「K-사이버 시큐리티 챌린지 2019」 설명회

[융합보안 챌린지]

- AI기반 네트워크 위협 탐지 트랙

손 경 아 주임

한국인터넷진흥원 보안기술확산팀

2019. 10. 1

Contents

1. AI기반 네트워크 위협 탐지 트랙 개요

개요

- 네트워크 보안 관제의 자동화 및 정확도 상승을 위해 AI를 활용하여 네트워크 트래픽에서 악성·정상을 탐지하는 기술의 성능을 검증하는 「AI기반 네트워크 위협 탐지」 트랙 개최

세부 절차

01 **신청 접수**
- ✓ 신청서 접수 및 참가자격 확인

02 **학습 데이터셋 배포**
- ✓ 신청 접수 후 3~5일 이내에 메일로 다운로드 URL 발송

03 **예선 진행**
- ✓ 온라인 예선
- ✓ 탐지율 상위 7개 팀 본선진출

04 **본선 진행**
- ✓ 오프라인 본선
- ✓ 탐지율 및 발표심사

05 **시상식 및 세미나**
- ✓ 3개팀 시·포상
- ✓ 공개 세미나 개최

2. 활용 데이터셋

실제 네트워크 환경에서 수집된 packet 파일에서 22가지의 Feature 정보를 추출·가공

- AI의 정상·악성 패턴 학습에 필요한 IP, TCP, UDP, HTTP request, HTTP response 관련 Feature 추출

학습 데이터셋

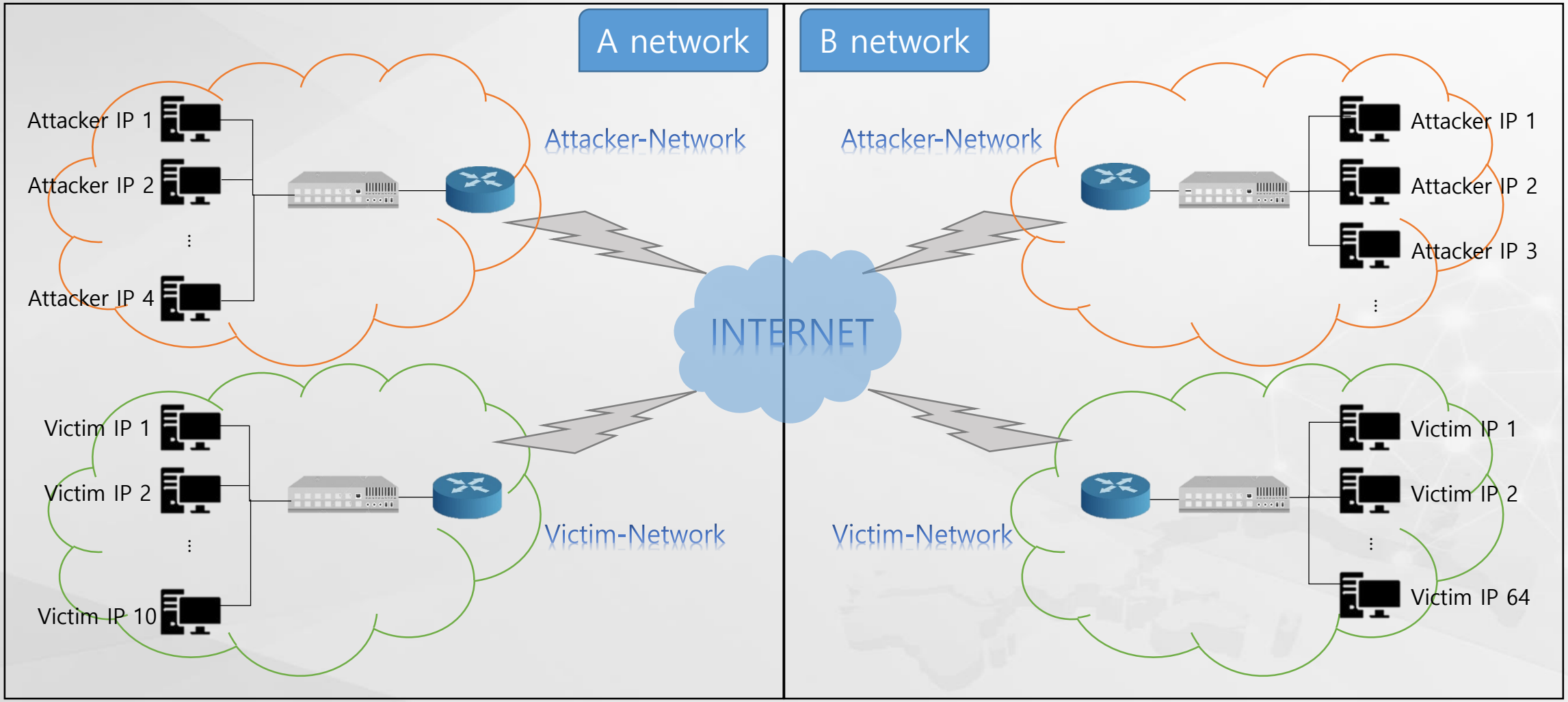
- ✓ (설명) 정상 데이터셋 + 악성 샘플
  - 정상 데이터셋 : IDS에서 탐지되지 않은 정상 패킷
  - 악성 샘플 : IDS에 탐지된 악성 유형별 샘플 패킷
- ✓ (규모) 약 3000만개 패킷(pcap파일 24GB)
- ✓ (구성) 패킷 별 feature 추출 csv 파일
  - pcap파일에서 추출한 22개의 Feature 정보

