사이버보안개론 중간고사

Introduction to Cybersecurity

학번:
이름:

총점: 30점

- 각 문항의 질문을 읽고 이유를 함께 설명하시오.
- 필요한 경우 수식이나 기호를 활용하여 설명해도 됩니다.

문제 1. Security Concepts and Design Principles (10점)

다음은 대학교의 학생 성적 관리 시스템 (Student Information System)에 관한 사례이다.

대학교는 학생들이 온라인으로 자신의 성적을 조회할 수 있는 시스템을 운영하고 있다. 이 시스템에서는 학생, 교수, 관리자가 각각 다른 권한을 가지고 있다.

어느 날 다음과 같은 상황이 발생하였다.

- **상황 A:** 학생 Alice가 시스템의 취약점을 이용하여 다른 학생 Bob의 성적을 무단으로 조회하였다.
- **상황 B:** Alice가 동일한 취약점을 이용하여 Bob의 성적을 B에서 A+로 변경하였다.

(1) [2점] 상황 A와 B에서 각각 침해된 CIA Triad의 Security Goal이 무엇인지 설명하시오.

(2) [2점] 상황 A와 B를 Active Attack과 Passive Attack의 관점에서 각각 분류하고, 그 이유를 설명하시오.

(3) [3점] 학생 Alice가 다른 학생 Bob의 성적을 조회하거나 변경할 수 없도록 하려면, Alice에게 어떤 권한만 부여해야 하는가? 이와 관련된 Security Design Principle의 이름을 제시하고 설명하시오.

(4) [3점] 학생 성적 관리 시스템을 보다 안전하게 설계하기 위해 적용할 수 있는 Security Design Principle을 두 가지 제시하고, 각각 어떻게 적용할 수 있는지 설명하시오. 단, (3)에서 답한 원칙은 제외한다.

문제 2. Symmetric Encryption and ECB Mode (6점)

Alice는 비밀키 K를 이용하여 여러 개의 Plaintext Block을 암호화하려고 한다.

각 Block은 동일한 크기이며, ECB Mode에서는 다음과 같이 암호화한다.

$$C_i = E_K(P_i)$$

여기서 P_i는 i번째 Plaintext Block, C_i는 Ciphertext Block, E_K는 비밀키 K를 사용하는 Encryption Algorithm이다.

Alice가 다음과 같은 Plaintext Block들을 암호화한다고 하자.

$$\boxed{P_1 = A, \quad P_2 = B, \quad P_3 = A, \quad P_4 = C}$$

단, A, B, C는 서로 다른 동일 크기의 Block이다.

(1) [2점] ECB Mode에서 C_1과 C_3는 어떤 관계를 가지는가? 그 이유를 설명하시오.

(2) [4점] 공격자 Eve가 비밀키 K를 알지 못하고 Ciphertext만 관찰할 수 있다고 하자.

이때 Eve가 Plaintext에 대해 알아낼 수 있는 정보가 있는지 설명하고, 이러한 특징이 Security Problem이 되는 이유를 서술하시오.

문제 3. Message Authentication and Hash Function (6점)

Alice가 Bob에게 메시지 M을 전송하려고 한다.

두 사람은 동일한 Hash Function H를 알고 있으며, 공격자 Eve는 전송 중인 메시지를 관찰하거나 변경할 수 있다.

Alice는 메시지의 무결성(Integrity)을 확인하기 위해 다음과 같이 전송한다.

$$\boxed{M \parallel H(M)}$$

여기서 $\parallel$는 두 값을 연결하는 Concatenation 연산을 의미한다.

(1) [3점] Bob은 수신한 메시지에 대해 Hash Value를 다시 계산하고, 함께 전달받은 Hash Value와 비교한다.

이 방법만으로 공격자에 의한 메시지 변조를 탐지할 수 있는가? 그 이유를 설명하시오.

(2) [3점] Alice와 Bob이 동일한 비밀키 K를 안전하게 공유하고 있다고 하자.

이때 MAC을 사용하면 (1)의 문제를 어떻게 해결할 수 있는지 설명하시오.

문제 4. Public-Key Cryptography and Key Distribution (8점)

Alice와 Bob은 Public-Key Cryptography를 이용하여 안전하게 통신하려고 한다.

두 사람은 각각 다음과 같은 Key Pair를 가지고 있다.

$$\begin{aligned} \text{Alice}: &\quad (PU_A, PR_A) \\ \text{Bob}: &\quad (PU_B, PR_B) \end{aligned}$$

여기서 PU는 Public Key, PR은 Private Key를 의미한다.

(1) [3점] Bob이 Alice에게 비밀 메시지 M을 보내려고 한다.

Bob은 어떤 Key를 이용하여 메시지를 암호화해야 하며, Alice는 어떤 Key를 이용하여 복호화해야 하는지 설명하시오.

(2) [3점] 공격자 Eve가 자신의 Public Key PU_E를 Bob에게 전달하면서 이것이 Alice의 Public Key PU_A라고 주장한다고 하자.

Bob이 이를 믿고 메시지 M을 암호화하여 전송하면 어떤 Security Problem이 발생할 수 있는지 설명하시오.

(3) [2점] (2)에서 발생하는 문제를 방지하기 위해 어떤 방법을 사용할 수 있는지 설명하시오.

— End of Exam —