

핵심기반시설 사이버 공격 경로 파악을 위한 자동화된 공격 그래프 생성 방안 연구

A Study on Automated Attack Graph Generation Method
to identify Critical Infrastructure Cyber Attack Paths

2021-10-12 (화)

전남대학교 정보보안협동과정
석사과정 신동혁
206413@jnu.ac.kr





I 연구 배경 및 목표

II 관련 연구

III 기존 연구의 문제점

IV 실험 및 결과

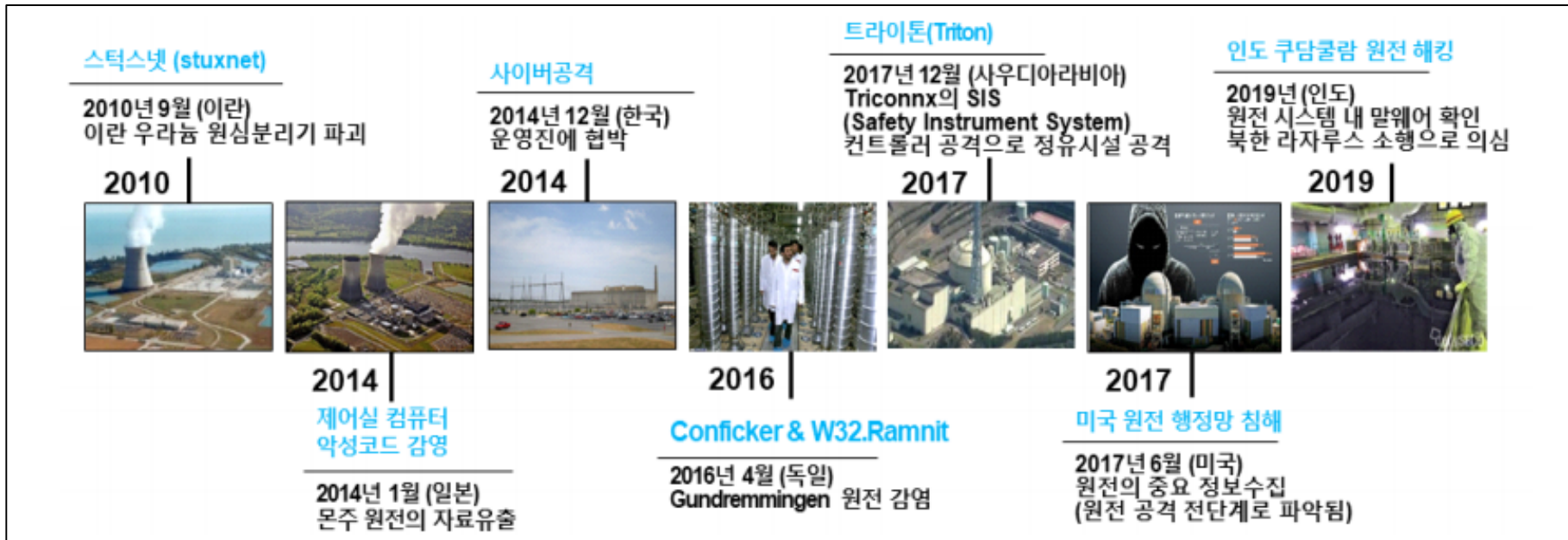
V 결론 및 향후 연구



01 연구 배경 및 목표

➡ 연구 배경

- ▶ 핵심기반시설에 대한 사이버 공격 사례 (망분리 환경에 대한 APT 공격 증가)



- ▶ 국내 원자력시설 사이버보안 규제 기준 KINAC RS-015 발표 (2014.10)

사이버 보안조치

- 필수디지털자산에 대한 **사이버 공격 및 영향 분석 (공격 벡터 및 공격 트리 등 활용)**을 수행하여 해당 보안조치로 인해 사이버공격이 가능하지 않음(공격벡터가 존재하지 않음)을 제시하고 문서화

