디지털산업정보학회 논문지 제16권 제1호-2020년 3월
http://dx.doi.org/10.17662/ksdim.2020.16.1.079

공격 그래프 기반의 공격 대상 예측 시스템 설계 및 구현에 대한 연구*

고 장 혁** · 이 동 호***

A Study on the Design and Implementation of System for Predicting Attack Target Based on Attack Graph

Kauh Janghyuk · Lee Dongho

〈Abstract〉

As the number of systems increases and the network size increases, automated attack prediction systems are urgently needed to respond to cyber attacks. In this study, we developed four types of information gathering sensors for collecting asset and vulnerability information, and developed technology to automatically generate attack graphs and predict attack targets. To improve performance, the attack graph generation method is divided into the reachability calculation process and the vulnerability assignment process. It always keeps up to date by starting calculations whenever asset and vulnerability information changes. In order to improve the accuracy of the attack target prediction, the degree of asset risk and the degree of asset reference are reflected. We refer to CVSS(Common Vulnerability Scoring System) for asset risk, and Google's PageRank algorithm for asset reference. The results of attack target prediction is displayed on the web screen and CyCOP(Cyber Common Operation Picture) to help both analysts and decision makers.

Key Words : Cyber, Security, Attack Graph, Attack Path, Cyber Situation Awareness, COP, Cyber Decision Making

Ⅰ. 서론

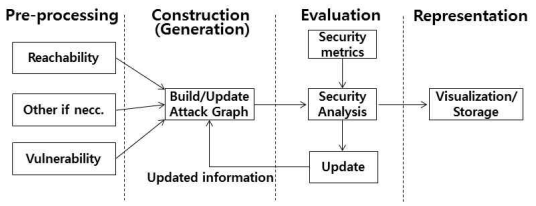
최근 IT 기술의 발전으로 보안 관리하여야 하는 시스템과 네트워크 장비의 규모는 기하급수적으로 늘어나고 사이버 공격이 증가함에 따라 기업 및 각 기관에서는 사이버 공격을 대비하고 정보자산을 지키기 위해 다양한 보안 시스템을 설치 및 운영하며 해킹 등과 같은 사이버 공격에 안전한 네트워크를 구성하기 위해 어느 시기보다 사이버 방어 상황인식(CDSA, Cyber Defense Situation Awareness) 능력이 요구되는 시기가 되었다[1-3].

하지만, 지속적으로 발전하는 사이버 공격 앞에서 보안 전문가들도 네트워크의 안전을 확신하지 못하고 있고 빠르게 늘어가는 최신의 취약점들을 모두 파악하지 못하고 있다. 조직의 내·외부에서 어떤 취약

* 이 논문은 2018년도 광운대학교 연구년에 의하여 연구되었음
** 국방과학연구소 책임 연구원
*** 광운대학교 컴퓨터소프트웨어학부 교수

점과 경로를 통해 사이버 공격이 일어날 수 있는지 확신하지 못하고 있다. 공격 그래프(Attack Graph)는 이러한 문제점을 해결하기 위해 조직의 네트워크 환경 및 취약점을 분석하여 공격자가 네트워크상에서 어떤 경로 조직의 핵심 정보자산에 도달할 수 있는지에 대한 공격 경로를 보여주기 위한 기법이다. 이를 통해서, 조직의 보안 담당자는 사이버 공격을 방어하기 위해 네트워크상의 어떤 부분에 우선적으로 집중해야 하는지 확인할 수 있다. 이렇게 네트워크 시스템이 방대하게 증가하여 복잡해짐에 따라 공격 그래프를 효율적으로 빠르게 생성해야 하는 문제점이 발생하였다. 이를 해결하기 위해서 가장 높은 확률로 예상되는 최적 공격 경로를 찾는 방법을 연구하여야 할 필요가 있다. 지금까지 공격 그래프에 관한 연구가 많이 진행되었지만 실제 공격자의 공격 경로를 예측하는 시스템의 자동화와 보안 업무에 사용할 수 있는 수준의 공격 그래프 연구는 많지 않았다. 따라서 본 연구에서는 자산, 취약점, 외부 보안정보의 수집을 최대한 자동화하고, 자산의 중요도와 참조도를 이용하여 자산의 위험도 지표를 수립하고, 공격 그래프를 통하여 공격 경로를 자동으로 예측하는 모델을 설계하고 프로토타입 시스템을 구현하였다. 또한 디바이스가 수시로 생성, 변경, 제거되는 네트워크 환경을 고려하여, 이를 빠르게 탐지하고 공격 그래프를 업데이트 할 수 있는 기술을 연구하였다. 공격 대상 예측 시스템의 프로토타입 시스템으로 웹 인터페이스는 물론이고, 사이버 공통상황도(CyCOP, Cyber Common Operation Picture) 인터페이스를 통해 조직의 지휘 결심자가 사이버 보안 상황에 대해 효율적이고 정확히 판단할 수 있도록 가시화를 통해 정보를 제공하는 기술을 개발하였다.

2장에서는 먼저 공격 그래프에 대한 기존 연구들의 특징 및 장단점을 간략하게 소개하고 3장에서는 공격 대상 예측 시스템의 정보 수집, 공격 그래프 생성, 공격 그래프 분석을 통해 공격 경로 및 대상을 예측하는 기술에 대해 설명하고 4장에서는 시험을 위한 모의 환경과 시험 결과에 대해 설명하며 5장에서는 결론으로 공격 대상 예측 기법의 성능을 높이기 위해 나아가야 할 방향과 추가 연구 필요성에 대해 기술한다.



<그림 1> 기능 구성도

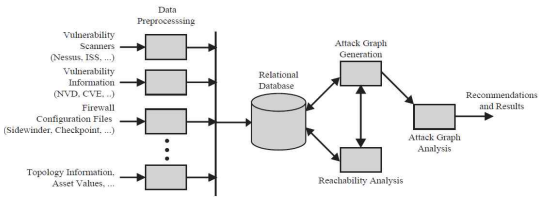
II. 기존 연구

공격 그래프를 이용한 예측시스템은 일반적으로 <그림 1>과 같은 구성을 이룬다. 전처리(Pre-processing) 단계에서는 공격 그래프를 생성하기 위한 데이터를 준비하는 단계로 공격 그래프 기법에 따라 다르지만, 일반적으로 자산 정보, 네트워크 토폴로지 정보를 이용한 접근 가능(Reachability) 정보, 그리고 취약점(Vulnerability) 정보를 수집 및 전처리한다. 이렇게 생성된 데이터를 이용하여 생성(Construction) 단계에서는 공격 그래프를 생성한다. 평가(Evaluation)단계에서는 이렇게 생성된 공격 그래프에 보안에 대한 평가 요소를 추가하여 보안 분석을 위한 그래프를 추가 생성한다. 표현(Representation) 단계에서는 이렇게 생성된 공격 그래프와 보안 분석 정보를 표현하는 단계로 인터페이스는 웹의 형태가 일반적이고 상황인식 능력을 공유하기 위해 공통상황도를 통해 표현하기도 한다[4].

