정보보호학회 트랙 소개

자동차용 침입탐지 트랙

2019. 10. 1.

고려대학교 정보보호대학원

김 휘 강

KOREA UNIVERSITY

HCRL
Hacking and Countermeasure Research Lab

2019년 정보보호학회 담당 트랙 소개

- **주안점 – 다양성, 연속성**

- **2019년 게임봇 탐지 트랙**
  - 다양한 분야 제공을 위해 신규 주제의 트랙 오픈
  - 기 게재되어 검증된 논문과 dataset 활용, academic follow-up research 활성화
  - 해당 참고 논문 주저자가 직접 문제 출제 담당

- **2017년의 차량 이상징후 탐지 트랙 ➔ 2018 차량주행 데이터 기반 도난탐지 트랙 ➔ 2019 자동차용 침입탐지 트랙**
  - 차량 보안 분야 트랙의 연속성 유지
  - 차량용 IDS 개발 분야에 응용 가능
  - 기 게재되어 검증된 논문과 dataset 활용, academic follow-up research 활성화
  - 해당 참고 논문 주저자가 직접 문제 출제 담당

Challenge

자동차용 침입 탐지 알고리즘 개발

✔ **차량 내부 네트워크 데이터셋 기반의 침입 탐지를 할 수 있는 알고리즘 및 프로그램을 제시하기 바랍니다.**

- **정상적인 차량 네트워크에서 차량 공격에 대한 침입 탐지**

사례

자동차를 타고 출근하는 K씨는 최근 자신의 차량이 조금씩 이상증세가 보이는것을 알게 되었습니다.

알고 보니, 차량에 대한 원격접속을 통해 차량의 내부 네트워크를 공격 당하고 있었습니다.
위 상황과 같이 **차량의 원거리 및 직접 접근을 통해 차량의 내부 네트워크 공격이 발생 가능하며, 이를 효율적으로 탐지하는 방안이 필요합니다.**

제출물

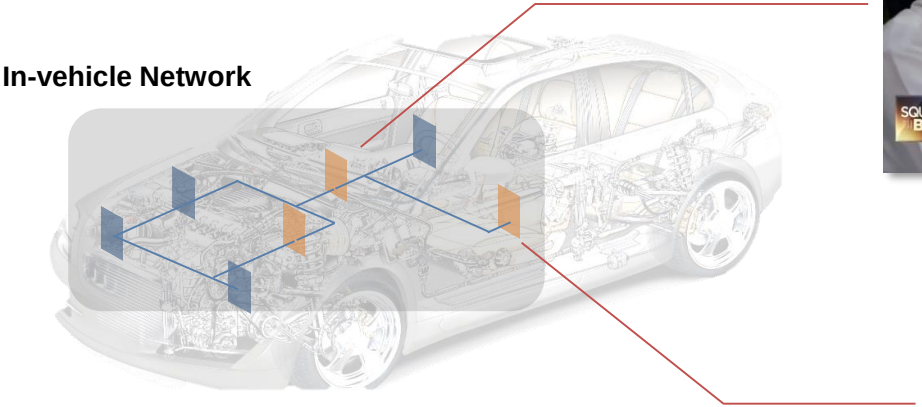
- **프로그램**
  - GitHub 링크 제출 (Public 링크)
- **결과파일**
- **알고리즘 설명 문서**

배경

차량 내부 네트워크 침입을 통해, 차량의 제어권한을 획득 및 원격에서 차량 제어

- **차량 원격 제어 – Charlie Miller and Chris Valasek (‘15)**
  - Jeep Cherokee 차량에 대한 CAN Bus로 악의적인 메시지 주입으로 차량 제어 시연

- **차량 원격 제어 및 취약점 탐지 – Keen Security Lab (‘16, ‘17)**
  - BMW 및 Tesla S 차량에 대한 공격을 통해 차량으로부터 12mile (약19km) 떨어진 거리에서 차량 제어 시연
  - ECU 제어를 통해 Tesla X 에 대한 헤드라이트 제어 시연