01 연구 배경 및 목표

연구 배경

공격 그래프 기법

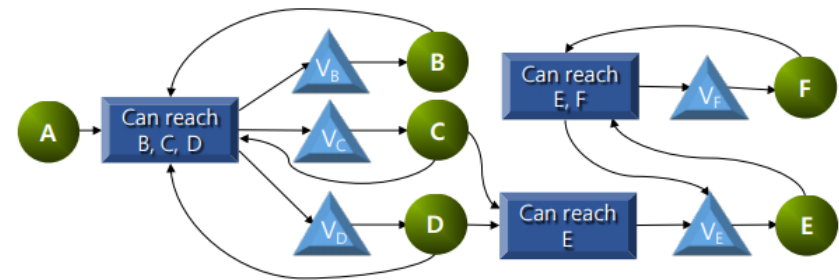
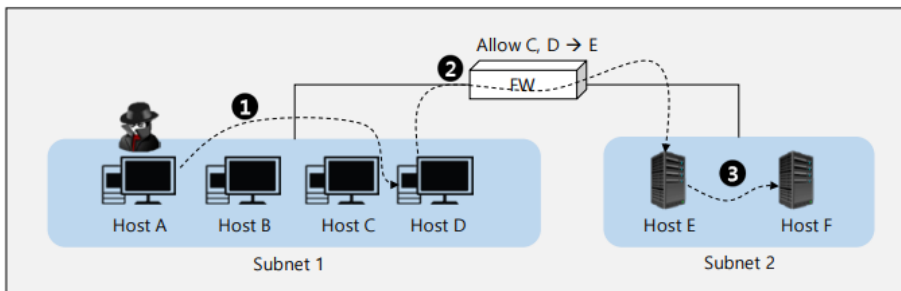
정의 : 네트워크 상에 존재하는 조직의 시스템에 대한 모든 연결 정보를 그래프로 표현하여 공격 경로가 될 수 있는 지점을 파악하기 위한 방법

특징 : 공격 그래프를 통해 조직의 네트워크 환경 및 취약점 분석을 수행하여 잠재적인 공격 경로 식별 및 가시화가 가능하여 위험 평가에 용이

연구 목표 및 방법

공격 그래프를 활용한 핵심기반시설 사이버 보안 위험 요소 파악 및 공격 경로 식별 방안 제시

1. 오픈 소스 프레임워크인 MuIVAL을 활용한 공격 그래프 생성 방안 제시
2. 가상으로 구축된 핵심기반시설 테스트베드 환경에서 공격 그래프 생성 실험 및 검증



공격 그래프 분석 예시

Subnet 1에 존재하는 호스트 A에 있는 공격자는 방화벽 규칙에 의해 Subnet2에 있는 호스트들로 접근이 불가능한 것처럼 보이지만, 호스트 C와 D에 내재된 취약점 Vc와 Vd를 이용해 궁극적으로 호스트 F와 E를 공격할 수 있음