공격 그래프 생성기법으로 널리 알려진 기법은 NetSPA[5-7], TVA[5, 8, 9], MulVAL[10] 등이 있다.

MIT Lincoln Lab에서 개발한 NetSPA (NETwork

Security and Planning Architecture)는 방화벽 규칙과 취약점을 분석하여 공격 그래프를 생성한다. NetSPA는 내부 또는 외부 공격자가 내부 호스트를 타켓으로 취약한 호스트를 공격할 수 있는 여러 방법을 도출하는 도구이다. 이를 통해, 공격 그래프는 공격자를 나타내는 root node를 시작점으로 하고, 링크를 통해 공격자가 악용할 수 있는 취약점의 특정 인스턴스(instance)가 표현된다.



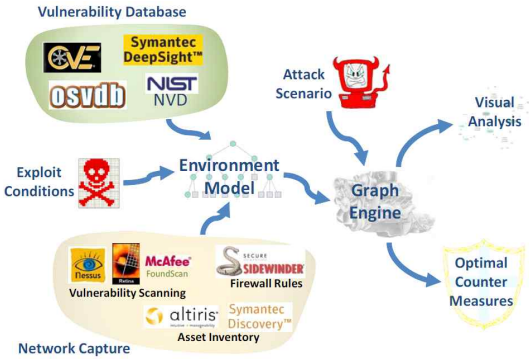
<그림 2> NetSPA System Block Diagram[6]

<그림 2>와 같이 NetSPA의 블록다이어그램은 여러 도구를 이용하여 자동으로 데이터베이스를 가져오는 기능으로 사용되었다.

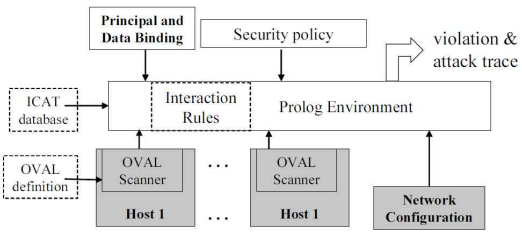
- Vulnerability scans : Nessus와 같은 도구로 네트워크의 취약점, 호스트 정보, open port 확인
- Vulnerability database : NVD에서 제공하는 취약점 데이터베이스 참고하여 확인
- Firewall rules : Sidewinder와 같은 rule sets을 통해 traffic이 해당 네트워크의 filtering장치를 통하는지 아닌지 확인
- Topology information : vulnerability scans으로부터 호스트와 firewall 연결을 확인

위의 정보들을 통해서 접근가능 정보가 자동으로 계산되어 공격 그래프가 생성되며 recommendation과 result가 나오게 된다.

TVA는 조지 메이슨 대학에서 초기 공격 그래프 연구의 확장성(Scalability) 및 성능에 초점을 맞추어 개발된 공격 그래프 기법이다. 그림에서 보는 바와 같이 취약점 데이터베이스, 네트워크 캡쳐, Exploit 조건, 등의 분야에서 상용제품을 최대한 활용하여 구축되었다. TVA기법은 계속 발전되어 MITRE CyCraph에도 적용되어 MITRE CDSA 솔루션 발전에 기여하였다.



<그림 3> Toplogical Vulnerability Analysis(TVA)[8]



<그림 4> The MulVAL framework[10]

MulVAL(Multihost, multistage, Vulnerability Analysis)은 캔사스 대학에서 개발되었고 <그림 4>에서 보는 바와 같이 Prolog 와 같은 logic-programming 기반의 공격 그래프 분석 방법이다. OVAL(Open Vulnerability Assessment Language)을 지원하는 취약점 스캐너 결과와 자산 및 네트워크의 토폴로지 정보(Routing rules, Access policies, NAT policies, Available services, Device configurations, Safeguard configurations, Host configurations)를 이용하여 공격 그래프를 생성한다.

네트워크 토폴로지 정보는 Datalog형태로 작성되며, OVAL문법의 취약점 스캐너 결과도 Datalog형태

로 변환되어 공격그래프를 생성한다. MulVAL은 DRDC(Defence Research and Development Canada)의 사이버상황인식 체계개발 프로젝트인 AMOUR[4] 프로젝트에도 활용되었다.

<표 1>은 앞서 설명한 대표적인 공격그래프 기법들의 특징을 기존 연구[5]를 참고하여 정리한 것이다.

<표 1> 공격 그래프들의 특징

	MulVAL		TVA		NetSPA	
Data Source	Advisory	NVD / Nessus	Vulnerability Database	NVD, OSVDB / Nessus Scan	Software Database	NVD / Nmap, Nessus
	Host Conf.	OVAL	Host Discovery	Altiris		Attack Loss Value
	Network Conf.	Smart firewall	Network Discovery	모든 구간에서 스캐닝 or 방화벽 정책	Network Model	Reachability Matrix
	Principal	공격자위치, Goal what-if	Attack Scenario	공격자위치, Goal what-if	Action Database	REM언어 Requirement Effect Modification
	Interaction	Interaction rule	Exploit Conditions	Pre-condition Post-Condition		
	Policy	정보별 접근 권한	-	-	Trust Relationship	
Attack Simulation	Reasoning Engine	Attack Simulation Trace	Graph Engine	Graph dependency 계산	Computation Engine	Depth-first Search
Graph Generation	Graph Builder	특이사항 없음	Visual Analysis	반복적 aggregation → Topology에 투영	Grapher	특이사항 없음

본 논문에서는 각 공격 그래프 기법들의 장단점을 <표 2>와 같이 분석하였고 이러한 점을 고려하여 새로운 공격 그래프 기법을 개발하였다.

