[용어, 축약 정리] ★

ASCA(acoustic side channel atk): 음향 사이드 채널 공격

> asc attacks

SCA(side channel atk): [암호학](https://ko.wikipedia.org/wiki/%EC%95%94%ED%98%B8%ED%95%99)에서 **부채널 공격**(side channel attack)은 [알고리즘](https://ko.wikipedia.org/wiki/%EC%95%8C%EA%B3%A0%EB%A6%AC%EC%A6%98)의 약점을 찾거나([암호 해독](https://ko.wikipedia.org/wiki/%EC%95%94%ED%98%B8_%ED%95%B4%EB%8F%85)과는 다름) [무차별 공격](https://ko.wikipedia.org/wiki/%EB%AC%B4%EC%B0%A8%EB%B3%84_%EB%8C%80%EC%9E%85_%EA%B3%B5%EA%B2%A9)을 하는 대신에 [암호 체계](https://ko.wikipedia.org/w/index.php?title=%EC%95%94%ED%98%B8_%EC%B2%B4%EA%B3%84&action=edit&redlink=1)의 물리적인 [구현](https://ko.wikipedia.org/wiki/%EA%B5%AC%ED%98%84) 과정의 정보를 기반으로 하는 공격 방법이다. 예를 들어, 소요 시간 정보, 소비 전력, [방출하는 전자기파](https://ko.wikipedia.org/wiki/%EC%A0%84%EC%9E%90%EA%B8%B0%ED%8C%8C), 심지어는 [소리](https://ko.wikipedia.org/w/index.php?title=%EC%9D%8C%EC%84%B1_%EC%95%94%ED%98%B8_%ED%95%B4%EB%8F%85&action=edit&redlink=1)를 통해서 시스템 파괴를 위해 악용할 수 있는 추가 정보를 얻을 수 있다.

부채널 = 사이드 채널

모듈식 노트북: 디스플레이도 자석으로 손쉽게 붙였다 떼어낼 수 있으며, 키보드 언어와 배치도 자유롭게 할 수 있음

--------

VoIP(voice over internet protocol): VoIP 전화 시스템은 일반 유선이나 모바일 네트워크 대신 광대역 인터넷 연결을 통해 전화를 거는 기술입니다. VoIP 통신 및 인스턴트 메신저 시스템은 광대역 연결을 통해 아날로그 음성 신호를 디지털 신호로 변환합니다. VoIP 서버는 통화를 다른 전화 네트워크에 연결하는 데 사용됩니다

----------------------------------------------------

[INTRO]

<부채널 공격에 대한 설명>

부채널 공격에는 장치에서 방출되는 신호의 수집 및 해석이 들어감

전자기파, 전력 소비, 모바일 센서, 소리와 다양한 발산 유형을 활용함

그 중에서도 가장 감지하기 쉽고 훨씬 더 널리 퍼지는 키 입력 소리가 존재함

<음향 부채널 공격이 쉽게 시도할 법한 공격임을 의견 제시 1 \_음향>

비밀번호를 입력할 때 화면은 숨기지만 소리를 난독화하려는 노력은 기울이지 않음

여러 논문에서 TC data에서 올바른 키를 추론할 수 있는 모델을 만들었지만 이러한 모델은 최신 키보드, 특히 노트북보다 음향이 훨씬 더 뚜렷한 오래되고 두꺼운 기계식 키보드에서 훈련 및 테스트되는 경우가 많음

<제시2 \_음향>

음향에 접근하고 처리할 수 있는 기술은 극적으로 향상됨

- VoIP(Voice over Internet Protocol) 통화 및 키 입력 녹음을 수집하는 데 사용되는 스마트워치와 같은 마이크 기술의 발전이 있음

<제시3 \_DL>

DL에 대한 간단한 설명(Dl이 이렇게 발전해왔다 정도)

<정리,타겟 설정>

마이크와 DL이 이렇게 성능이 높아져 최근 연구에서 키보드에 대한 음향 공격의 타당성이 보이기 시작했음

공공장소에서 자주 사용하는 노트북이 주요 타겟

노트북은 모듈식이 아니라 동일한 모델이면 동일한 키보드를 사용함

> 유사한 키보드 발산이 가능함

(우리는 노트북과 동일한 구조를 가진 기계식 키보드로 먼저 대상을 선정했음을 설명할 필요가 있음)

<현재 연구가 자세히 이뤄지지 않은 부야임을 설명 1>

예를 들어, 2011년 NIST 보고서[13]에서는 부채널 분석 대책을 활용하는 암호화 모듈이 원하는 보안 수준에 상응하는 이러한 공격에 대한 저항을 제공할 수 있는지 여부를 평가하기 위한 테스트 방법이 제안되었습니다.

