정보보안 기말고사 2022. 12. 14 학번: 이름:

※ 시험 시간은 50 분이며, 뒷면에 답을 적어도 됩니다.

1. 다음 물음에 대한 답을 작성하시오. (각 문제 당 4점)

1) 인가에 관련하여 사용자의 권한과 사용자가 수행하고 있는 프로그램의 권한이 서로 다름(예로 앨리스의 권한과 앨리스가 수행하는 컴파일러의 권한이 다름)으로써 발생하는 보안 문제는 무엇인가(보안 문제의 명칭만 기술)?

대리 혼돈

2) 일반적인 인증 프로토콜에서 응답 메시지의 신선함(freshness)를 보장하기 위해 Nonce 값 대신 사용할 수 있는 값(필드)은?

타임 스탬프(Time Stamp)

3) DB 질의 결과 크기에 따라 제어하는 하거나 N-응답, k% 지배 규칙 등은 어떤 보안 문제를 제어하기 위한 방법인가?

추론 제어

4) TCP 순서번호를 이용하는 Convert_TCP 해킹 도구는 정보보안 에서 어떤 방식의 보안문제를 발생시키는가(관련된 보안문제 명칭을 기술)?

은닉 통로

5) 암호학적 해시함수가 갖추어야 할 특성으로 "입력의 작은 변경이 출력에는 큰 변경의 결과로 나타내야 함"을 의미하는 용어는?

쇄도 효과

2. 다음의 설명이 옳은 내용이면 O 표를, 틀린 내용이면 X 표를 하시오. (각 문제 당 맞으면 3점, 틀리면 감점 2점)

1) 인가에서 사용되는 "접근제어목록"이 "권한목록"보다 구현하기 더 어렵다. (X)
2) 생체인식에서 동일 오류율로 생체인식 기법을 판달할 때, 지문인식 시스템이 손의 기하학적인 형태를 이용한 인식 시스템보다 오류율이 더 높다. (O)
3) IPSec 터널 모드에서는 통신 호스트의 주소 정보 등이 노출된다. (X)
4) 불법복사 음악 파일의 유출 경로를 탐지하기 위해서는 약하고 투명한 워터마킹을 디지털 음악에 삽입한다. (X)
5) SSL은 VPN(Virtual Private Network)의 보안 방식으로 많이 사용된다. (X)
6) IPSec의 ESP 헤더는 무결성 기능만 제공한다. (X)
7) IKE 1 단계 공개키 암호화 방식의 적극 모드에서는 사용자의 익명성을 보장하지 못한다. (X)
8) 커베로스 보안 프로토콜은 공개키 기반으로 설계되었다. (X)
9) 비정상 기반(Anomaly-based) IDS 구현을 위해서 통계적 판별 기법이나 인공지능 기법 등이 많이 사용된다.(O)
10) GSM 보안은 재연 공격에 강건하게 설계되었다.(X)

3. 다음 물음에 대한 답을 작성하시오. (각 문제당 5점)

1) 측정된 두 데이터(x, y)의 해밍 거리(Hamming Distance)를 d(x, y)로 정의할 때, $d(11010011_2, 11000010_2)$?

1/4(0.25)

2) 비정상 탐지의 예로, 앨리스가 각 파일 F_n에 대해 기존의 파일 접근비율 H_n이 아래와 같고, 최근 F_n에 대한 접근비율 A_n이 아래와 같을 경우, 비정상 탐지 판별 값 S와 새롭게 갱신된 파일 접근비율 $H_0 \sim H_3$을 구하라. 단 갱신된 파일 접근비율 계산에서 기존 파일 접근 비율을 70% 반영하고, 최근 파일 접근 비율을 30% 반영한다. (두 개의 계산이 모두 맞아야 정답으로 인정하고. 계산 과정도 기술해야 함).

$H_n = \{H_0=0.20, H_1=0.30, H_2=0.30, H_3=0.20\}$
$A_n = \{A_0=0.10, A_1=0.40, A_2=0.45, A_3=0.05\}$

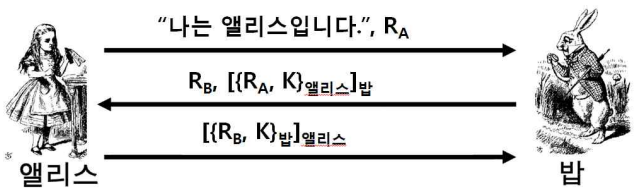
$S = 0.1^2 + 0.1^2 + 0.15^2 + 0.15^2 = 0.065$
$H_0 = 0.2*0.7 + 0.1*0.3 = 0.17$
$H_1 = 0.3*0.7 + 0.4*0.3 = 0.33$
$H_2 = 0.3*0.7 + 0.45*0.3 = 0.345$
$H_3 = 0.2*0.7 + 0.05*0.3 = 0.155$
$H_{new} = \{0.17, 0.33, 0.345, 0.155\}$

3) 아래 표와 같은 환경에서 패스워드 파일에서 임의의 한 사람 패스워드를 해킹하는데 예상되는 평균 작업량을 2의 제곱 값 형태의 수식(또는 값)으로 나타내시오. (패스워드 파일이 가염 처리되었다고 가정)

패스워드	8개 문자, 각 문자는 128개의 다른 문자로 구성
패스워드 파일	2^9개의 서로 다른 패스워드들의 해시로 구성,
패스워드 사전	총 2^{20}개로 구성된 유사 패스워드 사전을 사용, 임의의 패스워드가 존재할 확률은 1/4
해킹 작업량	해시 계산 횟수

$1/4*(2^{19}) + 3/4*1/4*(2^{20}+2^{19}) + (3/4)^2*1/4*(2*2^{20}+2^{19}) + \ldots + (3/4)^{511}*1/4*(511*2^{20}+2^{19})$

4. 다음의 상호 인증, 세션 키 전달 과정(그림의 R은 nonce, K는 생성된 세션 키)을 보고 아래의 물음에 답하시오(각 문제당 5점).