<표 2> 공격 그래프 모델 비교

프로젝트	그래프 타입	입력데이터 다양성		Target Open		Complexity		그래프의 직관성	
MulVAL	Logical Attack graph	3	다양하고 논리적	1	불가능	1	O(N2) ~O(N3)	1	보통
TVA	Penetration dependency Graph	1	가장 적음	1	불가능	2	O(N2)	3	직관적 (Vertice가 host)
NetSPA	Multiple Prerequisite Graph	2	보통	3	가능	3	O(N lgN)	2	보통

III. 공격 대상 예측 시스템

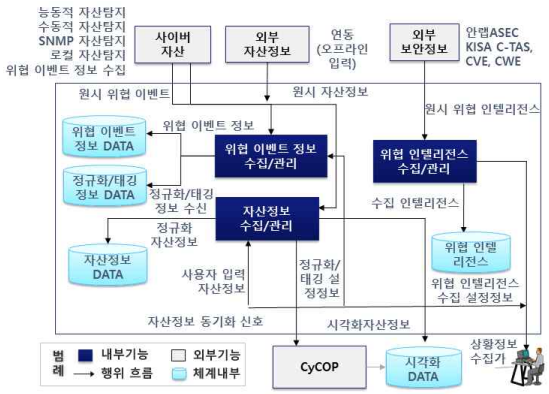
본 시스템은 취약점 정보, 네트워크 정보 및 애플리케이션 정보를 포함하는 자산 정보를 수집하는 정보 수집부, 자산 정보를 저장하고, 자산 정보에 대한 연관관계를 설정하여 자산 관계 그래프를 생성하고 자산 관계 그래프를 기반으로 도달 가능성 및 취약점을 판단하고, 도달 가능성 및 취약점을 이용하여 공격 그래프를 생성하는 공격 그래프 생성부, 공격 그래프를 기반으로 공격 경로를 탐색하고, 공격 경로 기반 공격 대상을 예측하는 공격 대상 분석부로 구성된다.

<그림 5> 공격 대상 예측 시스템 기능 구성도

3.1. 정보 수집 기술

정보 수집을 위한 기술 구성도는 <그림 6>과 같다.

사이버 자산 정보로는 자산정보, 자산의 공개 취약점 정보와 취약점 점검 결과 정보 등을 포함하는 취약점 정보, 그리고 자산의 네트워크 토폴로지, 접근 제어목록 정보 등을 포함하는 네트워크 정보와 자산에서 실행 가능한 응용 서비스 정보, 소유자 계정정보, 인증정보 등을 포함하는 애플리케이션 정보로 구성된다. 접근 제어목록 정보는 ACL(Access Control



<그림 6> 정보 수집부 기술 구성도

List) 설정정보일 수 있으며, 자산 접근과 관련된 권한 또는 정책에 대한 정보를 포함할 수 있으며 응용 서비스 정보는 응용 서비스의 명칭과 버전 등을 포함할 수 있다.

정보를 수집하기 위해 다음과 같은 4가지 종류의 센서를 활용하였다.

- 능동 자산수집센서(NMAP(Network Mapper))
- 수동 자산수집센서(BRO)
- SNMP(Simple Network Management Protocol)
- 로컬(윈도우, 리눅스) 자산수집센서

센서별로 수집된 정보가 상이한 경우를 대비하여 수집 자산에 대한 센서별 우선 순위는 "사용자 입력-로컬-SNMP-수동-능동" 센서 순으로 정의하였다. 센서에서 수집되는 정보는 <표 3>과 같다.

취약점 정보인 위협 이벤트정보는 호스트(윈도우, 리눅스)에 저장되는 로그, 네트워크 트래픽 로그(Bro), 그리고 보안 장비들(백신, EDR, IPS, 방화벽, 취약점 분석 스캐너(OpenVAS, Open Vulnerability Assessment System)) 로그를 수집하였으며 외부 보안정보는 연동을 통해 시스템에 입력되며 관리하는 외부 보안정보로는 AlienVault, X-Force(IBM), KISA(C-TAS), 안랩 위협정보, CVE, CPE 정보로 보안정보 기술에 사실상의 표준이라 할 수 있는 STIX

<표 3> 수집정보 항목

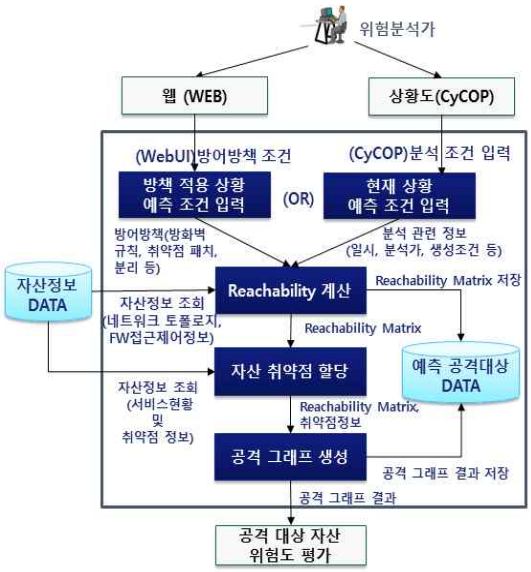
수집분류	수집항목	능동 (nmap)	수동 (bro)	SNMP	로컬
네트워크 주소	IP주소	O	O	O	O
	MAC 주소	O	O	O	O
	게이트웨이 주소			O	O
	서브넷 마스크			O	O
운영체제 정보	운영체제 명칭	O	O	O	O
	운영체제 버전	O	O	O	O
	패치정보				O
동작중인 응용서비스 정보	응용 서비스 명칭	O	O	O	
	응용 프로그램 명칭	O	O		O
	응용 프로그램 버전	O	O		O
	사용중인 포트번호	O	O		O
	사용자명				O
라우팅 테이블 정보	인터페이스 인덱스			O	
	목적지 IP 주소			O	
	다음 홉 IP 주소			O	
	넷마스크			O	
데이터 송수신량	데이터 수신량			O	
	데이터 송신량			O	

2.0 형식으로 관리함으로써 정보의 활용이 용이하도록 구현하였다. CVE 및 CPE는 RDB에 저장되고 나머지 4개의 연동 정보는 Graph DB에 저장하였다.

3.2. 공격 그래프 생성 기술

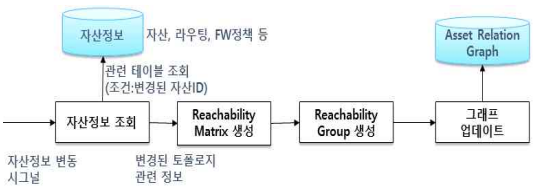
공격 그래프 생성 기술은 <그림 7>과 같이 웹 환경과 공통상황도상에 동시 구현되어 분석관 및 지휘관 모두를 지원하는 기술로 구현되었다. 주된 기능은 접근가능 정보 계산, 자산 취약점 할당, 그리고 공격 그래프 생성기능이다.

