정보보호론	지방 전산 9급	2023년 6월 10일

1. 데이터의 위변조를 방어하는 기술이 목표로 하는 것은? [2023년 지방 9급]

① 기밀성 ② 무결성
③ 가용성 ④ 책임추적성

♤ **위협 요소**

가용성	• **가용성 위협 요소** : 서비스 거부 공격(DoS 공격), 웜(worm), 방해(가로막기) 등 • 가용성은 데이터 백업, 중복 저장 등으로 위협 요소로부터 보호할 수 있다.
무결성	• **무결성 위협 요소** : **변조, 위조**, 유지보수, 부인, 재전송(replaying, 재연) 등 • 무결성의 환경적인 위협 요소 : 먼지, 열, 정전기, 서지(surge) 전류 등 • 서지(surge) 전류는 낙뢰 등에 의한 이상 전류를 의미한다.
기밀성	• **기밀성 위협 요소** : 트래픽 분석, 도난, 도청, **사회공학(social engineering)** 등 • 기밀성은 암호화, 접근통제 등을 이용하여 구현할 수 있다. • 기밀성은 정보 보관 및 정보 전송에도 적용되어야 한다.

정답 : ②

2. UDP 헤더 포맷의 구성요소가 아닌 것은? [2023년 지방 9급]

① 순서번호 ② 발신지 포트번호
③ 목적지 포트번호 ④ 체크섬

♤ **UDP 헤더 포맷**

source port number (16비트)	destination port number (16비트)	↑ UDP 헤더 ↓
length(16비트)	checksum(16비트)	
user data		

- source port number : 출발지 포트번호
- destination port number : 목적지 포트번호
- length : 전체 패킷 크기, UDP 헤더와 user data 크기를 더함(byte)
- checksum : 데이터 무결성을 검사하기 위한 것(손상된 데이터는 폐기 처리)
- **순서번호**는 TCP 헤더에 있다.

정답 : ①

3. 논리폭탄에 대한 설명으로 옳은 것은? [2023년 지방 9급]

① 사용자 동의 없이 설치되어 컴퓨터 내의 금융 정보, 신상 정보 등을 수집·전송하기 위한 것이다.
② 침입자에 의해 악성 소프트웨어에 삽입된 코드로서, 사전에 정의된 조건이 충족되기 전까지는 휴지 상태에 있다가 조건이 충족되면 의도한 동작이 트리거되도록 한다.
③ 사용자가 키보드로 PC에 입력하는 내용을 몰래 가로채어 기록한다.
④ 공격자가 언제든지 시스템에 관리자 권한으로 접근할 수 있도록 비밀통로를 지속적으로 유지시켜 주는 일련의 프로그램 집합이다.

♤ **논리폭탄(logic bomb)**

- 논리폭탄은 휴지상태에 있다가 사전에 정의된 **조건**이 **충족**되면 **동작**이 트리거되도록 한다.
- 논리폭탄은 사전에 정의된 조건이 충족되기 전까지는 휴지상태에 있다.
- 논리폭탄은 특정 **날짜**나 **시간** 등 조건이 충족되었을 때 **동작**되도록 할 수 있다.
- 논리폭탄은 컴퓨터 바이러스처럼 인터넷에서 범죄나 사이버 테러리즘의 수법으로 사용된다.
- 바이러스와 달리 논리폭탄은 자신을 복제할 수 없다.

- 지금까지 알려진 **사이버 무기** 가운데 가장 파괴력이 큰 것은 논리폭탄(logic bomb)이다.
- 논리폭탄은 여러 가지 종류가 있다.
- 가장 많이 연구되고 있는 것은 **기간통신망 파괴용** 폭탄이다.
- 이 폭탄이 **전화교환기**에 침투해 작동하는 순간에 그 나라의 **전화망**은 무용지물이 된다.
- 논리폭탄은 상대국가의 **방공망**이나 **중앙은행**의 컴퓨터 경제 통신망을 파괴할 수 있다.

정답 : ②

4. 대칭키 암호 알고리즘이 아닌 것은? [2023년 지방 9급]

① SEED ② ECC
③ IDEA ④ LEA

♤ **암호 알고리즘 종류**

대칭키 암호	DES, SEED, AES, LEA, ARIA, HIGHT, IDEA, RC4, SkipJack
공개키 암호	RSA, Rabin, ElGamal, **ECC**, DSA, KCDSA, ECDSA **(비대칭키 암호)**
해시함수	MD5, HAS-160, SHA-1, SHA-2, WHIRLPOOL(월풀)

정답 : ②

5. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에서 규정하고 있는 사항이 아닌 것은? [2023년 지방 9급]

① 정보통신망의 표준화 및 인증
② 정보통신망의 안정성 확보
③ 고정형 영상정보처리기기의 설치·운영 제한
④ 집적된 정보통신시설의 보호

♤ **정보통신망 이용촉진 및 정보보호 등에 관한 법률**

제8조(정보통신망의 표준화 및 인증)

