놀라운 CAN 공격 탐지 기법

2019. 11. 22.

정보보호 R&D 데이터 챌린지 2019(자동차용 침입탐지) 본선

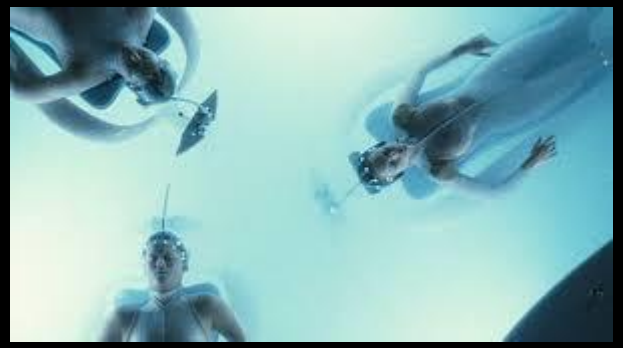
「차가놀라면?카놀라유!엌ㅋ」

팀원 소개

- 팀장
  - 최슬기
- 팀원
  - 박정연 (이상 이화여자대학교 사이버보안전공)
  - 권혁민
  - 김종민
  - 이상욱 (이상 고려대학교)

분석 방법론

- 3가지 알고리즘을 적용한 결과에 대한 다수결 판정
  - 메이저리티 리포트 방법론
- 사용된 알고리즘
  - Survival Rate
  - Hamming Distance
  - Loose Ground Truth



S.R.	H.D.	L.G.T.	Result
R	T	T	T
R	T	R	R

Survival Rate

- 특정 시점의 대상의 생존 확률
- Step 1. Survival Rate 계산
  - 공격이 없는 CAN 패킷을 활용하여 CAN ID 별 Survival Rate의 MIN 값 및 MAX 값을 계산
- Step 2. Survival Rate 검증
  - 임의의 패킷을 Chunk로 나눴을 때, 각각의 CAN ID의 Survival Rate를 계산한 다음, Step 1의 Survival Rate와 비교
    - MIN, MAX 값의 범위 내 – 정상
    - MIN, MAX 값의 범위 외 – 공격

$$SR(C_i^{CAN\_ID}) = \frac{F(C_i^{CAN\_ID})}{S(C_i^{CAN\_ID})} \quad (1)$$

- $C_i = \{C_1, C_2, \ldots, C_i \parallel 1 \le i \le n\}$: 특정 시간대의 CAN msg 들을 특정한 수로 나눈 Chunk들
- i: Chunk의 index
- $S(C_i^{CAN\_ID})$: 하나의 Chunk unit에 대한 모든 CAN msg
- $F(C_i^{CAN\_ID})$: 하나의 Chunk unit에서 특정 CAN msg가 출연하는 빈도
- $SR(C_i^{CAN\_ID})$: 하나의 Chunk unit에서 특정 CAN msg의 Survival rate

(*논문의 결과를 참조하여
Chunk size를 100으로 지정하였음)

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.

Hamming Distance

- Hamming Distance는 같은 길이를 가진 두 개의 문자열의 서로 다른 문자 개수를 의미
  - p_t - 시간 t에서의 CAN 패킷의 Payload
  - p_t^i - 해당 페이로드의 i번째 비트
  - $\mathcal{H}_d$ - 는 CAN ID d에서의 Hamming distance
    - d 에 해당하는 CAN ID의 시간 t와 시간 $t+1$ 사이의 모든 비트의 XOR 연산 결과에서의 1의 총 개수를 뜻한다.
- Survival Rate 기법과 마찬가지로, $\mathcal{H}_d$ 의 MIN, MAX를 계산 후 이를 임의의 패킷과 비교

$$\mathcal{H}_d(p_t, p_{t+1}) = \sum_{i=1}^{64} p_t^i \otimes p_{t+1}^i$$

05	21

0000 0101 0010 0001

XOR

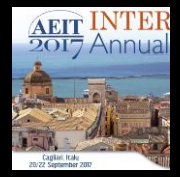
XOR

04	21

0000 0100 0010 0001

$\mathcal{H}$ = 1
(XOR 연산 후 1의 총 개수)

0000 0001 0000 0000



Stabili, Dario, Mirco Marchetti, and Michele Colajanni.
"Detecting attacks to internal vehicle networks through Hamming distance."
2017 AEIT International Annual Conference. IEEE, 2017.

