에듀윌

2018년 04월 07일 시행
9급 국가직 공무원시험 해설자료

과목 : 정보보호론
교수님 : 최희준 교수님

문 1. 전자우편 보안 기술이 목표로 하는 보안 특성이 아닌 것은?
① 익명성
② 기밀성
③ 인증성
④ 무결성
[정답] ①
[해설]
■ S/MIME
- 기존 전자우편 보안시스템의 문제점인 PEM 구현의 복잡성, PGP의 낮은 보안성과 기존 시스템과의 통합이 용이하지 않다는 점을 보완하기 위해 IETF의 작업그룹에서 RSADSI의 기술을 기반으로 개발된 E-메일 보안 기술이다.
- S/MIME은 SMTP를 한 단계 끌어올려 보안을 저해하지 않고도 광범위한 E-메일이 가능하게 하므로 SMTP만큼 중요한 표준이 되었다.
- S/MIME의 목표는 강력한 암호화, 디지털 서명, 사용 용이성, 융통성, 상호 운용성, 수출(export) 가능성등이다.
- S/MIME의 보안 서비스에는 기밀성, 무결성, 사용자 인증, 송신 사실 부인 방지가 포함된다.
- S/MIME는 E-메일에 대한 암호화는 물론 E-메일에 첨부되는 파일 등에 전자서명을 포함한다.
- S/MIME는 스니핑, 변조, 위조 등의 위험을 방지할 수 있다.

문 2. 프로그램이나 손상된 시스템에 허가되지 않는 접근을 할 수 있도록 정상적인 보안 절차를 우회하는 악성 소프트웨어는?
① 다운로더(downloader)
② 키 로거(key logger)
③ 봇(bot)
④ 백도어(backdoor)
[정답] ④
[해설]
① 다운로더 : 사용자의 동의 없이 소프트웨어를 다운로드 하여 설치하는 프로그램으로 사용자의 동의절차를 감추거나 백그라운드로 설치를 시켜 사용자는 잘 알지 못하거나 강제설치이므로 사용자가 설치를 막을 수는 없다.
② 키 로거 : 사용자의 컴퓨터에 악의적인 목적으로 설치되어 프로세스로 상주하면서 키보드에 입력된 모든 기록들을 .txt 혹은 지정된 확장자로 저장되게 하는 프로그램을 말한다.
③ 봇넷(botnet) : 봇(bot)은 로봇(robot)의 줄인 말로. 공격자는 사용자의 컴퓨터를 좀비라고도 하는 봇 상태로 바꿀 수 있는 악성 소프트웨어를 유포

한다.

문 3. 프로그램을 감염시킬 때마다 자신의 형태뿐만 아니라 행동 패턴까지 변화를 시도하기도 하는 유형의 바이러스는?
① 암호화된(encrypted) 바이러스
② 매크로(macro) 바이러스
③ 스텔스(stealth) 바이러스
④ 메타모픽(metamorphic) 바이러스
[정답] ④
[해설]
① 암호화된(encrypted) 바이러스 : 랜섬웨어처럼 컴퓨터를 사용할 수 없도록 암호화시키는 바이러스로 복호화키를 공격자에게 구매해야만 정상 복구가 가능하다.
② 매크로(macro) 바이러스 : 실행 파일에 감염되지 않고, 일반 문서 파일에 감염되기 때문에 감염 범위가 크다는 것이다. 특히 MS 오피스와 같은 응용 프로그램의 문서 파일에 삽입되어 스크립트 형태의 실행 환경을 악용하는 악성 코드이다.
③ 스텔스(stealth) 바이러스 : 스텔스 바이러스 1호는 컴퓨터에서 양키
두들이라는 록 음악이 나오는 형태, 스텔스 바이러스 3호는 '사생아'라는 이름이 붙여져 있으며 감염되는 순간, 5천부터 카운터를 시작해 제로가 될 때까지 하드 디스크의 모든 자료를 조금씩 남김없이 파괴해버린다.