① 과학기술정보통신부장관은 정보통신망의 이용을 촉진하기 위하여 정보통신망에 관한 표준을 정하여 고시하고, 정보통신서비스 제공자 또는 정보통신망과 관련된 제품을 제조하거나 공급하는 자에게 그 표준을 사용하도록 권고할 수 있다. 다만, 「산업표준화법」 제12조에 따른 한국산업표준이 제정되어 있는 사항에 대하여는 그 표준에 따른다. 〈개정 2013. 3. 23., 2017. 7. 26.〉

제45조(정보통신망의 안정성 확보 등)

① 다음 각 호의 어느 하나에 해당하는 자는 정보통신서비스의 제공에 사용되는 정보통신망의 안정성 및 정보의 신뢰성을 확보하기 위한 보호조치를 하여야 한다. 〈개정 2020. 6. 9.〉

1. 정보통신서비스 제공자
2. 정보통신망에 연결되어 정보를 송·수신할 수 있는 기기·설비·장비 중 대통령령으로 정하는 기기·설비·장비(이하 "정보통신망연결기기등"이라 한다)를 제조하거나 수입하는 자

제46조(집적된 정보통신시설의 보호)

① 다음 각 호의 어느 하나에 해당하는 정보통신서비스 제공자 중 정보통신시설의 규모 등이 대통령령으로 정하는 기준에 해당하는 자(이하 "집적정보통신시설 사업자등"이라 한다)는 정보통신시설을 안정적으로 운영하기 위하여 대통령령으로 정하는 바에 따른 보호조치를 하여야 한다. 〈개정 2023. 1. 3.〉

1. 타인의 정보통신서비스 제공을 위하여 집적된 정보통신시설을 운영·관리하는 자(이하 "집적정보통신시설 사업자"라 한다)
2. 자신의 정보통신서비스 제공을 위하여 직접 집적된 정보통신시설을 운영·관리하는 자

개인정보 보호법 : 제25조(고정형 영상정보처리기기의 설치·운영 제한)

① 누구든지 다음 각 호의 경우를 제외하고는 공개된 장소에 **고정형 영상정보처리기기**를 설치·운영하여서는 아니 된다. 〈개정 2023. 3. 14.〉

1. 법령에서 구체적으로 허용하고 있는 경우
2. 범죄의 예방 및 수사를 위하여 필요한 경우
3. 시설의 안전 및 관리, 화재 예방을 위하여 정당한 권한을 가진 자가 설치·운영하는 경우
4. 교통단속을 위하여 정당한 권한을 가진 자가 설치·운영하는 경우
5. 교통정보의 수집·분석 및 제공을 위하여 정당한 권한을 가진 자가 설치·운영하는 경우
6. 촬영된 영상정보를 저장하지 아니하는 경우로서 대통령령으로 정하는 경우

정답 : ③

6. CSRF 공격에 대한 설명으로 옳지 않은 것은? [2023년 지방 9급]

① 사용자가 자신의 의지와는 무관하게 공격자가 의도한 행위를 특정 웹사이트에 요청하게 하는 공격이다.

② 특정 웹사이트가 사용자의 웹 브라우저를 신뢰하는 점을 노리고 사용자의 권한을 도용하려는 것이다.

③ 사용자에게 전달된 데이터의 악성 스크립트가 사용자 브라우저에서 실행되면서 해킹을 하는 것으로, 이 악성 스크립트는 공격자가 웹 서버에 구현된 애플리케이션의 취약점을 이용하여 서버 측 또는 URL에 미리 삽입해 놓은 것이다.

④ 웹 애플리케이션의 요청 내에 세션별·사용자별로 구별 가능한 임의의 토큰을 추가하도록 하여 서버가 정상적인 요청과 비정상적인 요청을 판별하는 방법으로 공격에 대응할 수 있다.

♤ CSRF(XSRF) 공격

• 사용자에게 전달된 데이터의 악성 스크립트가 사용자 브라우저에서 실행되면서 해킹을 하는 것으로, 이 악성 스크립트는 공격자가 웹 서버에 구현된 애플리케이션의 취약점을 이용하여 **서버 측** 또는 URL에 미리 **삽입**해 놓은 것이다.(×)

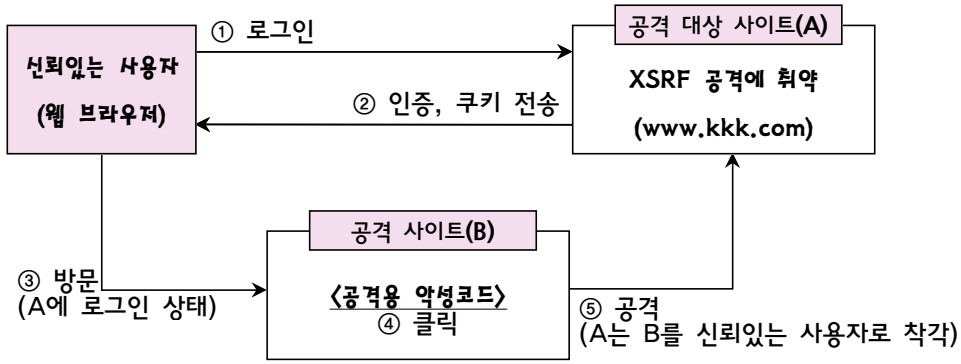
→ CSRF(XSRF) 공격이 아니고 XSS 공격이다.

