제 9 장
메시지 인증 코드

박 종 혁 교수

Tel: 970-6702

Email: jhpark1@seoultech.ac.kr

제1절 메시지 인증 코드

1.1 올바른 송금 의뢰

- 앨리스: 은행 A의 고객
- 밥: 은행 B의 고객
- A은행에 앨리스로부터 송금 의뢰가 도착

내용:

"내 계좌 앨리스-5374에서 B은행의 계좌 밥-6671로 1억 원을 송금바랍니다"

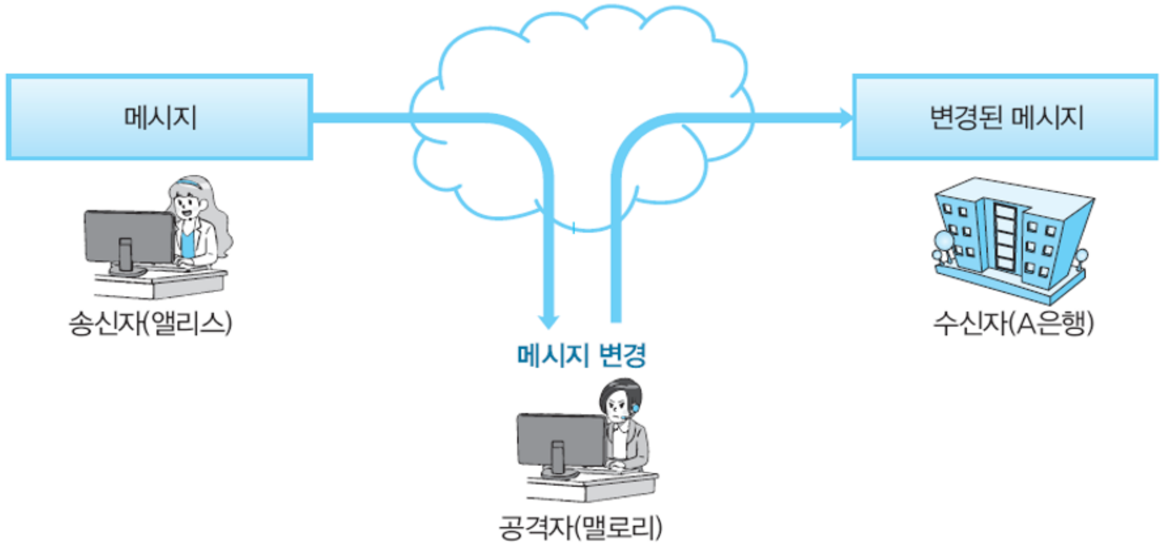
A 은행이 해야 할 일

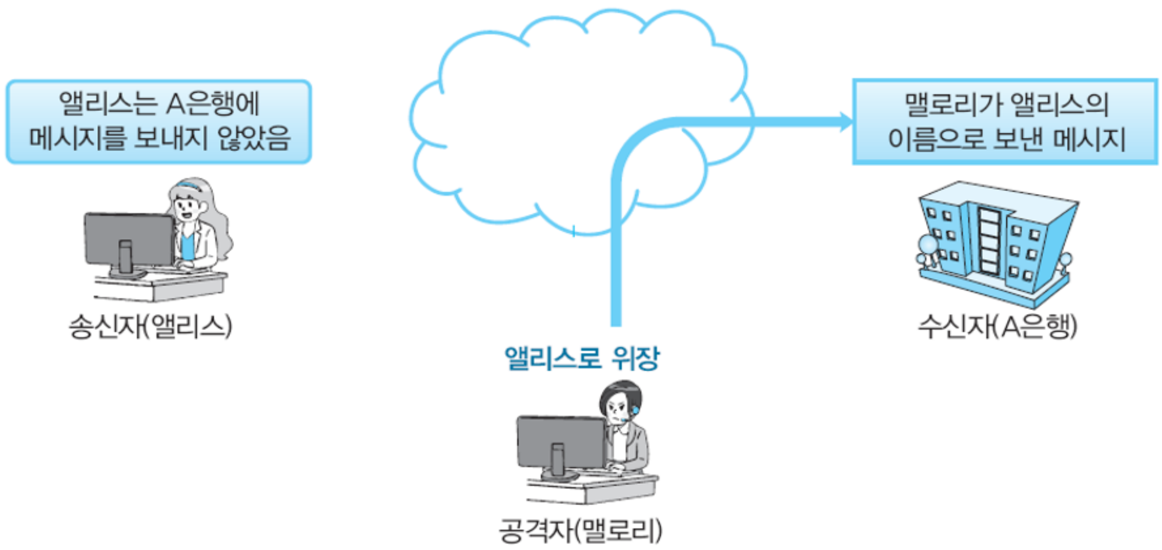
- 메시지 출처: 인증
- 통신 중 내용 변경 유무: 무결성

메시지 인증

- 메시지 인증(authentication)이란,「메시지가 올바른 송신자로부터 온 것이다」라는 성질

무결성과 인증에 대한 위협





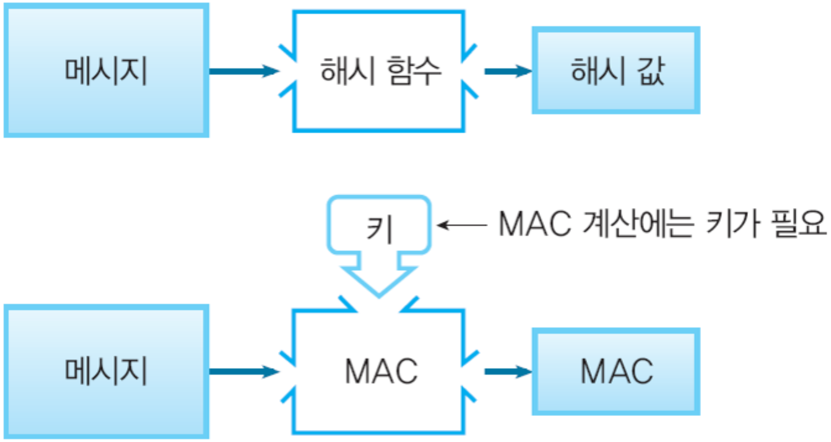
1.2 메시지 인증 코드란?

- 메시지 인증 코드(message authentication code)란, 무결성을 확인하고, 메시지에 대한 인증을 위한 코드
- 첫 글자를 따서 MAC이라 한다
- 입력: 메시지, 공유하는 키
- 출력: 고정 비트 길이의 코드