문 4. 증거의 수집 및 분석을 위한 디지털 포렌식의 원칙에 대한 설명으로 옳지 않은 것은?
① 정당성의 원칙 - 증거 수집의 절차가 적법해야 한다.
② 연계 보관성의 원칙 - 획득한 증거물은 변조가 불가능한 매체에 저장해야 한다.
③ 신속성의 원칙 - 휘발성 정보 수집을 위해 신속히 진행해야 한다.
④ 재현의 원칙 - 동일한 조건에서 현장 검증을 실시하면 피해 당시와 동일한 결과가 나와야 한다.
[정답] ②
[해설]
■ 디지털 포렌식의 기본 원칙
• 1. 정당성의 원칙 : 모든 증거는 적법한 절차를 거쳐서 획득되어야 한다. 위법하게 수집된 증거는 증거 능력이 없다.
• 2. 재현의 원칙 : 증거자료는 같은 환경에서 같은 결과가 나오도록 재현이 가능해야 한다.
• 3. 신속성의 원칙 : 컴퓨터 내부의 정보 획득은 신속하게 이루어져야한다.
• 4. 연계보관성의 원칙 : 증거는 획득되고, 이송/분석/보관/법정 제출의 과정이 명확해야한다.
• 5. 무결성의 원칙 : 획득한 정보는 위.변조되지 않았음을 입증할 수 있어야 한다.

문 5. 웹 애플리케이션의 대표적인 보안 위협의 하나인 인젝션 공격에 대한 대비책으로 옳지 않은 것은?
① 보안 프로토콜 및 암호 키 사용 여부 확인
② 매개 변수화된 인터페이스를 제공하는 안전한 API 사용

③ 입력 값에 대한 적극적인 유효성 검증
④ 인터프리터에 대한 특수 문자 필터링 처리
[정답] ①
[해설]
취약한 인증 및 세션 관리는 웹을 인증과 세션 관리가 불안하여 패스워드나 세션이 보호되지 않는다는 취약성이다. 대비책으로는 보안 프로토콜 및 암호 키 사용 여부 확인한다.

문 6. 개인정보 보호법 상의 개인정보의 수집.이용 및 수집 제한에 대한 설명으로 옳지 않은 것은?
① 개인정보처리자는 정보주체의 동의를 받은 경우에는 개인정보를 수집할 수 있으며 그 수집 목적의 범위에서 이용할 수 있다.
② 개인정보처리자는 개인정보 보호법 에 따라 개인정보를 수집하는 경우에는 그 목적에 필요한 최소한의 개인정보를 수집하여야 한다. 이 경우 최소한의 개인정보 수집이라는 입증책임은 개인정보처리자가 부담한다.
③ 개인정보처리자는 정보주체의 동의를 받아 개인정보를 수집하는 경우 필요한 최소한의 정보 외의 개인정보 수집에는 동의하지 아니할 수 있다는 사실을 구체적으로 알리고 개인정보를 수집하여야 한다.
④ 개인정보처리자는 정보주체가 필요한 최소한의 정보 외의 개인정보 수집에 동의하지 아니하는 경우 정보주체에게 재화 또는 서비스의 제공을 거부할 수 있다.
[정답] ④
[해설]
■ 개인정보의 수집 제한

- ① 개인정보처리자는 개인정보를 수집할 수 있는 모든 경우에 해당되어 개인정보를 수집하는 경우에는 그 목적에 필요한 최소한의 개인정보를 수집하여야 한다. 이 경우 최소한의 개인정보 수집이라는 입증책임은 개인정보처리자가 부담한다.
- ② 개인정보처리자는 정보주체가 필요한 최소한의 정보 외의 개인정보 수집에 동의하지 아니한다는 이유로 정보주체에게 재화 또는 서비스의 제공을 거부하여서는 아니 된다.

문 7. <보기 1>은 리눅스에서 일반 사용자(hello)가 'ls -al'을 수행한 결과의 일부분이다. <보기 2>의 설명에서 옳은 것만을 모두 고른 것은?

<보기 1>
-rwxr-xr-x 1 hello world 4096 Nov 21 15:12 abc.txt
ⓐ ⓑ

<보기 2>
ㄱ. ⓐ는 파일의 소유자, 그룹, 이외 사용자 모두가 파일을 읽고 실행할 수 있지만, 파일의 소유자만이 파일을 수정할 수 있음을 나타낸다.
ㄴ. ⓑ가 모든 사용자(파일 소유자, 그룹, 이외 사용자)에게 읽기, 쓰기, 실행 권한을 부여하려면 'chmod 777 abc.txt'의 명령을 입력하면 된다.
ㄷ. ⓑ가 해당 파일의 소유자를 root로 변경하려면 'chown root abc.txt'의 명령을 입력하면 된다.