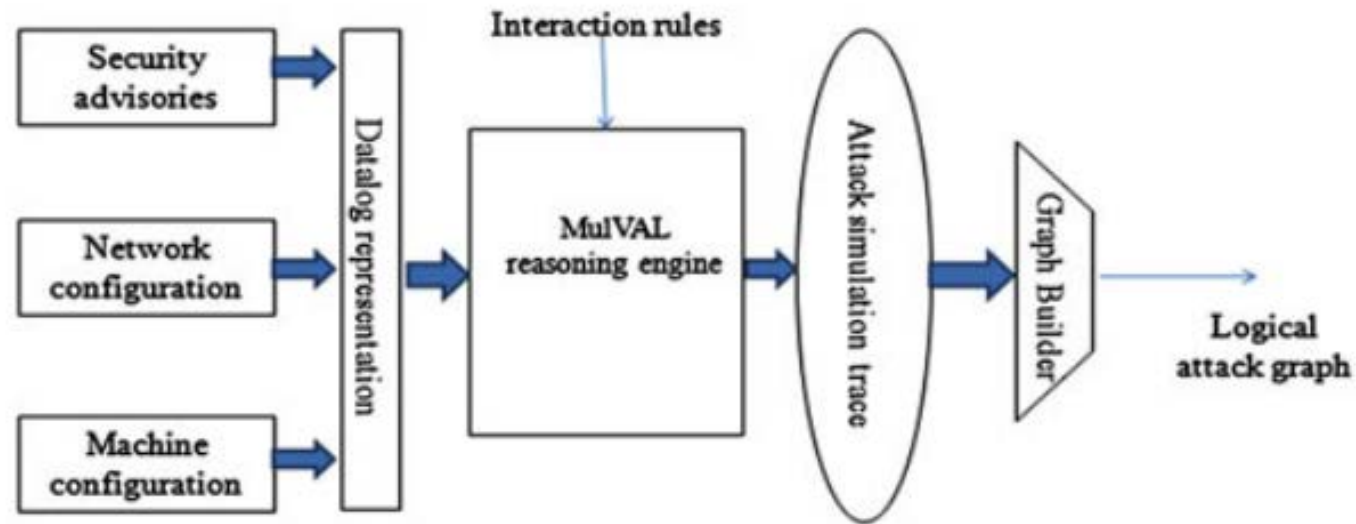
➡ 공격 그래프에서 사용되는 지표(Metric) 분류[1]

분류	특징	한계
네트워크 토폴로지 기반	<ul style="list-style-type: none"> 공격자의 정보, 시스템의 정보, 시스템 내의 보안 정책 등을 바탕으로 전체 시스템의 상태 구성 제한된 정보와 알기 쉬운 정보를 이용하여 네트워크 전반적인 안정성 및 공격 경로의 잠재적 위험성 분석 	<ul style="list-style-type: none"> 공격 그래프 연구 초기에 주로 사용된 기법 개별 자산의 안정성은 고려하지 않아 취약점을 통한 공격 경로 식별 불가능
취약점 기반	<ul style="list-style-type: none"> NVD의 취약점 데이터베이스를 활용하여 네트워크 내 취약점을 식별, 식별된 취약점으로 공격 경로 분석 공동 취약점 평가 체계(CVSS) 점수를 반영하여 공격 경로에 대한 정량적인 위험 평가 수행 	<ul style="list-style-type: none"> 취약점 데이터베이스에 의존하므로 소프트웨어 버전 등 자산에 대한 상세 분석 필요 공격자에 대한 정보가 반영되지 않아 취약점과 연결된 모든 공격 경로 식별
네트워크 토폴로지 및 취약점 기반	<ul style="list-style-type: none"> 네트워크 내에 존재하는 취약점에 대해 공격에 대한 저항성을 고려하여 공격 가능성을 예측 네트워크 전반적인 안정성과 개별 자산의 안정성도 함께 고려함으로써 각 지표의 한계를 보완 	<ul style="list-style-type: none"> 공격자의 공격 가능성을 예측할 수 있으나, 식별된 공격 경로에 대한 복잡성이 증가

➡ 공격 그래프 생성 기법 [2, 3, 4]