데이터셋

차량 내부의 CAN Bus Message들을 수집

□ 제공될 CAN Message는 Timestamp, CAN ID, DLC, Payload 로 구성됨

- 학습용 데이터셋에는 라벨링이 이뤄져있으며, 제출용 데이터셋에는 라벨링이 삭제되어 있음

```
Timestamp: 1481192898.078149    ID: 04b1 DLC: 8    00 00 00 00 00 00 00 00
Timestamp: 1481192898.078396    ID: 0164 DLC: 8    00 08 00 00 00 00 05 0d
Timestamp: 1481192898.078637    ID: 0370 DLC: 8    ff 20 00 80 ff 00 00 ec
Timestamp: 1481192898.078873    ID: 043f DLC: 8    10 50 64 ff 51 54 09 00
Timestamp: 1481192898.079115    ID: 0440 DLC: 8    ff f0 00 00 ff 54 09 00
Timestamp: 1481192898.079357    ID: 04f2 DLC: 8    00 00 90 38 00 00 00 a1
Timestamp: 1481192898.079597    ID: 0110 DLC: 8    e0 3c 30 09 00 00 00 00
```

CAN Message 예시

□ 차량 3종에서 정상 및 공격 데이터셋을 수집

- YF Sonata, KIA Soul, Chevrolet SPARK 차량에 대한 정상 상태 및 공격 상태에 대한 CAN 데이터셋 수집
- 공격에 대한 차량 돌발상황 대처를 위해, 정차상태에서 데이터셋 수집

YF Sonata

KIA Soul

Chevrolet SPARK

운영방식

온라인 예선(10.1~11월 중), 오프라인 본선(11~12월 중) 진행

온라인 예선
(2019.10.1~2019.11)

홈페이지 신청
- 개인, 팀(최대 5인) 신청
- 트랙 다중 신청 가능

데이터셋 배포
- 신청자에 한해 다운로드 링크 제공

결과물 제출
- 탐지결과파일(CSV)
- 알고리즘 설명 문서
- 프로그램

예선결과 심사
(2019.11)

제출물 심사
- 결격사유 만족 시 제외 (서류 누락, 허위 작성 등)

상위 팀 선정
- 탐지율 높은 순

본선진출자 발표
- 홈페이지 공지 및 개별 연락

오프라인 본선
(2019.11~2019.12)

데이터셋 배포
- 본선 진행 안내
- 데이터셋 배포 (예선 결과에 따라 난이도 조정)

탐지결과 제출
- 최대 3~5회 제출 가능
- 마지막 제출결과로 점수반영

프레젠테이션
- 알고리즘, 분석내용 발표
- 탐지율과 발표점수 합산하여 최종순위 산출

수상
정보보호학회 동계학술대회
(2019.12 中)

시상식
- 본선 최종순위에 따라 수상
- 학회 동계학술대회에서 진행

기술공유 세미나
- 챌린지 수상자, 업계 관계자 등 참석
- 상세 일정 협의 中

차량 내부 네트워크 데이터셋

데이터셋 구성

□ **KU-Survival Analysis Dataset**

- Mee Lan Han, Byung Il Kwak, and Huy Kang Kim. "Anomaly intrusion detection method for vehicular networks based on survival analysis." Vehicular Communications 14 (2018): 52-63.

