블록암호의 보안 취약점

송민호

유튜브:https://youtu.be/yag-C03ZUTk

한성대학교 HANSUNG UNIVERSITY

CryptoCraft LAB

NIST IR 8459 문제점 – ECB 모드의 보안 취약점

- ECB는 IV를 사용하지 않고 각 블록을 독립적으로 암호화함
  - 동일한 평문 블록이면 항상 같은 암호문 블록이 만들어져 패턴이 노출되는 문제 발생
  - $C_i = E_k(P_i) \rightarrow P_i = P_j$ 이면 항상 $C_i = C_j$
  - 암호문에서 특정 블록만 교체해도 주변 블록은 그대로 복호화되어 공격자가 평문의 일부를 의도한 값으로 바꿔치기할 수 있는 문제 발생 – 가변성 문제

- ECB 사용 취약 사례
  - Bouncy Castle(CVE-2016-1000344)
    - 일부 기능이 ECB를 허용하여 패턴 노출의 위험이 있어 ECB 지원을 제거함
  - Jenkins(CVE-2017-2598)
    - 비밀값을 ECB로 저장하는데 패턴 노출 및 블록 대치 위험성이 있어 AEAD(AES-GCM/CCM)로 교체함
  - Zoom(CVE-2020-11500)
    - 통화 스트림을 ECB로 암호화하는데 패턴 노출의 위험이 있어 AES-GCM으로 전환함

NIST IR 8459 문제점들 – IV/카운터 블록 생성 오류

- IV/카운터 블록 생성 오류
  - CBC/CFB: IV는 예측 불가능해야 하며 매 메시지마다 새 IV를 사용해야 함
    - IV가 미리 알려지거나 재사용되면 첫 블록 패턴을 통해 평문 추정 가능
  - OFB: IV는 유일해야 하며 이전 키스트림 출력을 IV로 재사용하면 안됨
    - IV가 같으면 같은 키스트림이 만들어져 한 쪽 평문을 통해 다른 쪽 평문 복원 가능
  - CTR: 고유한 카운터 블록을 사용해야함
    - 같은 카운터 블록 사용시 알고 있는 평문으로 나머지 복원 가능

- CBC 취약 사례 – BEAST 공격
  - TLS 1.0에서 CBC모드의 다음 IV를 이전 암호문의 마지막 블록으로 사용함
  - 암호화 전에 IV가 알려져 선택-평문 공격이 가능해짐
  - TLS 1.1에서는 독립적인 IV를 사용하도록 바뀌었으며 TLS 1.2 이후로는 AEAD 사용, TLS 1.3에서는 CBC 모드가 제거됨

NIST IR 8459 문제점들 – 가변성 문제

- 가변성(Malleability) 문제
  - 무결성 없는 모드는 암호문을 조금만 바꿔도 예측 가능한 방식으로 평문이 바뀜

  - ECB - 각 블록을 독립적으로 암호화
    - 블록 바꿔치기로 주변 블록 영향 없이 해당 블록의 평문만 바꿀 수 있음
  - CBC - 체이닝 모드로 첫 블록은 IV로 시작
    - IV 비트를 뒤집으면 P_1 동일 비트가 뒤집힘
    - C_i 비트를 뒤집으면 P_i는 깨지고 P_{i+1} 동일 비트가 뒤집힘
  - CTR/OFB - 키스트림으로 XOR
    - C_i 비트를 뒤집으면 다른 블록 영향 없이 P_i 동일 비트가 뒤집힘

- 무결성 없는 모드는 전부 가변적이므로 AEAD(AES-GCM/CCM)같이 무결성까지 검증하는 모드 사용을 권고함

NIST IR 8459 문제점들 – 패딩 오라클 공격

- 패딩 오라클 공격
  - CBC 복호화 시 패딩 성공/실패 신호(에러, 타이밍)가 보이면 공격자가 암호문 블록을 조금씩 바꿔 평문을 바이트 단위로 알아낼 수 있는 공격

- 무결성 확보를 위해 CBC+MAC 사용
  - 그러나 여전히 SSL 3.0 / TLS 1.0에서 패딩 오라클 문제(CVE-2003-0078) 발생
  - TLS 1.1/1.2에서 완화책을 넣었지만 Lucky13 공격이 타이밍 차이만으로도 오라클을 악용 가능함을 입증함
  - Lucky 13 공격의 완전 방어는 매우 어렵고 실제로 OpenSSL 패치가 새로운 취약점(CVE-2016-2107)을 유발한 사례도 존재함

- 가능하면 TLS 1.3의 AEAD 사용을 권고함

NIST IR 8459 문제점들 – 대용량 데이터 처리의 한계

- 키당 데이터 한계가 존재함
  - Birthday Paradox로 인해 블록 크기가 n비트인 모드는 같은 키로 처리한 블록 수 σ가 커지면 이론적 안전 보장(IND-CPA)이 무의미해짐. 안전 범위는 $\sigma \ll 2^{n/2}$
  - σ가 커지면 충돌 확률이 높아져 무작위성 가정이 붕괴됨

- 실제 공격 사례
  - 64비트 블록을 사용하는 3DES는 128비트에 비해 임계점이 훨씬 작음
  - Sweet32가 TLS에서 실제 공격으로 입증함

- 운영 대책
  - 키당 데이터 한도를 정해야 함
  - 사용하는 키를 주기적으로 교체해줘야 함
    - AEAD모드를 사용해도 블록 크기 한계는 그대로이기 때문에 키 교체 필수

Q & A