예 · 본선 데이터셋

- ✓ (설명) 정상 트래픽 + 악성 트래픽 혼합 데이터셋
- ✓ (규모) 추후 공지
- ✓ (구성) 패킷 별 feature 추출 csv 파일
  - pcap파일에서 추출한 22개의 Feature 정보

2-1. 활용 데이터셋 – 네트워크 구성도

- A, B 두 네트워크에서 수집된 트래픽으로, Windows, Linux, Mac 3가지 운영체제를 포함해 구성



3. 결과물 제출 및 심사기준

1. 결과파일

✓ 탐지결과 악성 Flow의 source IP, destination IP, source port, destination port, 공격 유형 (csv파일)

✓ 공격 유형 탐지 시 추가 점수 부여

	A	B	C	D	E
1	source_ip	destination_ip	source_port	destination_port	attack_type
2	xxx.xxx.xxx.xxx	ooo.ooo.ooo.ooo	1234	4321	DoS

(예시)

2. 알고리즘 설명문서

✓ 데이터 분석 및 분류 결과, AI 알고리즘 구성 방법,
수도코드(pseudocode), 예선 데이터 실험과정, 예상 결과, 보완점 등을 작성

✓ 평가 내역 : 자동화, 알고리즘 창의성 등

(※ 알고리즘 설명문서를 검토하여 편법 사용 등 문제 발견 시, 수상에서 제외될 수 있음)

3. 발표자료

✓ 알고리즘 설명문서를 바탕으로 15분 분량으로 작성

✓ 평가 내역 : 자동화, 알고리즘 창의성 등

탐지율 (80%) + 발표 점수 (20%)
(공격유형 탐지 추가 점수 포함)

4. 예·본선 진행방식

- (예선) 11월 8일 10:00~18:00, 온라인으로 진행
- (본선) 11월 21~22일 예정, 오프라인으로 진행 (발표 평가 포함)

예선

- (일정) 11월 8일 10:00~18:00
- (1라운드) Set1 / 약 10GB의 패킷에서 추출한 22개 Feature 분석
- (2라운드) Set2 / 약 10GB의 패킷에서 추출한 22개 Feature 분석
- (심사기준) 탐지율 100%

  ※ 공격유형 탐지 시 추가점수 부여
- (본선 진출팀) 상위 7개팀

본선

- (일정) 11월 21~22일 예정
- (1라운드) Set1 / 약 10GB의 패킷에서 추출한 22개 Feature 분석
- (2라운드) Set2 / 약 10GB의 패킷에서 추출한 22개 Feature 분석
- (심사기준) 탐지율 80% + 발표 점수 20%

  ※ 공격유형 탐지 시 추가점수 부여

※본선 일정은 추후 공지

5. 탐지율 채점기준

문제

o 주어진 네트워크 트래픽에서 공격이 발생한 **Flow**를 탐지하세요.