일방향 해시와 메시지 인증 코드

- 일방향 해시: 키를 사용하지 않는다
- 메시지 인증 코드: 키를 사용

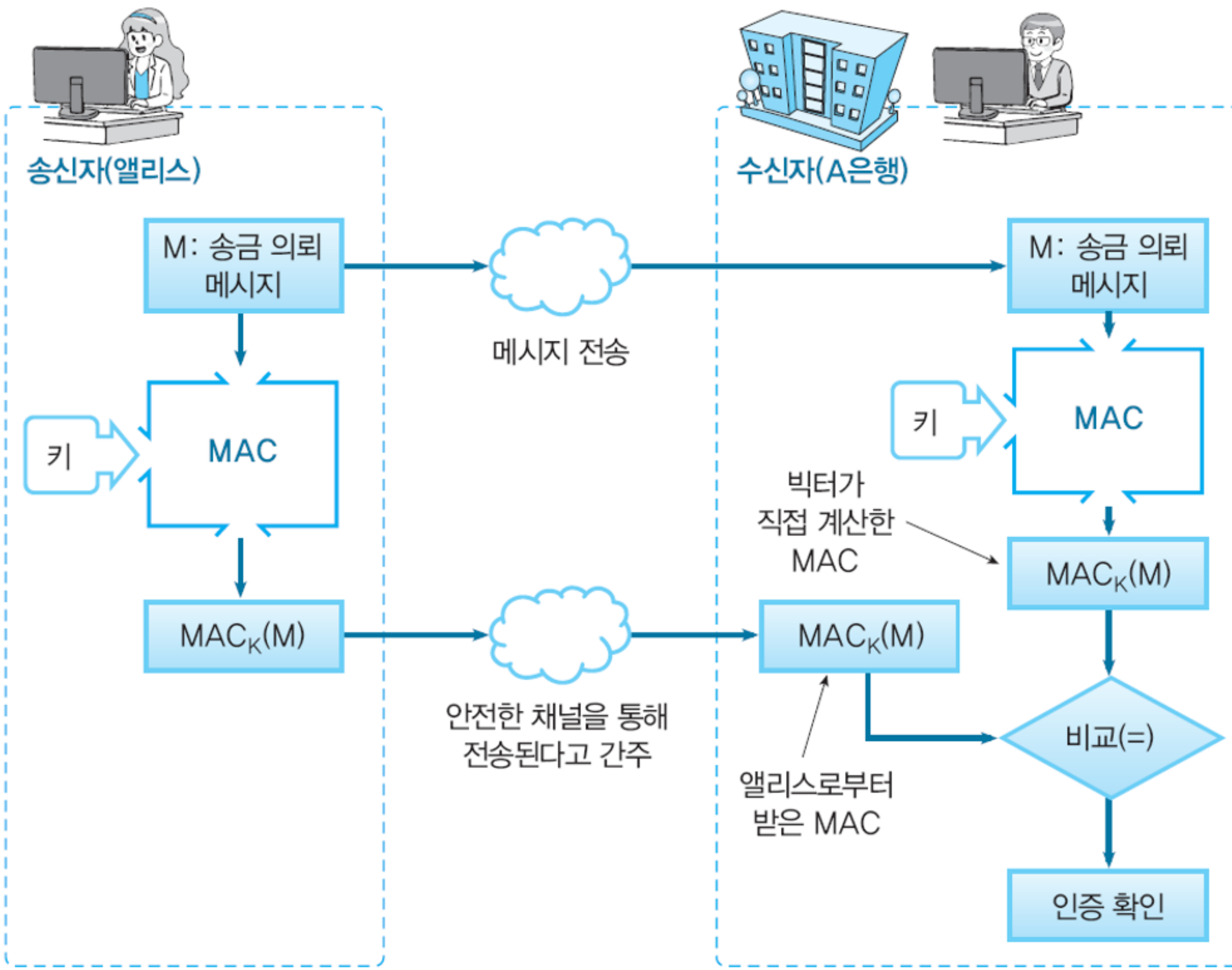
일방향 해시 함수와 메시지 인증 코드의 비교



1.3 메시지 인증 코드의 이용 순서

1) 앨리스와 수신자 A은행: 사전에 키(K) 공유
2) 앨리스: 송금 의뢰 메시지(M) 작성 MAC 값(MAC_K(M))을 계산
3) 앨리스: 수신자 A은행으로 송금 의뢰 메시지와 MAC 값을 전송
4) 수신자 A은행: 수신한 송금 의뢰 메시지를 기초로 해서 MAC 값을 계산
5) 수신자 A은행: 앨리스로부터 수신한 MAC 값과 자신이 계산한 MAC 값을 비교
6) 수신자 A은행:
   - 인증성공: 2개의 MAC 값이 동일하면 송금 의뢰가 틀림없이 앨리스로부터 온 것이라고 판단
   - 인증실패: 2개의 MAC 값이 동일하지 않으면 앨리스로부터 온 것이 아니라고 판단

메시지 인증 코드의 이용 순서



1.4 메시지 인증 코드의 키 배송 문제

- 대칭 암호 때의「키 배송 문제」와 같은 문제가 메시지 인증 코드에도 발생
- 키 배송 문제를 해결
  - 공개 키 암호
  - Diffie-Hellman 키 교환
  - 키 배포 센터
  - 키를 안전한 방법으로 별도로 보내기

제2절 메시지 인증 코드 이용 예

2.1 SWIFT

2.2 Ipsec

2.3 SSL/TLS

2.1 SWIFT

- SWIFT는 Society for Worldwide Internet Financial Telecommunication(국제은행간 통신협회)
- 은행과 은행은 SWIFT를 통해서 거래 메시지 교환
- 메시지 인증 코드를 사용

2.2 Ipsec

- 인터넷 기반의 통신 프로토콜인 IP (Internet Protocol)에 보안 기능을 첨가한 것

