자공학과 졸업
2004년 2월: KAIST 전기 및 전자공학과 석사
2013년 2월: KAIST 전기 및 전자공학과 박사
2013년 3월~현재: LIG넥스원 수석연구원
〈관심분야〉 사이버 보안 교육 훈련, 사이버 위협 및 방어 행위 자동화