본 논문에서 제안하는 공격 그래프 생성 방법은 기존 연구들이 공격 그래프 생성을 위해 많은 데이터 처리 시간이 소비되고, 이러한 이슈로 공격 경로를 예측하는데 제한적으로 특정 위치에서 목적지까지만을 계산하는 점을 해결하기 위해 접근가능 정보를 계



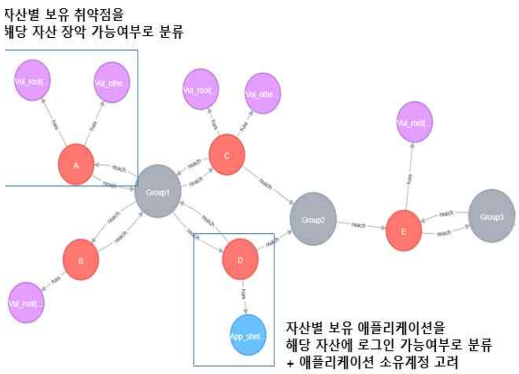
<그림 7> 공격 그래프 생성 프로세스

산하는 기능과 공격 그래프를 생성하는 기능을 분리하여 구현하였다. 이를 통해 공격 그래프 분석이 필요한 시점에는 미리 계산된 접근가능 정보를 이용해 공격 예측 경로를 예상할 수 있게 하였다.



<그림 8> 접근 가능 정보 생성

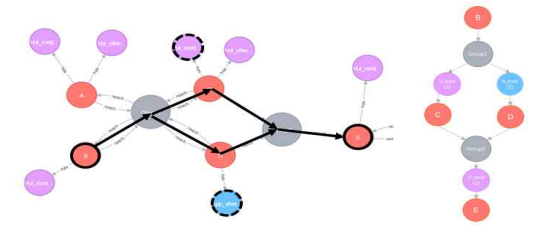
추가/변경된 자산정보(자산정보, 라우팅정보, FW정책)가 발생하면 변경된 자산에 대하여 토폴로지/라우팅정보/FW정책 등을 고려하여 나머지 N-1개의 자산과 통신 가능한지 여부를 계산하여 접근가능 정보 Matrix를 생성한다. 접근가능 정보 Matrix의 계산량을 줄이기 위해 NetSPA 기법에서도 적용되었던 그룹 개념을 적용하여 동일한 접근가능 정보를 가지는 자산들을 같은 그룹으로 구성해서 접근가능 정보를 계산하였다.



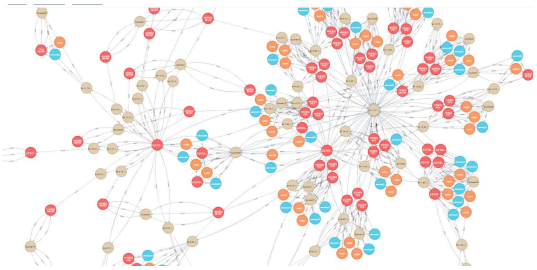
<그림 9> 자산 취약점 할당

자산 취약점 할당 기능은 자산정보가 변경될 때마다 해당 자산의 취약점 정보 및 사용 중인 어플리케이션 서비스 정보 및 권한 정보를 수집하여 공격 그래프를 업데이트한다. <그림 9>와 같이 취약점은 Vul_ 식별자로 어플리케이션 실행 권한 정보는 App_ 식별자로 정의해서 그래프에 추가하였다.

공격 그래프 생성 기능은 공격자의 위치/위협 상태를 고려하여 공격 그래프를 생성, 공격 가능 대상 자산을 식별할 수 있도록 개발되었다. <그림 10> (a)는 다음 접근가능 정보 그룹으로 가기 위해서는 경우 노드가 Vul_root 권한을 가지거나 App_shell을 수행할 수 있는 권한을 가지고 있어야 한다는 의미이다. 이러한 계산은 시스템 안에서는 백그라운드로 실행되며 실제 사용자에게는 (b)와 같은 결과만 보여 진다. 자산정보와 위협정보를 통한 공격 그래프는 최종적으로 2개의 경로가 존재함을 알 수 있다. 이렇게 생성된 공격 그래프를 보면서 공격자의 공격 경로를 예상하고 대비할 수 있다. (c)는 공격 그래프들이 그래프 DB인 Neo4j로 실제 저장/관리되는 것을 보여 준다.



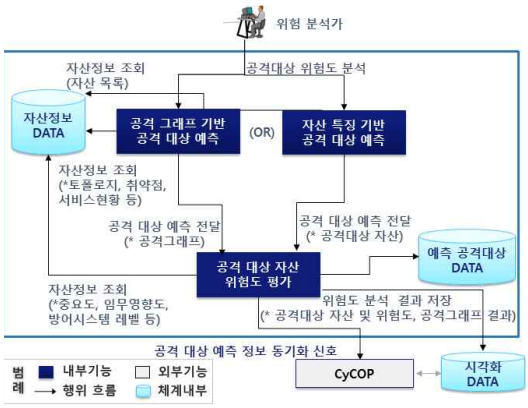
(a) 탐색 방식(백그라운드) (b) 그래프 결과



(c) 그래프 저장/관리 (Neo4j graph DB)

<그림 10> 공격 그래프

3.3. 공격 대상 분석 기술



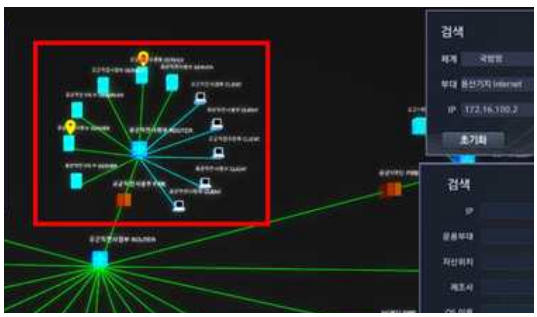
<그림 11> 공격대상 위험도 분석 기능

공격 그래프 생성 기능에서 자산정보와 위협정보를 이용하여 공격 그래프를 생성하였다. 하지만 자산 및 네트워크 규모가 증가함에 따라 공격 경로의 수도 증가하며 경로가 많으면 공격자의 공격을 대비하기 힘들다. 이 문제를 해결하기 위해 <그림 11>과 같이 자산 특징 기반 공격 대상 예측기능과 공격 그래프 기반 공격 대상 예측 기능을 개발하였고 각 기능은 공격 대상 자산 위험도 평가를 통해 보다 정확한 공격 대상을 예측할 수 있다.

자산 특징 기반 공격 대상 예측기능은 동일 취약점, 운영체제, SW 등 다양한 속성 조건을 이용하여 전체 또는 범위가 지정된 네트워크 내에서 공격 가능 자산을 식별하고 도시할 수 있다. 검색조건으로는 자산의 IP, 운용 조직, 설치 장소, 제조사, 등 다양하게 검색 가능하다.