- 통신 내용 인증과 무결성을 위해 메시지 인증 코드를 이용

2.3 SSL/TLS

- 웹에서 온라인 쇼핑을 할 때 사용되는 통신 프로토콜
- 통신 내용의 인증과 무결성 확인을 위해 메시지 인증 코드를 이용

제3절 메시지 인증 코드의 실현 방법

3.1 일방향 해시 함수를 이용한 실현

3.2 블록 암호를 이용한 실현

3.3 그 밖의 방법으로 실현

3.1 일방향 해시 함수를 이용한 실현

- SHA-1나 MD5와 같은 일방향 해시 함수를 이용하여 메시지 인증 코드를 실현

- HMAC

3.2 블록 암호를 이용한 실현

- **트리플 DES나 AES와 같은 블록 암호를 사용해서 메시지 인증 코드를 실현**
  - 블록 암호 키를 메시지 인증 코드의 공유키로 사용
  - CBC 모드로 메시지 전체를 암호화
  - 메시지 인증 코드에서는 복호화를 할 필요가 없으므로 최종 블록 이외는 폐기
  - 최종 블록을 MAC 값으로 이용

3.3 그 밖의 방법으로 실현

- 스트림 암호
- 공개 키 암호

인증 암호

- 인증 암호(AE혹은 AEAD)
  - AE: Authenticated Encryption
  - AEAD: Authenticated Encryption with Associated Data
  - 2000년 이후 연구 진행
  - 대칭 암호와 메시지 인증 코드를 조합하여 기밀성・무결성・인증을 동시에 충족시키는 구조

- Encrypt-then-MAC
- Encrypt-and-MAC
- MAC-then-Encrypt

Encrypt-then-MAC

- 평문을 대칭 암호로 암호화한 후 암호문의 MAC 값을 계산
- 메시지 인증 코드 입력에 암호문을 부여

- 2 개의 키 사용
  - 우선 메시지를 암호화하여 암호문 $C = E(K_2, M)$를 생성
  - 다음에 T=MAC(K_1, C)로 암호문을 인증하여 쌍 (C, T)를 생성