분류	공격 그래프 생성 방법	주요 특징	관련 도구
Dependency 공격 그래프	<ul style="list-style-type: none"> 공격에 필요한 사전 조건, 익스플로잇, 공격 성공에 따른 사후조건 간의 의존성을 모델링하여 공격 경로 생성 	<ul style="list-style-type: none"> 상용 취약점 스캔 도구 및 취약점 데이터베이스에 의존 	TVA (Topological Vulnerability Analysis)
Multiple Prerequisite 공격 그래프	<ul style="list-style-type: none"> 방화벽 규칙과 취약점을 통해 내부/외부 간 접근 가능 정보를 분석하여 공격 경로 생성 	<ul style="list-style-type: none"> 대규모 네트워크에서 공격 그래프 처리, 가시화에 특화 	NetSPA (Network Security and Planning Architecture)
시나리오 및 논리 기반 공격 그래프	<ul style="list-style-type: none"> 공격을 위한 악의적인 행위를 시뮬레이션 하고 공격 그래프를 생성, 공격자의 위치를 반영 공격 그래프간에 논리적인 관계를 반영, 시스템 구성 정보와 취약점으로 인한 잠재적 공격 결과간의 인과 관계를 정의 	<ul style="list-style-type: none"> Logic-Programming 기반 입력 데이터의 다양성으로 높은 확장성을 지원 오픈 소스 형태로 배포 	MuIVAL (Multihoist, Multistage, Vulnerability Analysis)
시맨틱 공격 그래프	<ul style="list-style-type: none"> 사이버 공격과 관련된 시맨틱 온톨로지를 구축 이를 기반으로 수집 자산 정보에 대한 지식 그래프를 생성하여 그래프 엔티티 간의 의미 관계를 추론 	<ul style="list-style-type: none"> 공격 벡터 정보를 이용한 공격 경로 검색이 가능 	-

➡ MuVAL 프레임워크 구성[5]



1. 전처리 단계 : 공격 그래프를 생성하기 위한 입력 데이터* 수집 및 Datalog 언어 형태로 변환
*입력 데이터 : 입력 정보는 네트워크 구성, 호스트 구성, 취약점, 주체, 상호작용 규칙, 보안 정책
2. 공격 경로 추론 단계: 입력 데이터를 기반으로 MuVAL 추론 엔진에 의해 공격 경로 생성
3. 그래프 표현 단계 : 트리 형태로 생성된 공격 경로를 그래프 형태로 변환

➡ MuIVAL 프레임워크의 문제 분석

- ▶ IT 시스템에 대한 모델링으로, 제어시스템(OT)에 대한 공격 경로 생성이 제한적

해결 방안 :

1. 필드 장비에 대한 자산 식별
2. 제어시스템 네트워크 구성 정의
3. 망 분리 환경에 대한 상호작용 규칙 정의

- ▶ 제어시스템 특성에 따른 취약점 동적 스캔(상용 취약점 스캐너 사용)의 제약

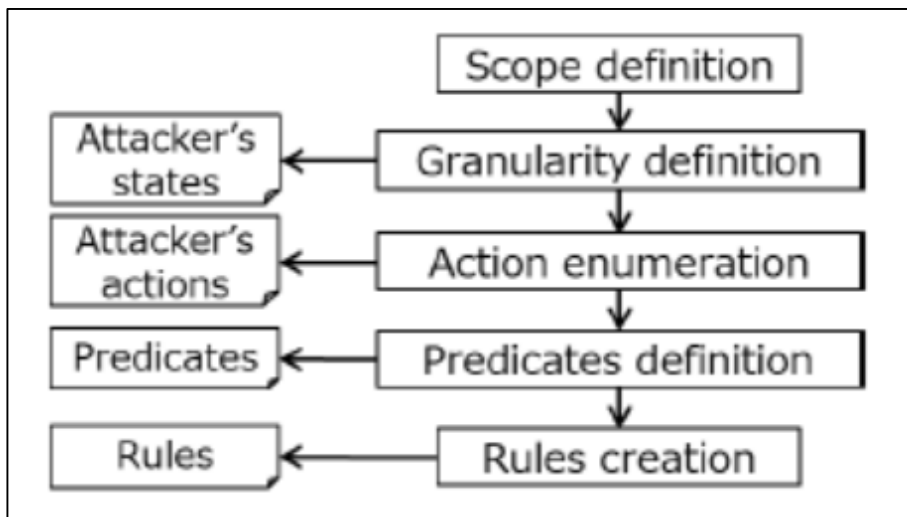
해결 방안 :