① ㄱ ② ㄱ, ㄴ
③ ㄴ, ㄷ ④ ㄱ, ㄴ, ㄷ
[정답] ②
[해설]
chown root hello : abc. txt의 현재 소유자인 hello를 root가 소유자로 되도록 변경한다.

문 8. 다음은 CC(Common Criteria)의 7가지 보증 등급 중 하나에 대한 설명이다. 시스템이 체계적으로 설계되고, 테스트되고, 재검토되도록 (methodically designed, tested and reviewed) 요구하는 것은?

낮은 수준과 높은 수준의 설계 명세를 요구한다. 인터페이스 명세가 완벽할 것을 요구한다. 제품의 보안을 명시적으로 정의한 추상화 모델을 요구한다. 독립적인 취약점 분석을 요구한다. 개발자 또는 사용자가 일반적인 TOE의 중간 수준부터 높은 수준까지의 독립적으로 보증된 보안을 요구 하는 곳에 적용 가능하다. 또한 추가적인 보안 관련 비용을 감수할 수 있는 곳에 적용 가능하다.

① EAL 2 ② EAL 3
③ EAL 4 ④ EAL 5
[정답] ③
[해설]
■ 평가보증등급(EAL: Evaluation Assurance Level)
- 평가보증등급1(EAL 1) : 기능적인 시험
- 평가보증등급2(EAL 2) : 구조적인 시험
- 평가보증등급3(EAL 3) : 체계적인 시험 및 검사
- 평가보증등급4(EAL 4) : 체계적인 설계, 시험 및 검토
- 평가보증등급5(EAL 5) : 준정형화된 설계 및 시험
- 평가보증등급6(EAL 6) : 준정형화된 설계 검증 및 시험
- 평가보증등급7(EAL 7) : 정형화된 설계 검증 및 시험

문 9. 다음에 설명한 Diffie-Hellman 키 교환 프로토콜의 동작 과정에서 공격자가 알지 못하도록 반드시 비밀로 유지해야 할 정보만을 모두 고른 것은?

소수 p와 p의 원시근 g에 대하여, 사용자 A는 p보다 작은 양수 a를 선택하고, $x = g^a \bmod p$를 계산하여 x를 B에게 전달한다. 마찬가지로 사용자 B는 p보다 작은 양수 b를 선택하고, $y = g^b \bmod p$를 계산하여 y를 A에게 전달한다. 그러면 A와 B는 $g^{ab} \bmod p$를 공유하게 된다.

① a, b
② p, g, a, b
③ a, b, $g^{ab} \bmod p$
④ p, g, a, b, $g^{ab} \bmod p$
[정답] ③
[해설]
p와 g는 공개되고, a와 b 비밀로 한다. $g^{ab} \bmod p$는 p와 g가 공개되어 있으므로 $g^{ab} \bmod$

p을 공개하면 a와 b를 공격자는 쉽게 알아낼 수 있다. 따라서 g^{ab} mod p식 자체도 비밀로 해야한다.

① 송신측과 수신측은 공통으로 소수 p와 Z_p의 원시근 g를 준비하여 (p, g)를 공개한다.
② 송신측은 키 교환을 위해 키를 생성하여 수신측에 전달한다. 이때 a는 자신의 비밀키로 한다.
송신측은 난수 a를 $a \in Z_{p-1}$를 선택하여, $x \equiv g^a \pmod p$를 계산하여, x를 수신측에 보내고, a는 자신의 비밀키로 한다.
③ 수신측은 키 교환을 위해 키를 생성하여 송신측에 전달한다. 이때 b는 자신의 비밀키로 한다.
수신측은 난수 b를 $b \in Z_{p-1}$를 선택하여, $y \equiv g^b \pmod p$를 계산하여, y를 송신측에 보내고, b는 자신의 비밀키로 한다.
④ 송신측은 자신의 비밀키 a를 이용하여 공통키를 생성한다.
$k_1 \equiv y^a \equiv g^{ba} \pmod p$를 계산하여 k_1을 수신측과의 공통키로 한다.
⑤ 수신측은 자신의 비밀키 b를 이용하여 공통키를 생성한다.
$k_2 \equiv y^b \equiv g^{ab} \pmod p$를 계산하여 k_2를 송신측과의 공통키로 한다. ($k_1 = k_2$)
• 비밀 키를 교환할 때 도청되어도 공통키를 구할 수 없다.
• 제3자가 x, y를 도청했다고 하더라도 개인의 비밀키 a나 b를 구하는 것은 이산 대수 문제이므로 계산하기가 매우 어려워 송신측과 수신측의 공통키를 구할 수 없다.