- 선택 암호문 공격을 막을 수 있음
- 예) Ipsec 프로토콜에서 사용됨

Encrypt-and-MAC

- 평문을 대칭 암호로 암호화하고, 그와는 별도로 평문의 MAC 값을 얻는 방법

- 2 개의 키 사용
  - 메시지를 암호화하여 암호문 $C = E(K_2, M)$을 생성
  - 평문을 T=MAC(K_1, M)으로 인증하고 쌍 (C, T)를 생성
  - 이 연산들은 어떤 순서로도 수행될 수 있음

- 예) SSH 프로토콜에서 사용됨

MAC-then-Encrypt

- 미리 평문의 MAC 값을 얻고, 평문과 MAC 값 양쪽을 정리하여 대칭 암호로 암호화하는 방법

- 2 개의 키 사용
  - 우선 MAC값을 T = MAC(K_1, M)으로 계산 [평문 인증]
  - 다음에 메시지와 태그를 암호화: $E(K_2, (M \| T))$

- 예) SSL/TLS 프로토콜에서 채택

4.1 GCM과 GMAC

- GCM(Galois/Counter Mode)
  - 인증 모드의 일종
  - AES와 같은 128비트 블록 암호를 CTR 모드로 이용하여 MAC 값을 얻기 위하여 덧셈과 곱셈을 반복하는 해시 함수를 사용
  - CTR 모드는 1씩 늘어가는 숫자를 암호화하기 때문에 각 블록을 병렬 처리하여 실행속도를 높일 수가 있음
  - CTR 모드와 MAC 값 생성에 공통 키를 사용하기 때문에 키 관리도 편리

- GMAC(Galois/Counter Mode MAC)
  - GCM을 메시지 인증 코드 전용으로 사용

제5절 HMAC

5.1 HMAC이란?

5.2 HMAC의 순서

5.1 HMAC이란?

- HMAC은 일방향 해시 함수를 이용하여 메시지 인증 코드를 구성하는 방법 (RFC2104)
- HMAC의 일방향 해시 함수는 모듈형으로 골라서 사용
  - HMAC-SHA1: SHA-1
  - HMAC-SHA224: SHA-224
  - HMAC-SHA256: SHA-256
  - HMAC-SHA384: SHA-384
  - HMAC-SHA512: SHA-512
- SHA-3 KECCAK을 사용해 HMAC 작성 가능

RFC2104 정의

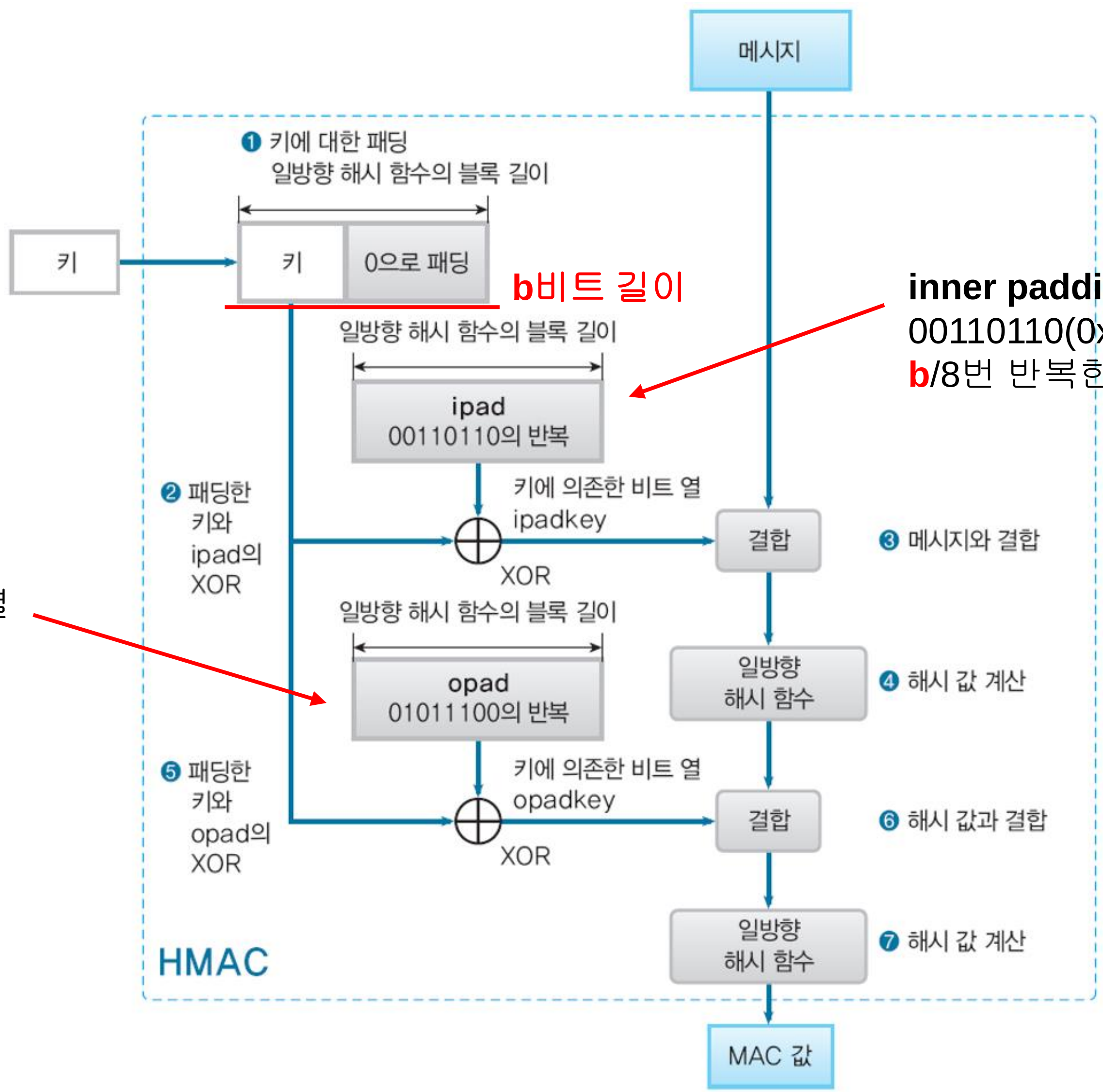
$$HMAC(K, m) = H\big((K' \oplus opad) \,||\, H\,(\,(K' \oplus ipad) \,||\, m)\big)$$

