암호 공격 유형

김상원

https://youtu.be/edXE0599FEc

암호 역사

암호 공격 기법

암호 공격 유형

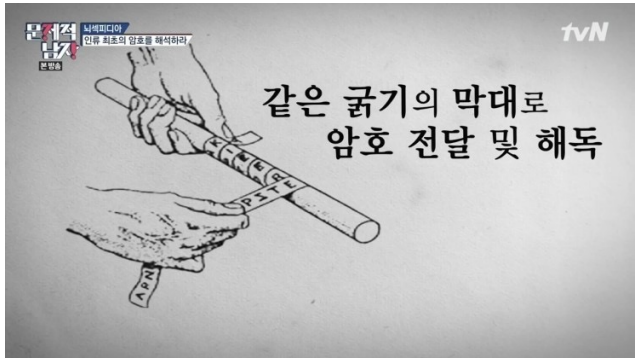
Q & A

암호 역사

- 고대 문명 시대
  - 스키테일
- 중세 시대
  - 비즈네르
- 현대 시대
  - 에니그마

스키테일

1. 전쟁터에 나갈 군대와 본국에 남아있는 정부는 각자, 스키테일(Scytale)이라고 하는 굵기의 원통형 막대기를 나누어 갖는다.
2. 비밀리에 보내야 할 메시지가 생기면, 본국 정부의 암호 담당자는 스키테일에 가느다란 양피지 리본을 위에서 아래로 감은 다음 옆으로 메시지를 적는다.
3. 리본을 풀어내어 펼치면 메시지의 내용은 아무나 읽을 수 없게 된다..
4. 전쟁터에 나가 있는 오로지 같은 굵기의 원통막대기를 가진 사람만이 메시지를 읽을 수 있다.



암호 공격 기법

- 능동적 공격
  - 능동적 공격은 공격자가 시스템에 직접적으로 영향을 주면서 암호 키를 추출하거나 시스템을 악용하는 공격
- 수동적 공격
  - 공격자가 시스템에 직접적인 영향을 주지 않고 존재하는 정보만을 관찰하는 공격

암호 공격 기법

구분	능동적 공격	수동적 공격
공격 방식	시스템 영향	시스템 관찰
공격 목표	암호 키 추출, 시스템 악용	암호 키 추출, 정보 획득
공격 예시	중간자 공격, 재생성 공격, 서비스 거부 공격	사용자 인증 정보 도청, 네트워크 트래픽 분석, 부 채널 공격
탐지 난이도	높음	낮음
방어 방법	암호 시스템 설계 및 운영 정보 보호, 엄격한 접근 제어	암호화 알고리즘 강화, 네트워크 보안 강화

능동적 공격

- 중간자 공격(man in the middle attack, MITM)
  - 합법적인 사용자와 서버 사이에 가입하여 통신 내용을 도청하고 변조하는 공격
- 재전송 공격(reply attack)
  - 암호화된 정보를 캡처하여 나중에 원하는 시점에 재전송하는 공격
- 서비스 거부 공격(denial-of-service attack, DoS attack)
  - 시스템에 과도한 트래픽을 생성하여 시스템을 마비시키는 공격

수동적 공격

- 사용자 인증 정보 도청
  - 공공 Wi-Fi 네트워크를 통해 사용자의 로그인 정보를 엿보는 공격
- 네트워크 트래픽 분석
  - 암호화된 통신 패킷을 분석하여 암호 알고리즘의 취약점을 찾는 공격
- 부 채널 공격(side channel attack)
  - 암호화 과정에서 발생하는 부수적인 정보 (예: 처리 시간, 전력 소비량)를 분석하여 암호 키를 추출하는 공격