문 10. IEEE 802.11i에 대한 설명으로 옳지 않은 것은?
① 단말과 AP(Access Point) 간의 쌍별(pairwise) 키와 멀티캐스팅을 위한 그룹 키가 정의되어 있다.
② 전송되는 데이터를 보호하기 위해 TKIP(Temporal Key Integrity Protocol)와 CCMP(Counter Mode with Cipher Block Chaining MAC Protocol) 방식을 지원한다.
③ 서로 다른 유무선랜 영역에 속한 단말들의 종단간(end-to-end) 보안 기법에 해당한다.
④ 802.1X 표준에서 정의된 방법을 이용하여 무선 단말과 인증서버 간의 상호 인증을 할 수 있다.
[정답] ③
[해설]
IEEE 802.11i는 중간에 인증 서버를 필요로 한다. 서버 없이 단말들의 종단간(end-to-end) 보안 기법에 해당하는 보안 프로그램은 telegram, PGP 등이 있다.

■ IEEE 802.11i
- IEEE 802.11에서의 무선 LAN 보안의 취약성을 해결하기 위한 표준기술이다.
- 무선 구간에서 데이터 보호(기밀성,무결성) 능력이 강화된 암호화 방식이다.
- 인증과 암호화의 두 기능이 완벽하게 분리된 강화된 인증 방식이다.
- 인증이 성공한 후, 인증 서버는 암호화키를 생성하고 배포한다.
- 블록 암호화 방식인 AES, 키 길이 128 비트, 블록 크기 128 비트를 사용한다.
- 사용자 인증 및 키 교환을 위해서 별도의 인증 서버 필요하다. 실제 인증 수행은 주로 EAP라는 인증 프레임워크 상에서 이루어진다.
- 802.1X 표준에서 정의된 방법을 이용하여 무선 단말과 인증서버 간의 상호 인증을 할 수 있다.
- 전송되는 데이터를 보호하기 위해 TKIP와 CCMP 방식을 지원한다.
- 단말과 AP(Access Point) 간의 쌍별(pairwise)키와 멀티캐스팅을 위한 그룹 키가 정의되어 있다.

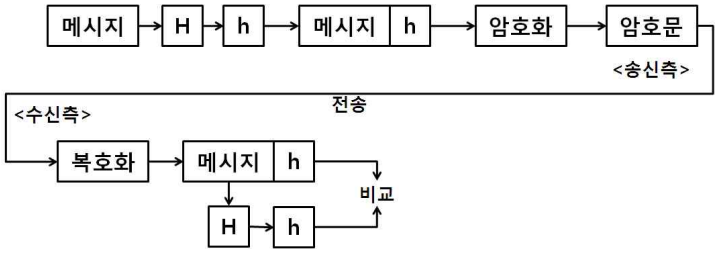
문 11. SSL(Secure Socket Layer)에서 메시지에 대한 기밀성을 제공하기 위해 사용되는 것은?
① MAC(Message Authentication Code)
② 대칭키 암호 알고리즘
③ 해시 함수
④ 전자서명
[정답] ②
[해설]
① MAC → 무결성
③ 해시 함수 → 무결성
④ 전자서명 → 인증성, SSL은 부인 방지는 제공하지 않는다.