Loose Ground Truth

- Ground Truth
  - 정상적인 CAN 패킷에서 CAN ID 별 Data field의 각각 Byte index에 올 수 있는 값을 산정하고, 이를 Ground Truth로 지정
  - 임의의 CAN 패킷들을 하나씩 비교하여 그 패킷이 Ground Truth 범위 내에 포함되는 패킷이라면 정상
  - 그렇지 않을 경우 공격
- Loose Ground Truth
  - Ground Truth 기법을 확장하여 데이터 필드의 인덱스를 고려하지 않고 등장하는 바이트만을 고려
  - 정상 패킷에서는 감지되지 않는 Ground Truth가 있을 가능성을 고려함

```
GROUND TRUTH REPORT
CAN ID | DLC | POSSIBLE VALUES
0x260  | 08  | <0:['0x1b', '0x1c', '0x1d']>
             | <1:['0x24', '0x25', '0x26', '0x27']>
             | <2:['0x25', '0x26', '0x27']>
             | <3:['0x30']>
             | <4:['0x00']>
             | <5:['0x90']>
             | <6:['0x65', '0x66', '0x67', '0x68', '0x69', '0x6
x79', '0x7a', '0x7b', '0x7c', '0x7d', '0x7e', '0x7f', '0x80', '
             | <7:['0x00', '0x01', '0x02', '0x03', '0x04', '0x0
x14', '0x15', '0x16', '0x17', '0x18', '0x19', '0x1a', '0x1b', '
 '0x2b', '0x2c', '0x2d', '0x2e', '0x2f', '0x30', '0x31', '0x32'
```

(SONATA의 CAN ID 0x260에 대한 Ground Truth)

AI가.... 없어....?

*RNN-LSTM 모델 학습

- 기계학습에 의한 탐지의 탐지율이 낮아 본 챌린지에 적용되지는 않은 방법
- RNN의 일종인 LSTM 신경망 모델을 사용하는 기법
  - Word Vector 학습을 통한 Binary Sentiment Classification 관련 논문에서의 방법론을 적용
  - Train 데이터에서 CAN ID와 Data field, Byte Index를 입력 데이터로 설정
  - 제출용 데이터의 CAN ID 와 Data field를 출력 데이터로 설정
  - 순환 신경망에서의 학습을 통해 제출용 데이터의 CAN ID와 Data field를 고려하여 Byte Index를 예측

Andrew L. Maas, Raymond E. Daly, Peter T. Pham, Dan Huang, Andrew Y. Ng, and Christopher Potts.
"Learning Word Vectors for Sentiment Analysis"
Proceedings of the 49th annual meeting of the association for computational linguistics: Human language technologies-volume 1, 142-150, 2011

분석 결과

- Test Set 기준

Survival Rate

	Spark	Sonata	Soul
Flooding	94.42%	81.11%	85.46%
Fuzzy	98.10%	90.45%	80.70%
Malfunction	97.87%	92.31%	98.24%

Hamming Distance

	Spark	Sonata	Soul
Flooding	100%	100%	100%
Fuzzy	100%	100%	100%
Malfunction	100%	64%	100%

Loose Ground Truth

	Spark	Sonata	Soul
Flooding	100%	100%	100%
Fuzzy	99.98%	99.59%	99.97%
Malfunction	100%	66.67%	100%

RNN-LSTM

	Spark	Sonata	Soul
Flooding	100%	100%	80.21%
Fuzzy	85.16%	83.33%	90.63%
Malfunction	84.34%	82.58%	93.91%

감사합니다

Q&A Time