<그림 12>의 (a)는 웹에서 자산 특징 기반 공격 대상을 예측한 결과로 웹 목록의 형태로 보이며 상세 정보를 선택하면 자세한 정보를 열람할 수 있으며 공격 그래프 예측을 선택하면 상황도 상에 (b)와 같은 결과를 볼 수 있다. 상황도에서는 자산 특징 검색 결과를 잘 식별할 수 있도록 검색된 자산 위에 추가적인 표식을 표시한다.

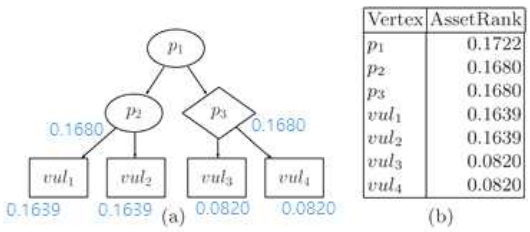
(a) 웹 상의 검색 결과



(b) 상황도 상의 검색 결과

<그림 12> 자산 특징 기반 공격 대상 예측 기능

공격자의 공격대상을 정확히 식별하기 위해서는 조직내 자산의 위험도 및 예산 피해를 정량적 제시하여 그 결과를 공격 그래프에 반영하여야 보다 정확한 공격 그래프가 생성될 수 있다. 본 논문에서는 자산의 중요도와 자산의 참조 정도를 이용하여 자산의 위험도를 산정하였다.



Vertex	AssetRank
p_1	0.1722
p_2	0.1680
p_3	0.1680
vul_1	0.1639
vul_2	0.1639
vul_3	0.0820
vul_4	0.0820

공격자능력 /획득한 권한 자산의 중요도

$$X = (D\Delta + \gamma P e^T)X$$

<그림 13> 자산 참조 알고리즘

자산의 참조 정도는 구글의 PageRank 알고리즘을 적용하여 참조하는 횟수를 수치화하는 방식으로 <그림 13>과 같이 자산의 위험도를 계산하였다. 이와 같은 연구는 ARMOUR 프로젝트[10]에서도 적용된 바가 있다.

서버, 네트워크 장비, 보안장비에 대해 중요도 평가를 수행하며 자산의 평가 등급 및 평가 점수 적용 방안으로 자산의 기밀성, 무결성, 가용성 평가점수는 CVSS 평가 항목 중 보안 요구도 항목으로 적용하며 자산의 중요도는 다음과 같다.

자산의 중요도 = 기밀성 + 무결성 + 가용성 + 과업 중요도 + 임무 중요도

자산피해산정은 CVSS(Common Vulnerability Scoring System) 계산식 적용하여 알려진 취약점에 대해 취약점 점수를 판별할 수 있게 구현하였으며 CVSS는 기준 점수, 임시 점수, 환경 점수 3가지로 구성되어 있다. CVSS 2.0과 3.0 모두 사용하였으며 CVSS 2.0은 모든 CVE(취약점 목록)에 대해 제공되며, CVSS 3.0은 CVE-2015-XXXX부터 제공된다.

자산의 중요도 평가 기준은 <표 4>와 같으며 경험을 바탕으로 기밀성, 무결성, 가용성을 기준으로 각 속성들의 가치는 동일하며, 자산 특성에 따라 불필요한 속성은 제외하고 평가요소 가중치를 정의하였다.

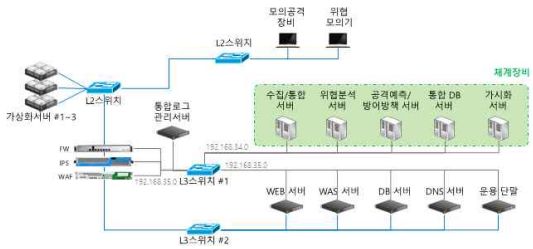
<표 4> 자산 중요도 평가 기준

자산 구분	평가 구분	평가요소	평가요소 가중치
서버 (DB 서버, 응용서버, 웹서버 등)	기밀성	자산정보 유출시 임무 등에 대한 위험 초래 정도	0.5
		각 자산이 포함하는 비밀 정보의 량	0.5
	무결성	자산 정보의 변조에 따른 임무, 서비스 수행에 대한 장애 유발 가능 정도	0.5
		자산 정보의 변조시, 원래 정보를 회복할 수 있는 정도	0.5
	가용성	해당 자산의 사용이 불가할 때, 대체(백업) 자산이 없어 임무, 서비스 수행 등이 불가능 한 정도.(24시간이상, 1~24시간, 1시간 미만)	0.25
		자산과 관련된 임무의 중요도(상, 중, 하)	0.25
		자산의 일일 세션 수	0.25
		자산을 이용한 통신 데이터량	0.25
네트워크 장비	가용성	해당 자산의 이용이 불가할 때, 임무, 서비스에 미치는 영향(24시간이상, 1~24시간, 1시간 미만)	1
보안장비 (IDS, IPS, 등)	무결성	자산 정보의 변조에 따른 임무 수행의 민감도	0.5
		자산 정보의 변조에 따라, 데이터의 무결성 검증이 어려운 정도	0.5
	가용성	해당 자산의 이용이 불가할 때, 임무, 서비스에 미치는 영향	1

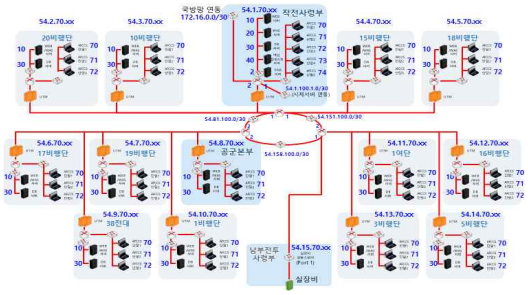
IV. 시험환경 및 결과

4.1 시험환경

시험 환경은 <그림 14>와 같이 체계 운용 장비와 모의 환경 장비로 구성된다.



(a) 운용 장비



(b) 모의환경 (100 노드이상)

<그림 14> 시험 환경

체계 장비로는 <표 5> 같이 응용서버 4대와 상황도 가시화를 위한 서버 1대로 구성된다. 본 연구의 프로토타입에서는 분석관을 위한 웹 체계와 지휘 결심자를 위한 공통상황도를 모두 지원하고 있다.