□ **예선: KIA Soul, HYUNDAI Sonata, CHEVORLET Spark 차량 3개에 대한 정상 (Attack free), 공격 (Flooding, Fuzzy, Malfunction) 데이터셋**

- 분석용 데이터셋의 경우 데이터 분석을 위해 정답지가 포함된 데이터셋을 제공
- 결과 제출시 정답지가 없는 제출용 데이터셋의 사용 결과를 제출해야 함

□ **본선: KIA Soul, HYUNDAI Sonata 차량 2개에 대한 정상 (Attack free), 공격 (Flooding, Fuzzy, Malfunction) 데이터셋**

- 예선과 동일하게, 분석용 및 결과 제출용으로 나누어 제공하며, 제출용 데이터셋에는 정답지를 제공하지 않음 (경우에 따라 차종 추가 가능)
- 예선 결과에 따라, 본선의 공격 데이터셋이 새롭게 추가될 수 있음

* 데이터셋 규모 및 정답지 여부는 진행상황에 따라 조정될 수 있음

구분	사용용도	정상 / 공격 (Flooding, Fuzzy, Malfunction)	클래스 정보 여부
예선	분석용	3개 차종에 대해 정상/공격 데이터를 40,000 ~ 70,000개 선정	제공
	제출용	3개 차종에 대해 정상/공격 데이터를 20,000 ~ 40,000개 선정	-
본선	1차 분석/제출	TBD (본선 진행 시간 고려하여 규모 조정)	분석용 제공 / 제출용 미제공
	2차 분석/제출		분석용 제공 / 제출용 미제공

상세 진행방식

예선 (온라인)

□ **진행기간**
- 2019. 10. 1 ~11월 중

□ **신청방법**
- 데이터 챌린지 홈페이지를 통해 신청 양식 작성 및 제출 (datachallenge.kr)
- 신청자에 한해 예선 데이터셋 다운로드 URL 및 파일 비밀번호 배포

□ **결과물 제출**
- 탐지결과파일 (CSV), 알고리즘 설명 문서, 프로그램
- 제출 방법은 사이트를 통해 추후 공지

□ **평가**
- 공격 탐지 정확도 점수 100%로 예선 평가
- 공격 탐지 정확도는 "**평가방법 – 탐지 정확도**"를 따름
- 알고리즘 설명 문서와 프로그램은 치팅 여부 검증을 위한 목적으로만 활용

상세 진행방식

본선 (오프라인)

□ **본선 진출자 발표**
- 예선 결과물을 채점하여 탐지정확도 순으로 상위 7팀 선정
- 홈페이지 공지 및 개별 연락(이메일)

□ **진행일자**
- 2019. 11~12월 중 (1일)

□ **본선 진행**
- 1차/2차로 나누어 총 2차례 테스트 데이터셋 배포
  - 예선과 동일한 형식으로, 정상 및 비정상 데이터셋을 배포
- 탐지 결과는 여러 번 제출 가능 (각 차수별 최대 3회까지 탐지 결과 제출 가능)
- 본선 당일 알고리즘 및 분석내용 발표 진행 (약 10분 발표, 5분 질의)

□ **평가**
- 탐지 정확도 80%, 발표 점수 20% 합산 – 조정될 수 있음 (예선 오픈 시 공지)
  - 탐지 정확도
    - 1차, 2차 탐지 정확도의 평균값으로 산정
    - 각 차수의 마지막 제출한 결과를 최종 점수로 반영
  - 발표
    - 문제 해결을 위한 방법론의 논리성, 창의성 위주로 채점

평가방법

탐지정확도(F1-score)

카테고리		실제결과	
		공격	정상
실험결과	공격	*True Positive (TP)*	*False Positive (FP)*
	정상	*False Negative (FN)*	*True Negative (TN)*

- Precision은 "정밀도"로써 공격으로 예측한 결과 (**TP + FP**) 중 실제로 공격인 (**TP**) 비율을 나타냄
- Recall은 "재현율"로써 실제 공격 (**TP + FN**) 중 유저 중 공격 (**TP**)으로 정확히 예측한 비율을 나타냄

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

- F1-Score는 Precision과 Recall의 조화평균으로, 공격과 정상 데이터의 비율이 일정하지 않은 상황에서 성능을 합리적으로 평가할 수 있음

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

Thank You

KOREA UNIVERSITY

HCRL
Hacking and Countermeasure Research Lab