$$K' \begin{cases} H(K) & K \textit{ is larger than block size} \\ K & \textit{otherwise} \end{cases}$$

5.2 HMAC의 순서

1) 키 패딩
2) 패딩한 키와 ipad의 XOR
3) 메시지 결합
4) 해시 값의 계산
5) 패딩한 키와 opad의 XOR
6) 해시 값과의 결합
7) 해시 값의 계산

일방향 해시 함수를 사용한 메시지 인증 코드의 예(HMAC)



inner padding
00110110(0x36)을
b/8번 반복한 2진 수열

outer padding
01011100(0x5C)을
b/8번 반복한 2진 수열

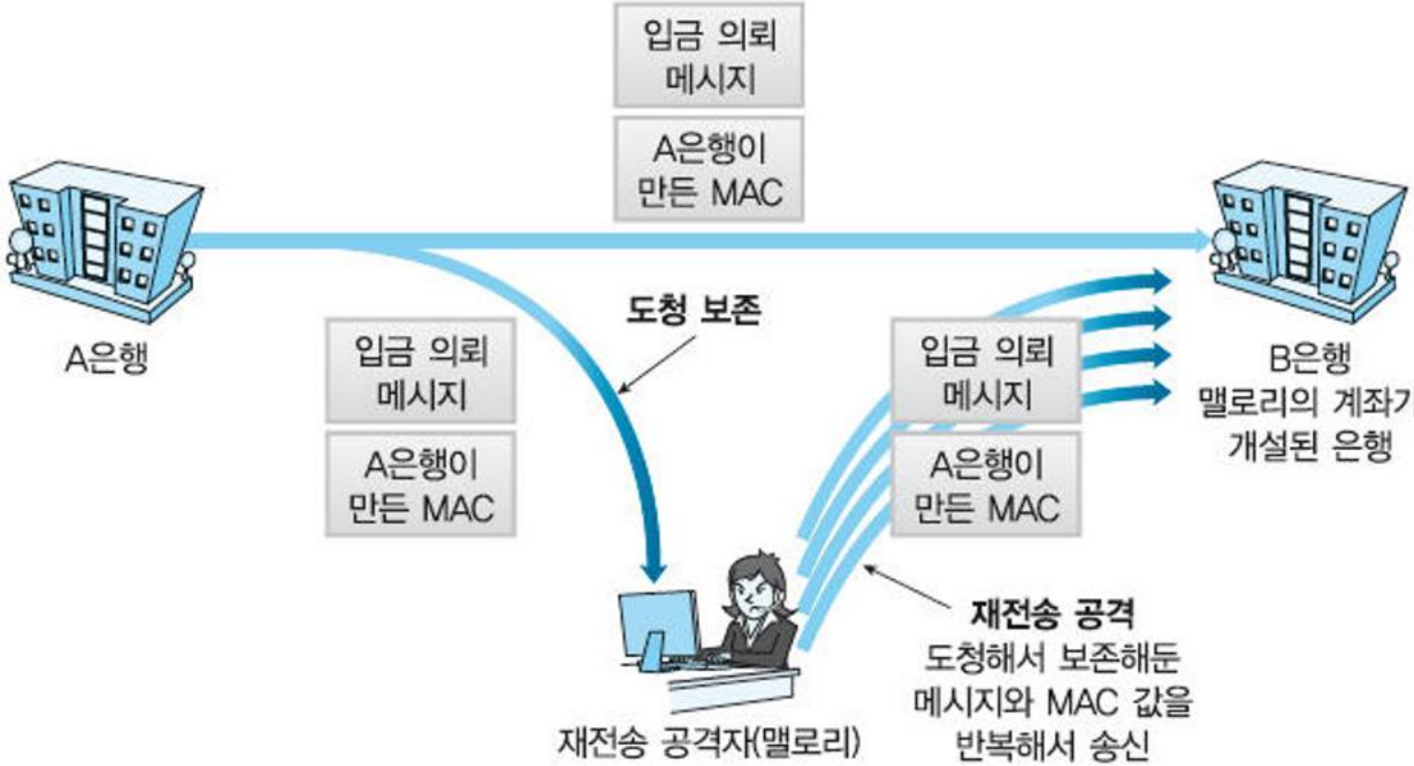
제6절 메시지 인증 코드에 대한 공격

6.1 재전송 공격

6.2 키의 추측에 의한 공격

6.1 재전송 공격

- 재전송(replay)공격
  - 보존해 둔 정당한 MAC 값을 반복해서 송신하는 공격



재전송 공격의 예

1) 맬로리는 A은행과 B은행의 통신을 도청하고 있다.

2) 맬로리는 A은행에 가서 B은행에 있는 자신의 계좌 M-2653으로 100만원을 입금한다. 그러면 A은행은 다음과 같은 입금 의뢰 메시지를 만든다.
   「계좌 M-2653으로 100만원을 입금하라」
   A은행은 이 입금 의뢰 메시지의 바른 MAC 값을 계산하여 그것을 메시지에 부가해서 B은행에 보낸다.

3) B은행은 받은 메시지를 기초로 MAC 값의 계산을 행하고, 그 계산 결과와 보내 온 MAC 값을 비교한다. 그리고 2개의 MAC 값이 같다는 것으로부터 A은행에서 온 메시지는 올바른 입금 의뢰라고 판단하고, 맬로리의 계좌 M-2653으로 100만원을 입금한다.