<표 5> 시스템 사양

용도	장비	사양
수집/통합 서버	HP DL60 Gen9	intel Xeon 2.4GHz, 2 CPU/ 128GB RAM
위협분석 서버	HP DL60 Gen9	
공격예측 서버	HP DL60 Gen9	
통합 DB 서버	HP DL60 Gen9	
가시화 서버	HP Z4 G4	intel Xeon 4.0GHz CPU/ 64GB RAM/914GB HDD

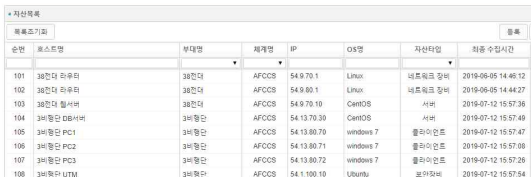
모의 환경은 <그림 14>의 (b)와 같이 군 C4I체계를 모의하였으며 <표 6>과 같이 실장비와 가상화 장비를 혼합해서 구축하였다. 단말, 서버, 네트워크, 정보보호 장비들로 구성되며 시험을 위한 트래픽 발생 및 위협모의 장비들을 사용하였다. 위협 모의기에서 VNC 세션 및 Telnet 세션 등을 활용하여 모의공격 장비에 접속, 모의공격 진행을 진행하고 사용자 행위를 캡쳐하며 공격 시나리오 단계에 따라 다양한 Test Case 작성 및 수행하였다.

<표 6> 모의 환경 장비(HW, SW)

	용도	제조사 및 모델명
HW	모의공격 장비	Dell XPS 15
	위협모의기	Dell XPS 15
	통합시연 장비	Dell XPS 15
	가상화 서버	Dell PowerEdge R720
	스토리지	Dell EqualLogic
	방화벽	Sniper AF2000
	웹방화벽	WEB INSIGHT SG
	침입방지시스템	Sniper IPS V8.5 NE1000
	통합로그관리 서버	nLM(netcruz Log Manager)
SW	위협모의기 SW	Spirent iTest
	가상화 솔루션	VMware vCenter x1, vSphere x6, NSX x6
	통합로그관리 SW	nLM LogSee v3.0
	백신	Hauri
	엔드포인트 탐지/대응(EDR)	Wazuh, Somma Monster
	위협 에뮬레이션 SW	위협이벤트 정보 수집 및 재현

4.2 시험 결과

정보 수집부에서는 자산정보, 위협정보 및 위협 인텔리전스 정보를 수집하며, 자산정보는 4개의 센서로부터 수집되며 <그림 15>와 같이 관리된다. 사용자 편의를 위해 CSV 파일형태로 import할 수도 있게 개발되었다.



<그림 15> 자산정보 관리

이렇게 수집된 자산정보는 다양한 검색 기술을 제공하며 공격 그래프 생성 및 자산 특징 기반 공격 대상 예측 기능에도 활용된다. 통신장비 및 시스템의 접근제어목록(ACL)과 라우팅 정보도 편의를 위해 CSV 형태로 import할 수 있게 개발되었다. 입력된 정보는 웹에서 추가, 수정, 삭제가 가능하다.

<그림 16> 위협정보 관리

위협정보는 <그림 16>과 같이 시스템 및 통신장비와 정보보호 장비들에서 탐지한 이벤트 로그 형태로 수집 및 관리된다. 각 로그들은 syslog 프로토콜을 이용하여 수집되지만 각 로그의 형태들이 상이하기 때문에 파서를 이용하여 필요한 정보 항목들을 분리/추출하여 관리한다.

외부 인텔리전스 정보는 <그림 17>과 같이 외부 연동을 통해 수집되며 수집되는 정보는 앞서 설명한 바와 같이 KISA(C-TAS), 안랩 위협정보, CVE, CPE 정보로 <그림 17>과 같이 STIX 2.0 형식으로 관리한다.

(a) 외부 인텔리전스 정보 연동

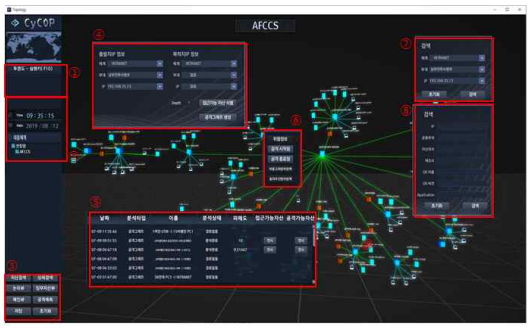
(b) 외부 인텔리전스 정보 관리

<그림 17> 외부 인텔리전스 정보 수집 및 관리 화면

공격 그래프 생성부와 분석부의 결과는 <그림 18>과 같이 지휘 결심자를 지원하기 위해 상황도에서도 운용되며 분석관을 위해 웹으로도 운영된다. 먼저 상황도의 운용 화면 및 기능은 <그림 18>과 같다.

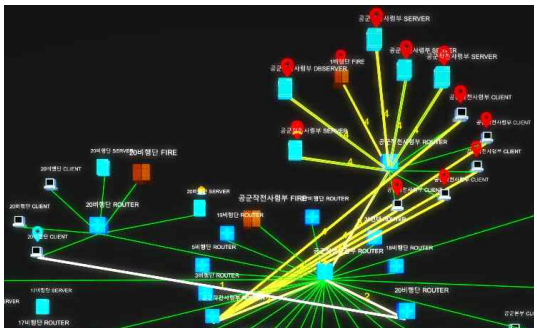
<그림 18> 좌편의 ①, ②, ③은 고정으로 도시되며 나머지 기능은 필요에 따라 도시 여부를 선택할 수 있으며 이동도 가능하다. 공격 예측 지정 메뉴를 통해 공격의 출발지와 목적지 IP를 설정하고 공격 그래프 분석 종류를 선택하면(<그림 18> ④) 수행 후 공격 예측 결과 목록(<그림 18> ⑤)에 게시된다. 보안분석관 및 지휘 결심자는 목록에서 다양한 공격 예측 결과를 클릭함으로써 사이버 상황도에 도시하면서 그 결과를 확인할 수 있다.

기본적으로는 출발지와 목적지 IP를 입력하게 되어 있으나 출발지나 목적지의 IP를 네트워크 대역이나 전체 네트워크로 설정해서 공격 그래프를 생성할 수도 있다. 이런 경우에는 네트워크 Depth (=Hop) 크기에 따라 계산에 소비되는 시간이 급수적으로 증가하는데 본 연구에서는 이러한 이슈를 해결하기 위해 기존 공격 그래프 생성 기법들과는 다르게 접근가능 정보 계산과 공격 그래프 생성 기능을 분리하여 접근가능 정보 Matrix를 미리 계산해 놓고 네트워크 및 접속 권한 정보가 변경할 때마다 자동으로 재계산되게 함으로써 처리 시간을 단축시켰다.