<설명2>

부채널 공격 표준화에 대한 구체적인 연구는 없지만 업계에서는 알려진 공격 중 일부를 수정하려는 시도가 있었음

구글, intel의 예시

그렇지만 음향 채널은 사이드 채널로 포함하지 않음

asca에 대한 명시적인 표준화 작업은 없음

[Research Question] ★

(RQ1) 키 입력 분리, 특징 추출 및 예측을 포함하여 완전히 자동화된 ASCA 파이프라인을 설계하고 구현할 수 있습니까?

(RQ2) ASCA에 정확한 딥 러닝 접근 방식을 배포할 수 있습니까?

(RQ3) 오디오 전송의 압축 및 정보 손실을 고려하여 VoIP 통신에 대해 정확한 원격 ASCA 공격을 수행할 수 있습니까?

[연구 효과] ★

(1) 키보드의 ASC 공격에 대해 selfattention 레이어를 갖춘 딥러닝 모델을 배포하는 새로운 기술을 최초로 제안합니다.

(2) 키보드에 대한 실용적인 딥러닝 기반 어쿠스틱 사이드 채널 공격을 제안하고 구현한다. 우리는 처음으로 키보드에 대한 공격에서 self-attention 변환기 레이어를 사용했습니다.

(3) 실제 공격 시나리오에서 설계된 공격을 평가했습니다. 공격자와 같은 방에 있는 노트북 키보드(모바일 장치를 통해) 및 Zoom 통화를 통한 노트북 키 입력. 우리는 실험을 수행하고 여러 평가를 실행했으며 결과는 이전 작업의 결과보다 뛰어납니다.

[research]

발산 기반 sca 최초 논문 \_[11]

nsa 음향 방출 -compromise침해 의 원인 \_[24]

화상회의, voip 통화에서 가로채는 키입력 \_ [8]

스마트 워치를 공격 벡터로 삼기도 함 \_[20]

★HMM(은닉 마르코프 모델) 시퀀스 위치에서 가장 가능성이 높은 단어나 문자를 예측하기 위해 텍스트 모음에 대해 훈련된 모델

\_ 한국어로 훈련된 모델이 있는지 확인해야 함

* 조금 더 자세히 HMM에 대해 알아볼 필요가 있음

1) 일련의 클래스에서 가능성있는 문자를 생성

2) 첫번째의 과정에서 나온 결과의 문법과 철자를 수정함(HMM 사용)

많은 문헌에서 신경망이 키 입력 인식을 수행할 때 좋은 모델로 인식되지 않음

여러 문헌에서 신경망이 최종 모델이 아니었음

//Transformers는 Vaswani et al.에 의해 2018년에 발명되었습니다. [33], 이 논문은 키보드에 대한 ASC 공격에 대해 self-attention 레이어를 갖춘 신경망을 처음으로 사용한 것입니다.

다양한 키보드에 대한 조사

- 플라스틱 키보드(ATM 키패드, 유선 전화기, 노트북 키보드)

- 현대적인 키보드

★ 조사된 문헌 중 [6]과 [8]은 전체 노트북 키보드에서 ASCA를 다룬 유일한 2개의 논문, 실제 구현과 관련하여 가장 유망한 연구

[8] Skype와 노트북에 내장된 마이크를 통해 키 입력을 수집하는 반면, [6]은 피해자의 컴퓨터 근처에 있는 휴대폰을 사용합니다. 또한 [8]에서는 k-NN 클러스터링과 로지스틱 회귀 분류기를 사용하고 [6]에서는 SVM(지원 벡터 머신)을 활용합니다.

- 어떤 방식으로 키 입력을 수집해야 할 지 정해야 함