재전송 공격의 예

4) 맬로리는 A은행에서 B은행으로 보내진 입금 의뢰 메시지와 MAC 값을 도청하여 자신의 컴퓨터에 보존한다.

5) 맬로리는 보존해 둔 입금 의뢰 메시지와 MAC 값을 한 번 더 B은행에 보낸다.

6) B은행은 받은 메시지를 기초로 MAC 값의 계산을 행하고, 그 계산 결과와 보내 온 MAC 값을 비교한다. 그리고 2개의 MAC 값이 같다는 것으로부터 이 메시지는 A은행에서 온 올바른 입금 의뢰라고 판단(오해)하고, 맬로리의 계좌 M-2653에 100만 원을 입금해 버린다.

7) 맬로리는 (5)를 100번 반복한다.

8) B은행은 (6)을 100번 반복해 버린다.

9) 맬로리는 B은행의 자신의 계좌에 100만원 × 100 = 1억원이 입금되면 바로 인출한다.

재전송 공격 방어

- 순서 번호(sequence number)
  - 송신 메시지에 매회 1씩 증가하는 번호(순서 번호, sequence number)를 붙이기
  - 마지막 통신시 순서번호를 저장
- 타임스탬프(timestamp)
  - 송신 메시지에 현재 시각 넣기
  - 송수신자 사이의 동기화 필요
- 비표(nonce)
  - 송신자가 일회용의 랜덤한 값을 전송
  - 메시지와 비표를 합해 MAC 값을 계산
  - 비표 값은 통신 때마다 교체

6.2 키의 추측에 의한 공격

- 메시지 인증 코드에 대한 공격
  - 전사공격
  - 생일 공격
- MAC 값만 획득한 공격자가 키를 추측하지 못하도록 해야 한다
  - 해시 함수의 일방향성
  - 해시 함수의 충돌내성
  - 키 생성에 의사난수 생성기 사용