암호 공격 유형

- 암호문 단독공격(Cipher text Only Attack, COA)
  - 도청된 암호문만 가지고 해독하려는 공격
- 기지 평문 공격(Known Plain text Attack, KPA)
  - 공격자가 사전에 알고 있는 평문과 그에 대한 암호문을 이용하여 암호 키를 추출하는 공격
- 선택 평문 공격(Chosen Plain text Attack, CPA)
  - 공격자가 원하는 평문을 암호화하여 얻은 암호문을 분석하여 암호 키를 추출하는 공격
- 선택 암호문 공격(Chosen Cipher text Attack, CCA)
  - 공격자가 원하는 암호문을 만들어 암호 시스템에 전송하여 암호 키를 추출하거나 시스템을 악용하는 공격

암호 공격 유형

공격 유형	공격자의 지식
암호문 단독공격 (Cipher text Only Attack, COA)	암호문만 알고 있음
기지 평문 공격 (Known Plain text Attack, KPA)	몇 쌍의 평문과 암호문을 알고 있음
선택 평문 공격 (Chosen Plain text Attack, CPA)	임의의 평문을 선택하여 암호문을 얻을 수 있음
선택 암호문 공격 (Chosen Cipher text Attack, CCA)	임의의 암호문을 선택하여 평문을 얻거나 변조할 수 있음

암호문 단독공격(Cipher text Only Attack, COA)

- 도청자가 알고리즘을 알고 있고, 암호문을 가로챌 수 있다는 가정 하에 도청자가 어떤 암호문을 얻어서 대응되는 평문과 키를 찾는 공격
- 공격자가 가장 적은 정보를 가지고 공격

기지 평문 공격(Known Plain text Attack, KPA)

- 공격자가 평문과 평문을 암호화한 암호문을 모두 알고 있을 때 사용할 수 있는 암호해독 기법
- '기지'(旣知) 란 "이미 알고 있다"는 뜻으로서, 기지 평문 공격은 알려진 평문 공격이라 하고, 암호학에서 기지 평문 공격은 공격자가 평문과 그를 암호화한 암호문을 모두 알고 있을 때 사용할 수 있는 암호 해독 기법들을 말함

기지 평문 공격(Known Plain text Attack, KPA)

- 이미 알고 있는 평문을 크립(crib)이라고 부름
- 크립이라는 용어는 제2차 세계 대전 당시 암호 해독 실인 블레츨리 파크(Bletchley Park)에서 유래
- 암호문 안에 이미 알고 있는 평문이 포함되어 있다면, 그 사실이 암호문과 평문 사이의 관계를 추정하기 위한 단서가 될 수 있음
- AES 등의 현대 암호체계는 기지 평문 공격의 영향을 받지 않는 것으로 알려짐

선택 평문 공격(Chosen Plain text Attack, CPA)

- 평문을 선택하면 대응하는 암호문을 얻을 수 있는 상황에서의 공격
- 공격자가 한꺼번에 선택한 평문들에 대한 암호문이 주어진다는 가정하에 복호화 키를 찾는 공격
- 공격자가 암호장치에 얼마든지 접근할 수 있어서 선택된 평문을 입력하고 그에 대한 암호문을 얻을 수 있는 상황에서 복호화 키를 찾아내거나 선택된 암호문에 대한 평문을 찾아내고자 함

선택 평문 공격(Chosen Plain text Attack, CPA)

- 암호 알고리즘이 하드웨어로 구현되어 있고 키는 내부에 내장된 암호장치를 공격자가 가지고 있다고 가정 시, 공격자는 원하는 만큼 선택한 평문을 입력시켜보고 그에 대한 암호문을 얻을 수 있음
- 공개키 암호 알고리즘의 경우 공개키가 알려져 있음으로 공격자는 선택한 어떤 평문도 암호화하여 암호문을 얻을 수 있음

선택 암호문 공격(Chosen Cipher text Attack, CCA)

- 선택 암호문 공격은 암호 분석가가 임의로 선택된 암호문과 일치하는 평문으로부터 암호키를 알아내기 위해 시도하는 공격
- 공개키 암호 방식에서 응용되는 것으로 사설 키가 한번 알려지면 같은 종류의 메시지에서는 모두 복호화하고, 다른 많은 보안 체계는 선택 암호문 공격에 의해 무효가 될 수 있음

Q & A