문 12. 메시지 인증에 사용되는 해시 함수의 요건으로 옳지 않은 것은?
① 임의 크기의 메시지에 적용될 수 있어야 한다.
② 해시를 생성하는 계산이 비교적 쉬워야 한다.
③ 다양한 길이의 출력을 생성할 수 있어야 한다.
④ 하드웨어 및 소프트웨어에 모두 실용적이어야 한다.
[정답] ③
[해설]
■ 해시 함수 조건
- 해시 함수는 다양한 길이의 메시지를 적용할 수 있어야한다.
- 해시 함수는 고정된 길이의 출력을 만들어야한다.
- 해시 함수는 계산하기 쉬어야한다.
- 해시 함수와 해시 코드만 주어졌을 때 메시지를 복원하는 것이 불가능하도록 해야 한다.
- 해시 함수는 같은 출력을 갖는 두 입력을 찾기 어려워야한다.

문 13. 사용자 A가 사용자 B에게 보낼 메시지 M을 공개키 기반의 전자 서명을 적용하여 메시지의 무결성을 검증하도록 하였다. A가 보낸 서명이 포함된 전송 메시지를 다음 표기법에 따라 바르게 표현한 것은?

PUx: X의 공개키
PRx: X의 개인키
E(K, M): 메시지 M을 키 K로 암호화
H(M): 메시지 M의 해시
||: 두 메시지의 연결

① E(PUB, M)　　② E(PRA, M)
③ M || E(PUB, H(M))　　④ M || E(PRA, H(M))
[정답] ④
[해설]
PUx : PUA는 A의 공개키, PUB는 B의 공개키
PRx : PRA는 A의 개인키, PRB는 B의 개인키



M → H(M) → M || M(H) → **M || E(PRA, H(M))** → D(PUA, H(M)) → M || H(M)
<송신 측> → <수신 측>

문 14. 대칭키 블록 암호 알고리즘의 운영 모드 중에서 한 평문 블록의 오류가 다른 평문 블록의 암호 결과에 영향을 미치는 오류 전이(error propagation)가 발생하지 않는 모드만을 묶은 것은? (단, ECB: Electronic Code Book, CBC: Cipher Block Chaining, CFB: Cipher Feedback, OFB: Output Feedback)

① CFB, OFB ② ECB, OFB
③ CBC, CFB ④ ECB, CBC

[정답] ②

[해설]

■ **ECB(Electronic CodeBook) Mode**

• 가장 단순한 방법으로 평문을 암호화한다.

• 평문을 평문 블록으로 구분한 후, 블록 별로 암호 시스템의 알고리즘에 적용하는 방식이다.

• 코드북(Codebook)이라 하며, 가장 간단하게 평문을 동일한 크기의 평문블록으로 나누고 키로 암호화하여 암호블록을 생성한다.

  • 동일한 평문이 동일한 암호문으로 암호화되지 않기 때문에 확산의 효과가 크며, 전수 공격으로부터 안전하다.

  • 하나의 블록의 오류가 발생하더라도 다음 블록에는 영향을 주지 않는다.

■ **OFB(Output FeedBack) Mode**

• 평문을 암호화한 출력 블록을 다시 n비트를 선택한 후 n비트 평문과 XOR하여 암호화한다.

• 오류의 전이가 없고 키수열이 평문과 무관하여 미리 계산이 가능하고 또한 스트림 암호로 사용이 가능하다.

문 15. 유닉스/리눅스 시스템의 로그 파일에 기록되는 정보에 대한 설명으로 옳지 않은 것은?

① utmp - 로그인, 로그아웃 등 현재 시스템 사용자의 계정 정보
② loginlog - 성공한 로그인에 대한 내용
③ pacct - 시스템에 로그인한 모든 사용자가 수행한 프로그램 정보
④ btmp - 실패한 로그인 시도

[정답] ②

[해설]

② loginlog - 실패한 로그인 시도 내역

문 16. 개인정보 보호법 상 개인정보처리자가 개인정보가 유출되었음을 알게 되었을 때에 지체 없이 해당 정보주체에게 알려야 할 사항에 해당하지 않는 것은?
① 유출된 개인정보의 항목
② 유출된 시점과 그 경위
③ 조치 결과를 행정안전부장관 또는 대통령령으로 정하는 전문기관에 신고한 사실
④ 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처
[정답] ③
[해설]
■ 개인정보 유출 통지 사항
1. 유출된 개인정보의 항목
2. 유출된 시점과 그 경위
3. 유출로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보
4. 개인정보처리자의 대응조치 및 피해 구제절차
5. 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처