제7절 메시지 인증 코드로 해결할 수 없는 문제

7.1 제 3자에 대한 증명

7.2 부인방지

7.1 제 3자에 대한 증명

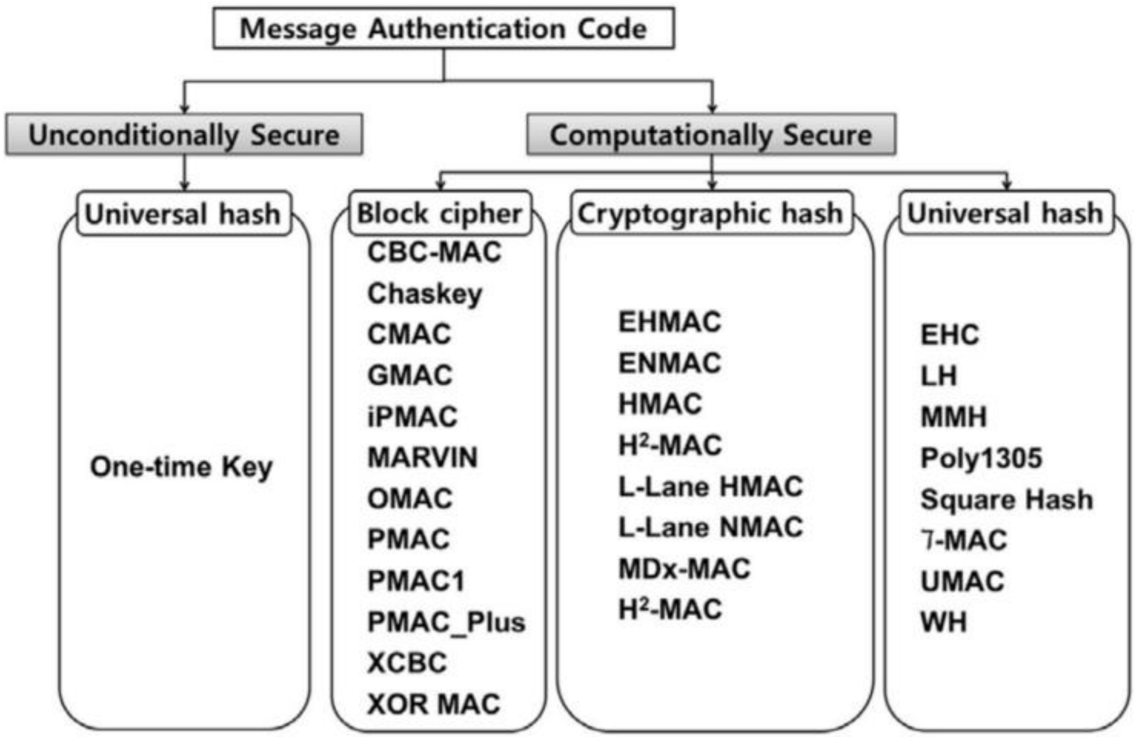
- 앨리스로부터 메시지를 받은 밥이 「이 메시지는 앨리스가 보낸 것이다」라는 것을 제삼자인 검증자 빅터에게 증명할 수 없다

- 이유:
  - 일단 키를 빅터에게 알려줘야 한다
  - 앨리스와 밥 모두가 키를 가지고 있으므로 둘 중 누가 작성했는지 말할 수 없다

7.2 부인 방지

- 밥이 MAC 값이 딸린 메시지를 받았고, 「이 메시지는 앨리스로부터 온 것이다」라는 걸 확실히 알 수 있다
- 하지만 앨리스가 전송 자체를 부정할 경우 제3자에게 이 사실을 증명할 수 없다
- 앨리스의 송신자체에 대한 부정을 부인 (repudiation)이라고 한다
- 메시지 인증 코드로는 부인 방지(nonrepudiation)를 할 방법이 없다

기타 – MAC 알고리즘 분류



연습문제 풀이

연습문제

1. 메시지 인증 코드를 사용해서 막을 수 있는 공격 유형으로 묶인 것은?

① 무결성 침해와 위장

② 기밀성 침해와 위장

③ 부인과 기밀성 침해

④ 무결성 침해와 부인

⑤ 무결성 침해와 기밀성 침해

연습문제

2. 메시지 인증 코드라고 알려진 기술에서는 메시지에 붙여지는 작은 데이터 블록을 생성하기 위해 __________을(를) 이용하는 방법이다.

① 패스워드

② 스트림 암호

③ 암호 블록

④ 비밀 키

⑤ 초기 값

연습문제

3. 메시지 인증 코드와 해시 함수와의 차이점을 설명한 것으로 맞는 것은?

① 메시지 인증 코드는 입력 값에 따라 출력 비트의 길이가 다르지만 해시 함수는 입력 값에 따라 출력하는 비트의 길이가 같다.

② 메시지 인증 코드에서는 키를 사용하지만 해시 함수에서는 키를 사용하지 않는다.

③ 두 경우 모두 송신자와 수신자가 사전에 정보를 공유하고 있을 필요가 없다.

④ 두 경우 모두 공개 키 암호는 사용할 수 없다

⑤ 차이점이 없고 기술적인 구현 방법만 다르다.

연습문제

4. 메시지 인증 코드와 대칭 암호 시스템이 가지고 있는 공통점으로 올바른 것은?

① 키 배송문제가 해결되어야 한다.

② 해시 함수를 사용해야만 한다.

③ 타임 스탬프가 필요하다.

④ 난수 생성기를 필요로 한다.

⑤ 비표 사용을 해야만 한다.

연습문제

5. 메시지 인증 코드의 실제적인 응용이 아닌 것은?

① SWIFT

② IPSec

③ SSL

④ TLS

⑤ RSA

연습문제

6. 블록 암호 모드를 사용해서 메시지 인증 코드를 실현할 수 있는데 이때 사용되는 모드로 적합한 것은?