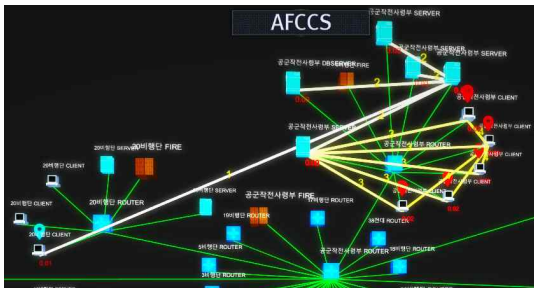


순번	내용	설명	비고
①	투명도	상세뷰 투명도 처리 버튼	
②	시간 및 체계	현재 날자 및 시간 전시	
③	메뉴	검색 및 공격예측 버튼	
④	공격예측 지정	공격예측 출발지 IP, 목적지 IP 선택	
⑤	공격예측	공격 예측 결과 및 공격 예측 결과 검색	
⑥	공격 및 방어방책	공격 시작점, 공격 종료점 및 방어방책 버튼	
⑦	검색	체계, 부대, IP 자산 검색	1~5
⑧	상세 검색	IP, 부대, 제조사 등 상세 검색	

<그림 18> 공격 대상 예측 시스템 (공통상황도)



(a) 접근 가능 경로



(b) 공격 가능 대상 (공격 경로)

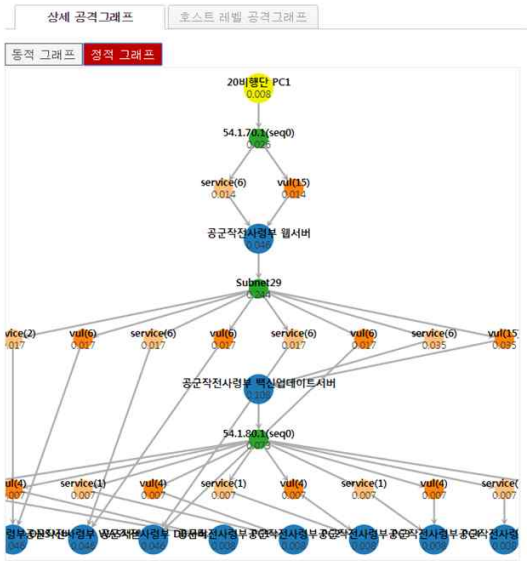
<그림 19> 공격 그래프 생성 기능

<그림 19> 출발지와 목적지 IP를 동일하게 입력했을 때 네트워크 정보와 ACL정보를 기반으로한 접근 가능 경로와 이런 정보에 자산 및 응용서비스 등의 취약점 정보를 반영하여 생성한 공격 가능 대상 그래프 생성 결과 화면이다. 출발지에서 목적지까지는 선위에 Hop 숫자가 표시되어 있다.

보안 분석관은 사이버 상황도를 보면서 분석을 할 수도 있지만 보다 상세한 정보를 필요로 하는 경우가 많다. <그림 20>은 이러한 경우를 해결하기 위해 웹으로 지원하는 공격그래프 생성 결과로 공통상황도에는 자산만을 노드로 표시하고 그래프로 네트워크를 도시한다면 웹에서는 자산의 취약점과 자산에서 운용되는 응용서비스의 취약점은 물론 자산 위험도까지 포함된 공격 그래프를 지원한다. 또한 분석을 용이하게 하기 위해 각 노드들에 대한 상세한 정보도 <그림 21>와 같이 동시에 제공하게 개발하였다. 노드의 종류는 자산, 접근가능성, 응용서비스, 취약점으로 앞서 설명한 자산 중요도와 참조도로 자산의 공격 위험도를 계산하여 표시하였으며 분석 중 What-IF 분석을 위해 조건을 변경하여 다시 공격 그래프를 생성할 수 있으며 "자산 특징" 버튼을 클릭함으로써 <그림 12> (a)와 같이 네트워크 내 자산 특징으로 장비를 검색할 수 있다.

<그림 22>와 같이 공격 그래프에 필터링 기능을 적용하여 호스트 레벨 정보만을 볼 수도 있다. 이렇게 하면 앞서 상황도에서 보았던 공격 그래프와 유사하게 취약점보다는 공격 대상이 되는 장비들이 잘 보이게 된다.

공격 대상을 예측하기 위해 본 연구에서는 2종류의 공격 대상을 예측하는 기능을 제시하였다. 한 가지는 앞서 설명한 <그림 12>와 같은 데이터베이스 검색을 통한 정보 검색 및 상황도 도시를 하는 자산 특징 기반 공격 대상 예측 기능이고 체계의 활용성 및 편의성을 높이기 위해서이고, 다른 한 가지는 <그림 23>와 같은 공격 그래프 기반 공격 대상 예측

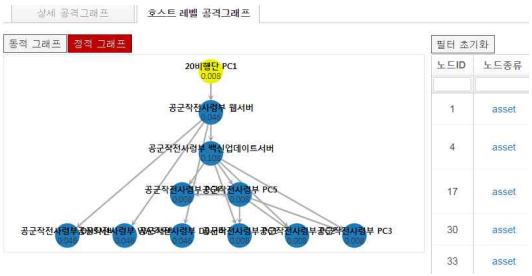


<그림 20> 공격 그래프 (웹)

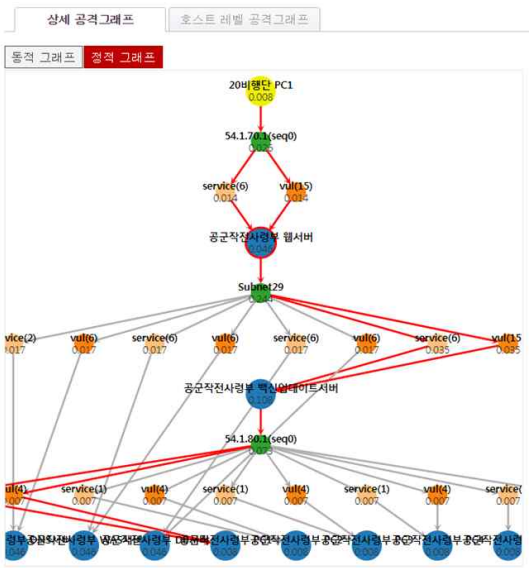
노드ID	노드종류	노드속성	위험도	depth	추가분석
1	asset	node_name : 20비행단 PC1 ip_addr : 54.2.80.70	0.008	1	자산상세
2	reachability	node_name : 54.1.70.1(seq0)	0.026	2	What-IF
3	application	node_name : service(6) count : 6 app_name : FTP Daemon;MySQL;mysqld;proftpd;ssh ;sshd	0.014	3	What-IF
5	vulnerability	node_name : vul(15) count : 15 vul_id : CVE-2013-4391;CVE-2014-3539;CVE-2013-4394;CVE-2013-4327;CVE-2013-4392;CVE-2017-5651;CVE-2017-5648;CVE-2017-12617;CVE-2017-7675;CVE-2017-5647	0.014	3	What-IF
4	asset	node_name : 공군작전사령부 웹서버 ip_addr : 54.1.70.10	0.046	4	자산상세
6	reachability	node_name : Subnet29	0.244	5	What-IF

