

정보보호론

2014년 시행 5급(기술) 공채 제2차시험

응시번호 :

성명 :

제 1 문. ISO 27001과 ISO 27002 표준에서 제시하고 있는 위험 관리 체계와 관련하여 다음 물음에 답하시오. (총 12점)

- 1) 위험 규모의 산출 요소인 자산, 위협, 취약성의 개념을 설명하시오. (6점)
- 2) 위험 대처 방안으로 위험 수용, 위험 회피, 위험 전가, 위험 감소가 있다. 각각의 방안을 설명하시오. (6점)

제 2 문. 큰 소수 p 와 $Z_p^*=\{1,2,\dots, p-1\}$ 의 생성원 g 에 대해 두 사용자 A, B가 공개 채널을 통해 비밀키를 공유할 수 있는 Diffie-Hellman 키교환 방식은 아래와 같이 이루어진다. 다음 물음에 답하시오. (총 15점)

- 사용자 A는 $p-1$ 보다 작은 양의 정수 R_A 를 랜덤하게 생성하고 $T_A = g^{R_A} \bmod p$ 를 계산하여 이 T_A 를 사용자 B에게 전송한다.
- 마찬가지로 사용자 B도 $p-1$ 보다 작은 랜덤한 양의 정수 R_B 를 생성, $T_B = g^{R_B} \bmod p$ 를 계산하여 이를 사용자 A에게 전송한다.

- 1) 두 사용자가 상대방에게서 받은 T_A 또는 T_B 를 이용하여 동일한 비밀키 K 를 산출하는 과정을 설명하시오. (6점)
- 2) 상기 키교환 방식은 중간자 공격(man-in-the-middle attack)에 취약한 것으로 알려져 있다. 공격자 C가 두 사용자의 중간에서 교환되는 메시지들을 조작하여 두 사용자가 전혀 눈치 채지 못하는 방식으로 암호문을 도청할 수 있음을 보이시오. (6점)
- 3) 이러한 중간자 공격이 성공할 수 있는 이유를 설명하고, 이를 막기 위한 방안은 무엇인지 기술하시오. (3점)

제 3 문. 서버가 공격받더라도 사용자 패스워드가 공격자에게 노출되지 않도록 서버에는 패스워드를 그대로 보관하지 않는다. 또한 공격자가 쉽게 예측할 수 없는 패스워드를 사용해야만 한다. 다음 물음에 답하시오. (총 11점)

- 1) 관리자조차도 저장된 패스워드 파일로부터 일반 사용자의 패스워드를 식별해 내지 못하도록 패스워드를 서버에 저장하는 방법을 기술하시오. (5점)
- 2) 위 방법으로 패스워드를 저장하더라도 사용자가 사전적 단어를 패스워드로 사용하면 안전하지 않은 이유를 쓰시오. (3점)
- 3) 위 서버에서 솔트(salt)를 이용하면 안전성을 높일 수 있음을 설명하시오. (3점)

제 4 문. TCP SYN flooding 공격과 방어에 대하여 다음 물음에 답하시오. (총 12점)

- 1) TCP 연결을 설정하기 위해 클라이언트와 서버가 주고 받는 메시지를 3단계(TCP 3-way handshake)로 설명하시오. (5점)
- 2) TCP SYN flooding은 대표적인 DoS(서비스 거부) 공격 방법의 하나이다. 이에 대하여 설명하시오. (5점)
- 3) TCP SYN flooding 공격을 막기 위해 SYN Cookie를 이용하는 방법을 설명하시오. (2점)

안전행정부 시험출제과장