① ECB 모드 : Electric CodeBook mode(전자 부호표 모드)

② CFB 모드 : Cipher-FeedBack mode(암호 피드백 모드)

③ CBC 모드 : Control Block Chaining mode(컨트롤 블록 연쇄 모드)

④ OFB 모드 : Output-FeedBack mode(출력 피드백 모드)

⑤ CTR 모드 : CounTeR mode(카운터 모드)

연습문제

7. 대칭 암호와 메시지 인증 코드를 조합하여 기밀성, 무결성, 인증을 동시에 충족시키는 암호로서 2000년대 이후에 연구가 진행되고 있는 암호는 무엇인가?

① 인증 암호

② 스트림 암호

③ 일회용 암호

④ 갈로아 암호

⑤ 블록 암호

연습문제

8. AES와 같은 128비트 블록암호를 CTR 모드로 활용하여 MAC 값을 구하기 위해 덧셈과 곱셈을 반복하는 해시 함수를 사용하는 모드는 무엇인가?

① MAC

② GCM

③ HMAC

④ HMAC-MD5

⑤ HMAC-RIPEMD

연습문제

9. 메시지 인증 코드를 깨지 않고도 메시지 인증 코드에 대한 공격을 할 수 있는데, 사용자의 바른 MAC 값을 단지 보존해 놓고 반복해서 사용하는 공격을 ___________이라고 한다.

① 생일공격

② 중간자 공격

③ 서비스 거부 공격

④ 재전송 공격

⑤ 전사 공격

연습문제

10. 재전송 공격을 막는 방법으로 올바르지 않은 것은?

① 순서번호를 사용한다.

② 타임스탬프를 사용한다.

③ 두 개의 키를 사용한다.

④ 비표를 사용한다.

연습문제

11. HMAC에서는 일방향 해시 함수의 ___________을 이용하여 MAC 값으로부터 키를 추측할 수 없도록 하고 있다.

① 일방향성 및 충돌 내성

② 키를 사용하지 않는 점

③ 빠른 처리 시간의 장점

④ 재전송 공격에 대한 내성

⑤ 키 배송이 필요하지 않은 점

연습문제

12. 메시지 인증 코드만 가지고는 해결 수 없는 암호학적인 문제로만 묶인 것은?

① 키 배송과 부인방지

② 제 3자에게 증명하기와 기밀성

③ 무결성과 키 배송

④ 제 3자에게 증명하기, 부인방지

⑤ 부인방지와 무결성

연습문제

13. 재전송 공격을 막기 위해 사용되는 것으로서 송신자와 수신자가 동기화를 하고 송신 메시지에 현재 시각을 넣어 전송하는 방법을 무엇이라고 하는가?

① 비표

② 타임스탬프

③ 일회용 패드

④ 순서번호

⑤ 해시

연습문제

14. 재전송 공격을 막기 위해 사용되는 것으로서 메시지를 수신하기에 앞서 수신자는 송신자에게 일회용의 랜덤한 값을 건네주고 송신자는 메시지 안에 그 값을 포함해서 MAC 값을 계산한다. 이 때 이 랜덤한 값을 무엇이라고 하는가?

① 비표

② 타임스탬프

③ 일회용 패드

④ 순서번호

⑤ 해시

연습문제

15. 재전송 공격을 막기 위해 사용되는 것으로서 송신 메시지에 매회 1씩 증가하는 번호를 붙이기로 약속하고, 이 번호를 포함하여 MAC 값을 계산하여 매번의 통신에서 MAC 값이 변동하도록 하는 방법이 있는데, 이 값을 무엇이라고 하는가?

① 비표

② 타임스탬프

③ 일회용 패드

④ 순서번호

⑤ 해시

연습문제

16. 앨리스와 밥은 키를 공유하고 있고, 앨리스는 자신이 작성한 메시지와 키를 이용한 그 메시지의 MAC을 밥에게 보낸 뒤에 자신이 그 메시지를 보낸 적이 없다고 주장하였다. 앨리스가 보냈다는 사실을 증명하는 것을 __________(이)라고 한다.

① 인증

② 무결성

③ 기밀성

④ 부인방지

⑤ 정확성

연습문제

17. 메시지 인증 코드를 이용하여 확인 할 수 없는 보안 서비스에 해당되는 것 들로만 묶인 것은?

① 인증, 부인방지

② 무결성, 기밀성

③ 기밀성, 인증

④ 부인방지, 기밀성

⑤ 무결성, 인증

참고문헌

- “네트워크 보안 에센셜 3판”, 윌리엄 스톨링스 저(전태일 등역) , 교보문고
- “Authenticated Encryption and Cryptographic Network Protocols”, David Brumley, Carnegie Mellon University
- “메시지 인증 코드에 대한 연구 동향 분석 및 성능 비교”, 김민우, 권태 경, 정보과학회논문지, 2016.

Q & A

Thanks!