1. 네트워크 토폴로지 기반 공격 경로 식별
2. 제어 망 네트워크 구성 및 필드 장비 프로토콜 식별 상호작용 규칙 정의

03 기존 연구의 문제점

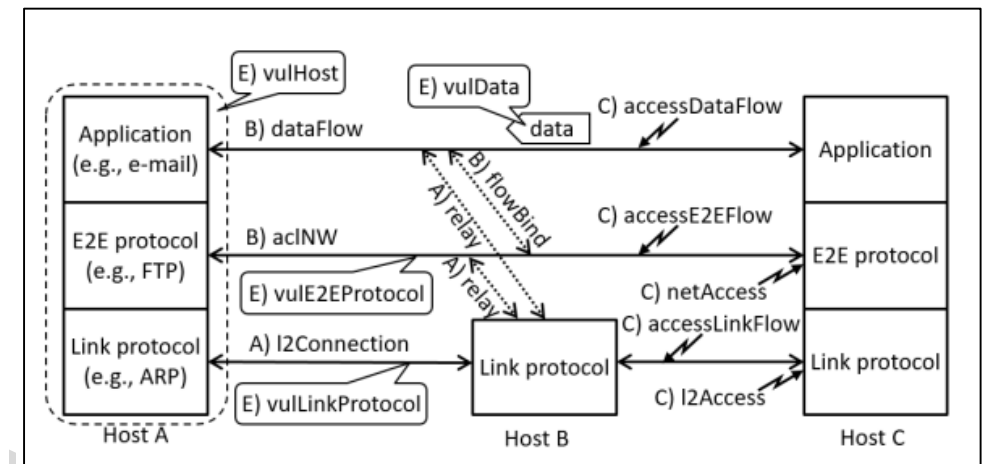
➡ MuVAL 프레임워크의 확장을 통한 해결 방안

- ▶ 보안성 평가를 위한 공격 그래프 생성 규칙 설계 및 구현에 관한 연구[6]



- Mitre ATT&CK 프레임워크에 기반한 공격자의 공격 범위 정의
- 연구 적용 방안 : 제어시스템 구성에 따른 공격 규칙 정의

- ▶ 통신 프로토콜에서 사이버 공격 경로를 식별하는 공격 그래프 확장[7]

