Side Channel Attacks

https://youtu.be/v6_e0IL8sB4

부채널 공격?

- 암호학적 측면에서 알고리즘의 약점을 찾거나 무차별 공격을 하는 대신, 암호체계의 **물리적인 구현 과정의 정보를 기반**으로 하는 공격

- 디바이스 내의 보안 모듈이 구동되면서 발생하는 다양한 정보를 획득, 가공, 분석하여 보안 모듈의 암호키를 크래킹하는 공격

부채널 공격?

디바이스 훼손 여부	종류
비침투형 공격(non-invasive attack)	• **전력 분석 공격(power analysis)** • **비침투형 전자파 분석 공격** • 전압 가변 방식의 오류 주입 • 클럭 가변 방식의 오류 주입
(준)침투형공격 ((semi)-invasivce attack)	• **레이저 오류 주입(fault injection)** • 강한 EM 방사를 통한 오류 주입

암호에 대한 공격자의 능력에 따른 모델 분류

- **블랙박스 공격**
- **그레이박스 공격** (부채널 공격)
- **화이트박스 공격**

암호에 대한 공격자의 능력에 따른 모델 분류

- **블랙박스 공격**
  - 공격자는 연산이 일어나는 도중 **연산 장치 내부 정보 관찰 x**
  - 알고리즘의 **입력문과 출력문만 관찰 가능**
  - 선택평문 공격(CPA), 선택암호문 공격(CCA) 등이 있음
  - 대응 방안 : 이론적 안전성을 고려하여 암호를 설계

암호에 대한 공격자의 능력에 따른 모델 분류

- **그레이박스 공격**
  - 공격자가 **블록박스 모델에서 획득할 수 있는 정보+부채널 정보** 추가적으로 접근 가능
  - **연산 시간, 전력 소비량, 자기장** 등을 추가적으로 확인 가능
  - 공격자는 암호 연산 수행에 대한 부가 정보를 활용하여 공격
  - 대응 방법 : 내부 연산 구조를 랜덤화
    - 마스킹 및 하이딩 , N차 부채널 안전성
      - 마스킹 및 하이딩? 연산 중간 처리값을 랜덤화 , 연산시 소모 전력량을 랜덤화

암호에 대한 공격자의 능력에 따른 모델 분류

- **화이트박스 공격**
  - 공격자에게 **가장 많은 능력을 부여**하는 모델
  - SW 실행시 연산이 이루어지는 장비의 **모든 계산 과정 관찰 & 메모리에 대한 접근과 변경 허용** 추가적으로 확인 가능

CPA(선택평문 공격)

- 평문을 선택하면 대응하는 암호문을 얻을 수 있는 상황에서의 공격
- 공격자가 한꺼번에 선택한 평문들에 대한 암호문이 주어진다는 가정 하에 복호화 키를 찾는 공격
- 종류? 적응적 선택 평문 공격, 차분 공격
  - 적응적 선택 평문 공격
    - 공격자는 공격하면서 원하는 평문과 암호문 쌍을 계속 얻을 수 있음.
    - 공격자의 능력이 크다
  - 차분 공격
    - 치환이 약하게 설계되었을 경우, 키의 XOR 여부와 관계없이 차분은 유지된다는 성질 이용
      - ✓ 키를 전수조사보다 효과적으로 유추 가능

CCA(선택암호문 공격)

- 임의로 선택된 암호문과 일치하는 평문으로부터 암호키를 알아내기 위해 시도하는 공격
- 공개키 암호 방식에서 응용됨.
- 적응형과 미적응형으로 분류
  - 적응형
    - 공격자는 이전 암호 해독의 결과를 사용,
    - 암호문을 선택할 수 있는 정보 제공
  - 미적응형
    - 공격자는 결과를 보지 않고 해독할 암호문 선택 가능
    - 공격자는 평문을 본후, 추가 암호문 해독 불가 :

부채널 공격 기법

기법	설명
소요 시간 분석	다양한 계산을 하는데 소요되는 시간측정 기반
전력 모니터링 공격	연산 중 HW가 소비하는 전력변화 측정 기반
전자기파 공격	HW 외부로 방출되는 전자기파를 측정, 해독하여 정보 획득
음성 암호 해독	연산 중 HW가 생성한 음향 측정 후 악용
차분 오류 분석	계산 과정에서 오류를 의도적으로 끼워넣어 암호를 빼냄
잔존 데이터	삭제된 것으로 추정되는 데이터 읽어냄
로우해머 공격	접근 허락되지 않은 메모리 영역 강제로 수정

전력/전자파 분석 공격

- 가장 대표적인 부채널 공격
- 디바이스의 전자파 방사를 측정하여 암호키를 해킹하는 공격
- 단순 전력/전자파 분석 공격(SPA, SEMA) , 차분 전력/전자파 분석 공격(DPA, DEMA)
- 1999년 DES가 공격된 후, 현대 암호 시스템을 위협하는 가장 강력한 공격수단으로 연구 됨
- 거의 모든 암호 알고리즘 공격 가능
- 스마트 디바이스로 공격 대상으로 확대될 것으로 예상 됨

시간차 분석 부채널 공격

- 암호화를 구동하는 데 걸리는 시간을 측정하고 분석하여 암호를 해독하는 방식

- 멜트다운과 스펙터에 여기에 해당

  - 멜트다운
    - 인텔 CPU에 적용된 '비순차적 명령어 처리' 기술의 버그를 악용한 보안 취약점,
    - 보안을 위해 응용 프로그램이 CPU의 캐시 메모리에 접근하지 못했던 기존 HW보안 구조가 통째로 무너짐
  - 스펙터
    - CPU 속에 담겨있는 수많은 명령어에서 일어나는 버그를 악용한 취약점
    - 해킹 프로그램이 다른 응용프로그램이 담긴 메모리 내부 구조를 들여다 볼 수 있음.

- 시간차 노이즈를 암호화 과정에 추가하는 등의 공격의 위험성을 줄이기 위한 노력을 하고 있음

타자 소리를 해킹하는 음향 부채널 공격

- 공격대상이 비밀번호를 입력하는 소리를 듣고 암호키 획득
- 스마트폰조차 활용되어 공격 가능할 수 있음.
- 정교한 머신러닝 모델이 필요하여 키를 누르는 것과 다른 키를 구별할 수 있는 충분한 훈련 데이터 필요

Q & A