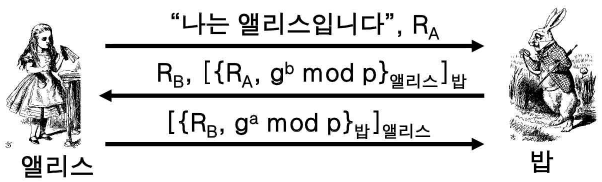


1) 상호 인증, 세션 키 전달이 안전하게 수행되는 지를 판단하시오.

상호 인증: 수행됨, 세션키 전달: 안전하게 수행됨

2) 위의 보안 과정은 PFS(완전 순방향 비밀성 보안)가 지원되지 않는데, 이를 지원하는 방법을 아래에서 (위의 그림과 같은 형식으로) 보이시오.

정보보안 기말고사 2022. 12. 14 학번: 이름:

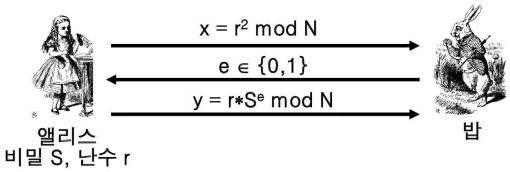


5. 다음에 대해 구체적으로 설명하시오(각 문제 당 5점).

1) 생체 인식의 오류 종류인 "기만율"과 "모욕율"에 대해 설명하시오.
- 기만율: 사용자 A를 B로 잘못 인식하는 확률
- 모욕율: 사용자 A를 A가 아니라고 잘못 판단하는 확률

2) SSL 보안 프로토콜에서 SSL 세션과 SSL 접속을 구별하여 구현하는 이유에 대해 설명하시오.
- SSL 세션에서는 인증 등을 위해 공개키 연산을 수행하는데 많은 비용이 든다.
- SSL은 HTTP 와 주로 사용되는데 HTTP는 보통 다수 접속을 병렬적으로 수행한다.
- 따라서 SSL 세션이 이미 존재할 경우, 효율적으로 각 접속에 대한 비밀성을 위한 키만 생성하기 위해 별도로 SSL 접속을 구현한다(별도 인증을 위한 공개키 연산이 필요없다).

3) 다음은 지식-제로 증명을 위한 피아트-샤미르 프로토콜 적용 예이다.



이 때 앨리스는 매번 다른 r 값을 사용해야 하는데, 그 이유에 대해 구체적으로 설명하시오.

동일한 r을 계속 사용한다면,
밥은 e=0일 때, 앨리스가 보낸 3번째 메시지에 의해 r을 알고,
밥은 e=1일 때, 앨리스가 보낸 3번째 메시지에 의해 r*S를 알게 되므로, 밥은 r*S/r 에 의해 S를 알게되므로 지식-제로가 깨지게 된다.

4) 서비스 거부(DoS) 공격을 경감하기 위해서는 프로토콜 서버가 비상태성(stateless) 성질을 가지는 것이 유리하다고 하는데 그 이유에 대해 설명하고, 커베로스 보안 프로토콜에서 KDC 서버가 어떻게 비상태성 성질을 만족하는 지를 설명하시오.
- 비상태성 프로토콜은 서버가 자신의 이전에 클라이언트에 대해 수행한 상태나 관련 데이터를 저장(기억)하지 않고, 클라이언트가 전송한 메시지를 보고 수행 동작을 즉시 처리하는 방식으로 설계된다.
- 이러한 비상태성 프로토콜은 서버가 상태 기억을 위한 자원 할당이 필요 없기 때문에, 이러한 점을 노리고 공격하는 DoS 공격에 상대적으로 강건하다.
- 커베로스는 사용자 인증 처리 후 발행하는 TGT나 앨리스가 다른 사용자(밥)에게 연결을 요구할 때 발행하는 Ticket-to-Bob 같은 메시지를 요구 사용자에게 직접 전달하는 방식으로 비상태성 성질을 만족한다.

5) GSM 보안에서 "위장 기지국 공격"에 의해 발생할 수 있는 보안 문제점에 대해 설명하시오.
- 위장 기지국이 암호화를 하지 않도록 지정할 수 있기 때문에 위장 기지국과 연결된 휴대 전화의 대화 내용은 모두 노출되게 된다.
- 해독된 3개 값(RAND, XRES, Kc)를 계속 이용하여 무선 데이터 감청이 가능함

6) 온라인 입찰(밀봉 경매이며 최고가에 의한 입찰)에서 공정성(입찰자와 경매 사이트의 유착에 의한 입찰액 사전 노출 방지)을 보장하기 위한 방법으로 해시를 사용하는 방법과 절차를 구체적으로 설명하시오.
① 입찰 진행기관에서는 입찰자들의 입찰 금액은 받은 후, 각 입찰자들의 입찰 금액에 대한 해시 값을 우선 공개하게 한다(입찰 금액은 공개하지 않음).
② 입찰이 끝나고 낙찰자가 결정된 후에 낙찰자의 낙찰 금액을 공개한다.
③ 다른 참가자들은 낙찰 금액의 해시 값과 먼저 공개된 낙찰자의 입찰 금액 해시 값을 비교함으로써, 해시 공개 후 입찰 금액의 변경이 없었음을 확인할 수 있다.