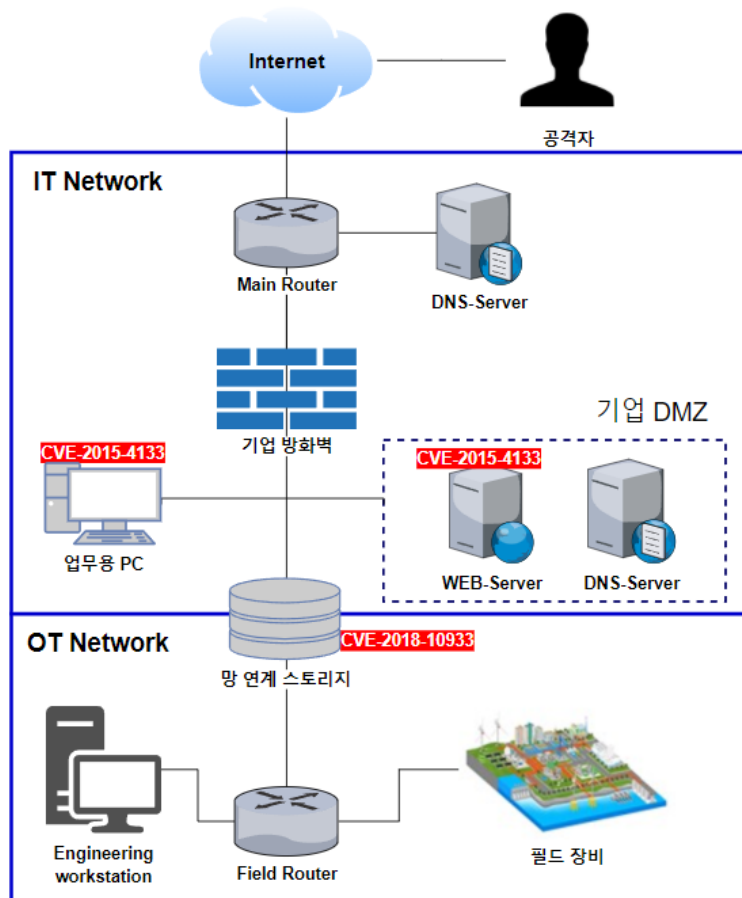


- 네트워크 프로토콜 취약점 모델링
- 물리적 네트워크 토폴로지 정의
- 산업 통신 아키텍처 모델링
- 연구 적용 방안 : 산업 통신 프로토콜 취약점 모델링

03 공격 그래프 생성 및 실험 결과

실험 환경 구성

가상으로 구축한 발전설비 테스트베드
네트워크 토폴로지



네트워크 구성 및 시스템 정보

네트워크 접근 제어 구성 정보

송신지	수신지	접근 제어 정책
Internet	DMZ	Web-server 접근 허용
업무망	제어망	망 연계 스토리지
제어망	업무망	FTP 서버 접근 허용
제어망	필드망	필드 장비 제어

식별된 취약점 정보

취약점 식별자	취약점 내용
CVE-2015-4133	웹 페이지 파일 업로드
CVE-2016-0189	IE11 브라우저 임의 코드 실행
CVE-2018-10933	원격 프로토콜(SSH) 인증 우회

공격자 정보

공격자의 위치 : 외부 인터넷

공격자의 목표 : 필드 장비

03 공격 그래프 생성 및 실험 결과

➡ 공격 그래프 생성

▶ Datalog 형태로 정의한 네트워크 구성 및 시스템 정보

```
attackerLocated(internet).  
attackGoal(commandInjection(engineering_Workstation, field_Device)).
```

```
/* configuration information of External Network */  
hacl(internet, webServer, tcp, 80).  
hacl(office_PC, webServer, _, _).
```

```
/* configuration information of webServer */  
vulExists(webServer, 'CVE-2015-4133', _).  
vulProperty('CVE-2015-4133', remoteExploit, executeCode).  
cvss('CVE-2015-4133', h).  
networkServiceInfo(webServer, wordPress, tcp, 80, apache).
```

```
/* configuration information of office_PC */  
installed(office_PC, 'Internet Explorer 11').  
isWebBrowser('Internet Explorer 11').  
vulExists(office_PC, 'CVE-2016-0189', 'Internet Explorer 11').  
vulProperty('CVE-2016-0189', remoteExploit, privEscalation).  
cvss('CVE-2016-0189', h).
```

```
/* configuration information of Internal Network */  
hacl(office_PC, fileServer, ssh, 22).  
hacl(office_PC, fileServer, ftp, 21).
```

```
/* configuration information of FileServer */  
vulExists(fileServer, 'CVE-2018-10933', libssh).  
vulProperty('CVE-2018-10933', remoteExploit, privEscalation).  
cvss('CVE-2018-10933', c).  
networkServiceInfo(fileServer, libssh, ssh, 22, root).  
networkServiceInfo(fileServer, proftpd, ftp, 21, root).
```

```
localFileProtection(fileServer, root, write, '/Engineer').  
localFileProtection(fileServer, root, read, '/Engineer').
```

```
/* configuration information of Control Network */
```

```
hacl(engineering_Workstation, fileServer, ftp, 21).  
hacl(engineering_Workstation, field_Device, modbus, 502).
```

```
execFile(engineering_Workstation, fileServer, read, '/Engineer').  
execFile(engineering_Workstation, fileServer, write, '/Engineer').
```

```
inCompetent(field_Device).
```