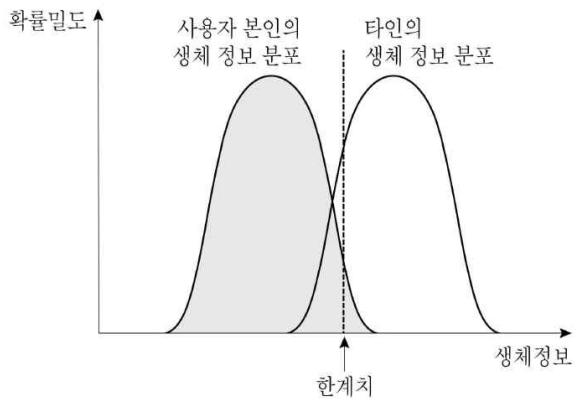
문 17. 인증서를 발행하는 인증기관, 인증서를 보관하고 있는 저장소, 공개키를 등록하거나 등록된 키를 다운받는 사용자로 구성되는 PKI(Public Key Infrastructure)에 대한 설명으로 옳지 않은 것은?
① 인증기관이 사용자의 키 쌍을 생성할 경우, 인증기관은 사용자의 개인키를 사용자에게 안전하게 보내는 일을 할 필요가 있다.
② 사용자의 공개키에 대해 인증기관이 전자서명을 해서 인증서를 생성한다.
③ 사용자의 인증서 폐기 요청에 대하여 인증기관은 해당 인증서를 저장소에서 삭제함으로써 인증서의 폐기 처리를 완료한다.
④ 한 인증기관의 공개키를 다른 인증기관이 검증하는 일이 발생할 수 있다.
[정답] ③
[해설]
• 사용자의 인증서 폐기와 인증서 삭제는 다르다.
• 사용자의 인증서를 삭제한 것은 유효기간과 상관없이 설치된 곳만 삭제한 개념이기 때문에 사용 기간이 남아 있다면 아직 유효한 상태이다.
• 사용자의 인증서를 폐기한 것은 인증서가 더 이상 필요한지 않을 때 인증서 자체를 중단하는 것을 말한다.

문 18. 암호학적으로 안전한 의사(pseudo) 난수 생성기에 대한 설명으로 옳은 것은?
① 생성된 수열의 비트는 정규분포를 따라야 한다.
② 생성된 수열의 어느 부분 수열도 다른 부분 수열로부터 추정될 수 없어야 한다.
③ 시드(seed)라고 불리는 입력 값은 외부에 알려져도 무방하다.
④ 비결정적(non-deterministic) 알고리즘을 사용하여 재현 불가능한 수열을 생성해야 한다.
[정답] ②
[해설]

틀린 설명을 올바르게 고치면 다음과 같다.
① 난수로 생성된 수열의 비트는 무작위로 발생하므로 일정한 형태인 정규분포를 따를 수 없다.
③ 시드(seed) 값을 알게 되면 난수를 추정할 수 있게 되므로 비밀로 해야 한다.
④ 특정한 입력이 들어오면 언제나 똑같은 과정을 거쳐서 언제나 똑같은 결과를 내놓는 결정적(non-deterministic) 알고리즘을 사용하여 재현 불가능한 수열을 생성해야 한다.