<그림 21> 그래프 노드 상세 정보(웹)

기능이다. 본 연구의 프로토타입 체계에서 <그림 23> 처럼 빨간 색으로 공격 그래프를 보여 주지는 않는다. 하지만 분석관은 공격 그래프에 나와 있는 공격의 방향과 노드마다 표시되는 자산의 위험도를 보면서 공격자의 공격 경로와 대상이 될 수 있는 장비를 식별할 수 있으며 <그림 21>과 같은 상세정보를 참조한다면 더욱 자세한 분석을 수행할 수 있다.



<그림 22> 호스트 레벨 공격그래프



<그림 23> 공격 그래프 기반의 공격 대상 분석 화면

V. 결론 및 향후 연구

시스템과 네트워크 장비의 규모가 기하급수적으로 늘어나고 지속적으로 발전하는 사이버 공격 앞에서 보안 전문가들도 네트워크의 안전을 확신하지 못하고 있고 빠르게 늘어가는 최신의 취약점들을 모두 파악하지 못하고 있다. 이런 상황에서 본 연구는 자산 및 취약점을 자동으로 수집하고, 수집된 정보로 공격자의 사이버 공격 경로 및 대상을 예측하는 기술을 제안하였으며 프로토타입을 통해 그 가능성을 보였다. 이러한 프로토타입 시스템은 보안 담당관과 사이

버 지휘 결심자의 신속한 분석 및 판단을 도와 사이버 방어 상황인식(Cyber Defense Situation Awareness) 능력 향상에 도움이 될 것으로 판단된다.

본 연구는 공격자의 사이버 공격이 있기 전에 미리 수집 자산 및 취약점을 이용해 정보자산의 오남용되고 있는 접근권한이나 미 조치된 취약점을 보안하기 위한 사전 활동(Proactive)에 이용되는 시스템이다.

향후 연구로는 본 연구에서 제안한 공격 그래프 기법을 취약점 대신 실시간 탐지한 이벤트 정보에 적용하고 실시간 처리를 고려한다면 사이버 공격에 대한 대응 활동(Reactive)에도 적용이 가능할 것으로 판단된다. 본 연구에서도 처리 성능을 향상시키기 위해 접근가능 정보 계산과 공격 그래프 생성 기능을 분리해서 개발한 것처럼 근 실시간 대응을 위해 수집 데이터의 전처리 및 병렬화 기능에 추가적인 연구가 필요하다. 본 연구에서도 접근가능 정보 Matrix를 활용했지만, 공격 그래프에서 참고하는 다른 데이터들을 Matrix 형태로 설계하고 Matrix 연산에 좋은 성능을 보이는 GPU를 적용한다면 높은 성능 향상이 있을 것으로 기대된다.

참고문헌

[1] 고장혁, 이동호, “네트워크 트래픽 수집 및 복원을 통한 내부자 행위 분석 프레임워크 연구,” 디지털산업정보학회 논문지, 제13권 제4호, 2017a, pp.125-139.

[2] 고장혁, 이동호, “정보 유출 탐지를 위한 머신 러닝 기반 내부자 행위 분석 연구,” 디지털산업정보학회 논문지, 제13권 제2호, 2017b, pp.1-11.

[3] 고장혁, 이동호, “국방정보시스템 성능향상을 위한 효율적인 GPU 적용방안 연구,” 디지털산업정보학회 논문지, 제11권 제1호, 2015, pp.27-35.

[4] N. Nakhla, K. Perrett and C. McKenzie, “Automated computer network defence using ARMOUR: Mission-oriented decision support and vulnerability mitigation,” 2017 International Conference On Cyber Situational Awareness, Data Analytics and Assessment(Cyber SA), Lodon, 2017, pp.1-8.

[5] Barik, M.ridul & Sengupta, Anirban & Mazumdar, Chandan, “Attack Graph Generation and Analysis Techniques,” Defence Science Journal. Vol, 66, No.6, 2016, pp.559-567.

[6] R. Lippmann et al., "Validating and Restoring Defense in Depth Using Attack Graphs," MILCOM 2006, IEEE Military Communications conference, Washington, DC, 2006, pp. 1-10.

[7] K. Ingols, M. Chu, R. Lippmann, S. Webster and S. Boyer, "Modeling Modern Network Attacks and Countermeasures Using Attack Graphs," 2009 Annual Computer Security Applications Conference, Honolulu, HI, 2009, pp. 117-126.

[8] S. Noel, M. Elder, S. Jajodia, P. Kalapa, S. O'Hare and K. Prole, "Advances in Topological Vulnerability Analysis," 2009 Cybersecurity Applications & Technology Conference for Homeland Security, Washington, DC, 2009, pp. 124-129.

[9] Jajodia S., Noel S. (2010) Topological Vulnerability Analysis. In: Jajodia S., Liu P., Swarup V., Wang C. (eds) Cyber Situational Awareness. Advances in Information Security, vol 46. Springer, Boston, MA

[10] A Singhal, X Ou, “Security risk analysis of enterprise networks using probabilistic attack graphs,” Gaithersburg, MD: U.S. Dept. of Commerce, National Institute of Standards and Technology, 2011, http://purl.fdlp.gov/GPO/gpo28803.

■ 저자소개 ■

고 장 혁
Kauh Janghyuk

1998년 3월~현재 국방과학연구소 책임 연구원
2018년 8월 광운대학교 컴퓨터과학과 공학박사
1998년 2월 광운대학교 컴퓨터과학과 이학석사
1996년 2월 광운대학교 컴퓨터과학과 이학사

관심분야 : 정보 보호, 사이버 상황인식, 병렬처리, 머신러닝
E-mail : jhkauh@add.re.kr

이 동 호
Lee Dongho

1984년 9월~현재 광운대학교 컴퓨터소프트웨어학부 교수
1988년 2월 서울대학교 컴퓨터공학과 공학박사
1983년 2월 서울대학교 컴퓨터공학과 공학석사
1979년 2월 서울대학교 전자공학과 공학사

관심분야 : 컴퓨터 네트워크, 차세대 인터넷
E-mail : dhlee@kw.ac.kr

논문접수일 : 2020년 3월 2일
게재확정일 : 2020년 3월 13일