03 공격 그래프 생성 및 실험 결과

➡ 공격 그래프 생성

▶ 망분리 및 OT 환경을 반영한 상호작용 규칙 정의

파일 업로드 공격 규칙

```
interaction_rule(  
  (fileUpload(H, Software) :-  
    vulExists(H, VulID, Software, remoteExploit, executeCode),  
    networkServiceInfo(H, Software, Protocol, Port, Perm),  
    netAccess(H, Protocol, Port)),  
  rule_desc('remote file Upload', 'certain')).
```

필드 장비 명령 주입 공격 규칙

```
interaction_rule(  
  (commandInjection(Host, Victim) :-  
    execCode(Host, Perm),  
    hacl(H, Victim, Protocol, Port),  
    inCompetent(Victim)),  
  rule_desc('PLC Coil Write', 'certain')).
```

웹사이트 악성코드 다운로드 (Drive by Download) 공격 규칙

```
interaction_rule(  
  (execCode(H, _Perm) :-  
    vulExists(H, VulID, Software, remoteExploit, privEscalation),  
    installed(H, Software),  
    isWebBrowser(Software),  
    hacl(H, H2, httpProtocol, httpPort),  
    fileUpload(H2, _)),  
  rule_desc('Drive by download', 'possible')).
```

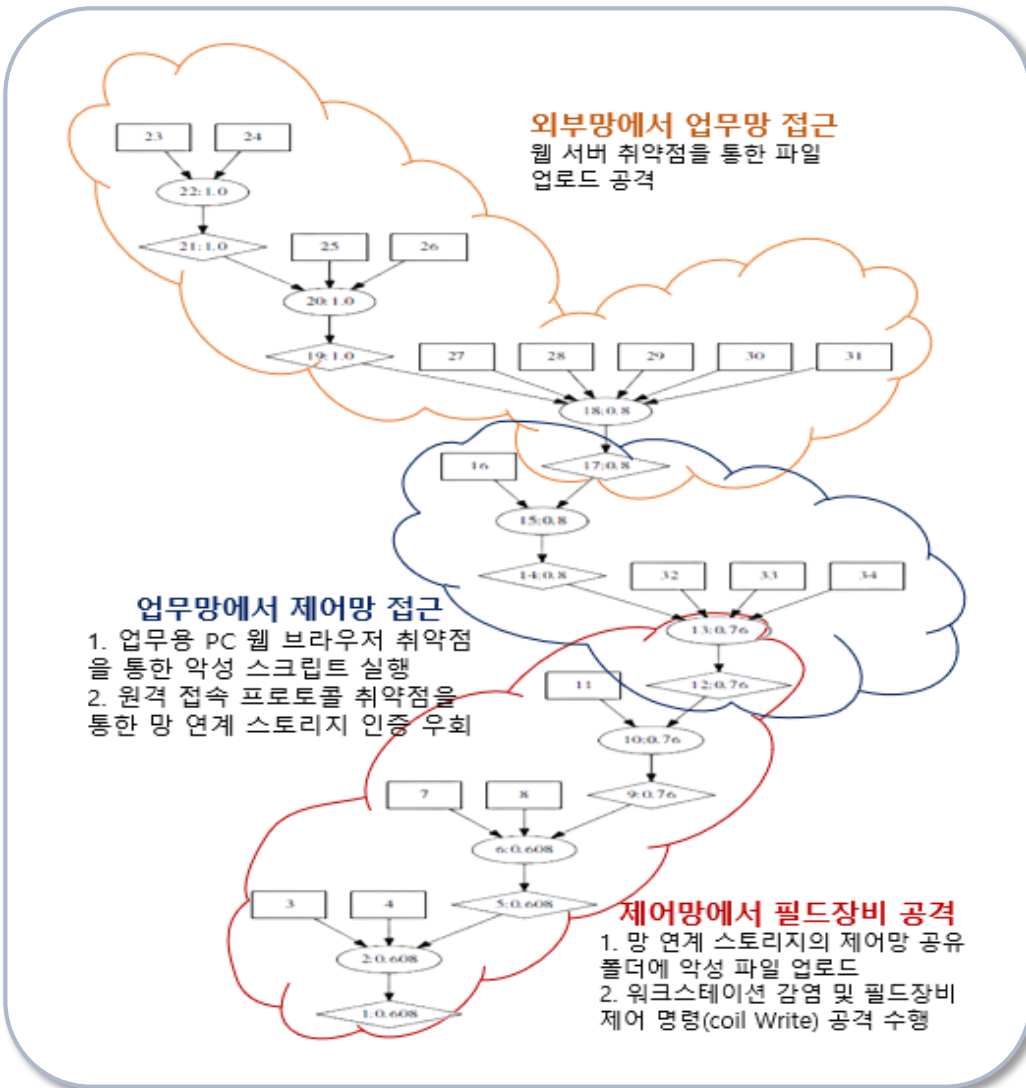
웹사이트 악성코드 다운로드 (Drive by Download) 공격 규칙

```
interaction_rule(  
  (execCode(H, _Perm) :-  
    accessFile(H2, write, Path),  
    execFile(H, H2, read, Path),  
    hacl(H, H2, Protocol, Port)),  
  rule_desc('Mulware Execute', 'likely')).
```