탐지 정확도

o F1-score 수식으로 탐지 정확도 측정

$$F1\text{-}score = 2 \times \frac{Precision \times Recall}{Precision + Recall}$$

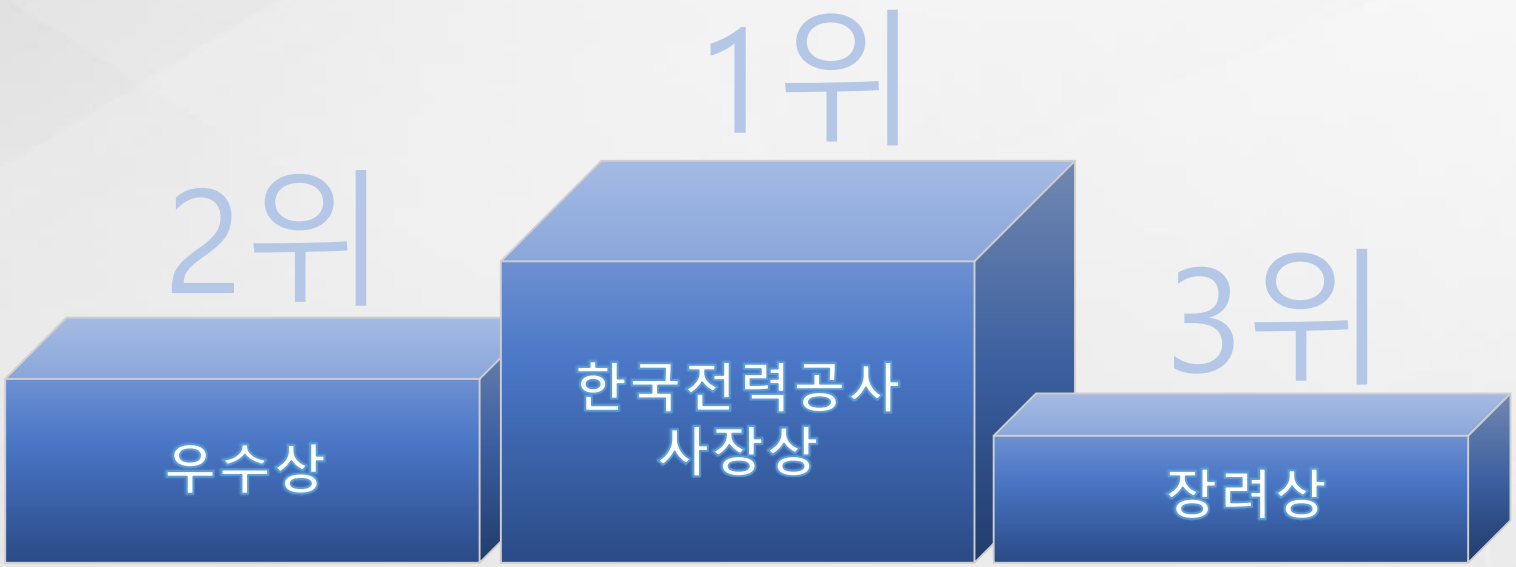
o Precision (정확률) : 제안한 알고리즘이 공격을 판단했을 때 실제 공격이 이루어진 비율 $\left(\frac{\text{정답 인정수}}{\text{참가자가 예측한 공격 수}}\right)$

o Recall (재현율) : 실제 공격이 이루어졌을 때 제안된 알고리즘이 공격을 판단하는 비율 $\left(\frac{\text{정답 인정수}}{\text{실제 공격 수}}\right)$

카테고리		정답	
		공격	정상
탐지결과	공격	True Positive (TP)	False Positive (FP)
	정상	False Negative (FN)	True Negative (TN)

$$Precision = \frac{TP}{TP+FP} \qquad Recall = \frac{TP}{TP+FN}$$

6. 시상내역



7. 접수기간 및 신청절차

접수기간

2019.10.1(화) ~11.6(수)

신청절차

01 datachalleng.kr
- ✓ 정보보호 R&D 데이터챌린지 홈페이지 접속

02 「AI기반 네트워크 위협 탐지 트랙」
- ✓ 트랙 선택

03 신청서류 다운 및 작성
- ✓ 참가신청서
- ✓ 약정서

04 rnd_dataset@kisa.or.kr로 제출
- ✓ 이메일로 신청서류, 소속증명서 제출

감사합니다.

<문의처>
한국인터넷진흥원 손경아 주임
(T. 061-820-1256)
(E. rnd_dataset@kisa.or.kr)