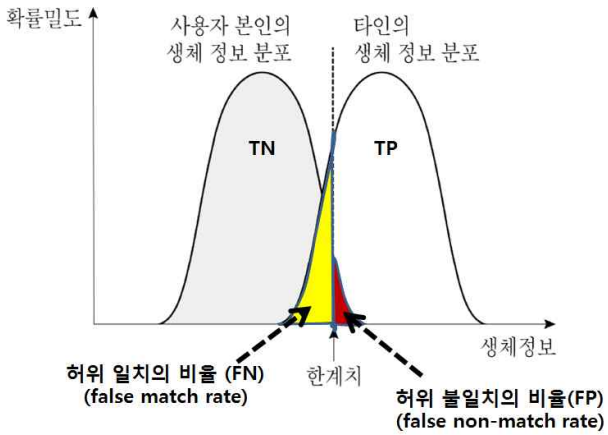
문 19. 사용자 워크스테이션의 클라이언트, 인증서버(AS), 티켓발행서버(TGS), 응용서버로 구성되는 Kerberos에 대한 설명으로 옳은 것은? (단, Kerberos 버전 4를 기준으로 한다)
① 클라이언트는 AS에게 사용자의 ID와 패스워드를 평문으로 보내어 인증을 요청한다.
② AS는 클라이언트가 TGS에 접속하는 데 필요한 세션키와 TGS에 제시할 티켓을 암호화하여 반송한다.
③ 클라이언트가 응용서버에 접속하기 전에 TGS를 통해 발급 받은 티켓은 재사용될 수 없다.
④ 클라이언트가 응용서버에게 제시할 티켓은 AS와 응용서버의 공유 비밀키로 암호화되어 있다.
[정답] ②
[해설]
틀린 설명을 올바르게 고치면 다음과 같다.
① 클라이언트는 사용자의 ID(IDc), 패스워드(Pc), 사용하고자 하는 서버의 식별자(IDv)를 중앙 집중 인증 서버(AS)에 전송한다.
③ 클라이언트가 응용서버에 접속하기 전에 TGS를 통해 발급 받은 티켓은 재사용될 수 있다. 단 티켓의 유효 기간은 존재한다.
④ 클라이언트가 응용서버에게 제시할 티켓은 AS에 존재하는 사용자 암호의 해시 값으로 암호화되어 있다.

문 20. 생체 인식 시스템은 저장되어 있는 개인의 물리적 특성을 나타내는 생체 정보 집합과 입력된 생체 정보를 비교하여 일치 정도를 판단한다. 다음 그림은 사용자 본인의 생체 정보 분포와 공격자를 포함한 타인의 생체 정보 분포, 그리고 본인 여부를 판정하기 위한 한계치를 나타낸 것이다. 그림 및 생체 인식 응용에 대한 설명으로 옳은 것만을 고른 것은?



ㄱ. 타인을 본인으로 오인하는 허위 일치의 비율(false match rate, false acceptance rate)이 본인을 인식하지 못하고 거부하는 허위 불일치의 비율(false non-match rate, false rejection rate)보다 크다.
ㄴ. 한계치를 우측으로 이동시키면 보안성은 강화되지만 사용자 편리성은 저하된다.
ㄷ. 보안성이 높은 응용프로그램은 낮은 허위 일치 비율을 요구한다.
ㄹ. 가능한 용의자를 찾는 범죄학 응용프로그램의 경우 낮은 허위 일치 비율이 요구된다.

① ㄱ, ㄷ ② ㄱ, ㄹ
③ ㄴ, ㄷ ④ ㄴ, ㄹ
[정답] ①
[해설]
■ **민감도(Sensitivity)와 특이도(Specificity)**



- 민감도 = TP/(TP+FN)×100%, 본인인데, 본인으로 판단하는 경우
- 특이도 = TN/(TN+FP)×100%, 본인이 아닌데(타인인데), 본인이 아닌 것으로(타인으로) 판단 경우
- 민감도와 특이도가 높을수록, 보안성이 높다는 것을 의미한다.
- 예를 들어 TN=50, FN=10이고, TP=50, FP=5이면,
  민감도 = TP/(TP+FN)×100% = 50/(50+10)×100 = 83.33%
  특이도 = TN/(TN+FP)×100% = 50/(50+5)×100 = 90.90%

틀린 보기를 올바르게 고치면 다음과 같다.
ㄴ. 한계치를 우측으로 이동시키면 FN이 커지므로 민감도가 낮아지므로 보안성이 약화된다. 민감도가 낮아지는 것은 사용자들이 쉽게 본인으로 판다하므오 편리성은 높아진다.
ㄹ. 가능한 용의자를 찾는 범죄학 응용프로그램의 경우 낮은 허위 불일치 비율이 요구된다. 범죄학에서 “열 명의 범죄자를 잡지 못해도 한 명의 억울한 피해자는 만들지 말라"는 원칙이 있는 것 처럼 허위 불일치 비율이 낮을수록 특이도가 커지므로 범인이 아닌 사람을 범인으로 판단하지 않는 확률이 높아진다.