03 공격 그래프 생성 및 실험 결과

실험 결과

테스트베드에 대한 공격 그래프 생성 결과



공격 그래프 노드 별 의미

노드	내용
1-2	commandInjection(engineering_Workstation, field_Device)
3	inCompetent(field_Device)
4	haci(engineering_Workstation,field_Device, modbus,502)
5-6	execCode(engineering_Workstation_)
7	haci(engineering_Workstation,fileServer,ftp,21)
8	execFile(engineering_Workstation,fileServer,read,'/Engineer')
9-10	accessFile(fileServer,write,'/Engineer')
11	canAccessFile(fileServer,root,write,'/Engineer')
12-13	execCode(fileServer,root)
14-15	netAccess(fileServer,ssh,22)
16	haci(office_PC,fileServer,ssh,22)
17-18	execCode(office_PC,_)
19-20	fileUpload(webServer,wordpress)
21-22	netAccess(webServer,tcp,80)
23	haci(internet,webServer,tcp,80)
24	attackerLocated(internet)
25	networkServiceInfo(webServer,wordpress,tcp,80,apache)
26	vulExists(webServer,'CVE-2015-4133', wordpress,remoteExploit,executeCode)
27	haci(office_PC,webServer,httpProtocol,httpPort)
28	isWebBrowser('Internet Explorer 11')
29	installed(office_PC,'Internet Explorer 11')
30	cvss('CVE-2016-0189',h)
31	vulExists(office_PC,'CVE-2016-0189','Internet Explorer 11',remoteExploit,privEscalation)
32	networkServiceInfo(fileServer,libssh,ssh,22,root)
33	cvss('CVE-2018-10933',c)
34	vulExists(fileServer,'CVE-2018-10933',libssh,remoteExploit,privEscalation)

04 결론 및 향후 연구

➡ 결론

- ▶ 핵심기반시설에 대한 자동화된 공격 경로 생성을 위한 공격 그래프 확장
 - 가시화된 공격 경로 식별을 통한 효과적인 보안성 평가에 기여
- ▶ 취약점 평가 체계를 반영한 공격 경로별 정량적인 위험도 산출

➡ 향후 연구 방향

- ▶ 알려진 취약점에 의존하는 공격 그래프 생성 방식의 한계를 극복하기 위해 공격자의 성격 및 공격 패턴, 전술을 반영한 규칙을 정의하는 방안 연구

Q & A