// XSS와 XSRF 비교

XSS	• XSS는 사용자들이 특정 **웹사이트**를 신뢰하는 점을 노린 공격이고
XSRF	• XSRF는 특정 웹사이트가 **사용자**의 웹 브라우저를 신뢰하는 점을 노린 공격이다.

// XSRF 공격

다음 그림은 XSRF 공격을 개략적으로 보여 준다.



정답 : ③

7. IPSec의 터널모드를 이용한 VPN에 대한 설명으로 옳지 않은 것은? [2023년 지방 9급]

① 인터넷상에서 양측 호스트의 IP 주소를 숨기고 새로운 IP 헤더에 VPN 라우터 또는 IPSec 게이트웨이의 IP 주소를 넣는다.

② IPSec의 터널모드는 새로운 IP 헤더를 추가하기 때문에 전송모드 대비 전체 패킷이 길어진다.

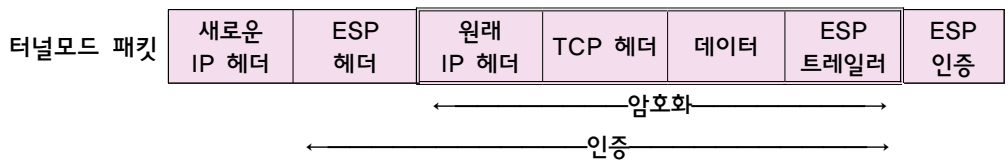
③ ESP는 원래 IP 패킷 전부와 원래 IP 패킷 앞뒤로 붙는 ESP 헤더와 트레일러를 모두 암호화한다.

④ ESP 인증 데이터는 패킷의 끝에 추가되며, ESP 터널모드의 경우 인증은 목적지 VPN 라우터 또는 IPSec 게이트웨이에서 이루어진다.

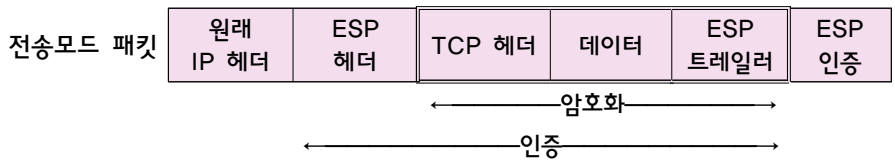
♤ **IPSec의 터널모드**

· ESP는 원래 IP 패킷 전부와 원래 IP 패킷 앞뒤로 붙는 **ESP 헤더**와 트레일러를 모두 암호화한다.**(×)** → **ESP 헤더**는 암호화되지 않는다.

// 다음은 **[정보통신기술용어해설]**을 참조하였다.



· 전체 IP 패킷을 **암호화**한다.
· 내부 IP 패킷의 **인증**은 **선택**사항이다.
· ESP는 **인증. 무결성, 기밀성**을 제공한다.



· 원래 **IP 헤더**를 **제외한** 나머지 부분만 **암호화**한다.
· 내부 IP 패킷의 **인증**은 **선택**사항이다.
· ESP는 **인증. 무결성, 기밀성**을 제공한다.

· 위 2가지 중 **터널모드**가 **전송모드**보다 **안전**하나 **과부하**를 준다.

정답 : ③

8. 「전자서명법」상 전자서명인증사업자에 대한 전자서명인증업무 운영기준 준수사실의 인정(이하 "인정" 이라 한다)에 대한 설명으로 옳지 않은 것은? [2023년 지방 9급]

① 인정을 받으려는 전자서명인증사업자는 국가기관, 지방자치단체 또는 공공기관이어야 한다.

② 인정을 받으려는 전자서명인증사업자는 평가기관으로부터 평가를 먼저 받아야 한다.

③ 평가기관은 평가를 신청한 전자서명인증사업자의 운영기준 준수 여부에 대한 평가를 하고, 그 결과를 인정기관에 제출하여야 한다.

④ 인정기관은 평가 결과를 제출받은 경우 그 평가 결과와 인정을 받으려는 전자서명인증사업자가 법정 자격을 갖추었는지 여부를 확인하여 인정 여부를 결정하여야 한다.

♤ **전자서명법 – 전자서명인증사업자에 대한 전자서명인증업무 운영기준 준수사실의 인정**

제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다.

1. "전자문서"란 정보처리시스템에 의하여 전자적 형태로 작성되어 송신 또는 수신되거나 저장된 정보를 말한다.
2. "전자서명"이란 다음 각 목의 사항을 나타내는 데 이용하기 위하여 전자문서에 첨부되거나 논리적으로 결합된 전자적 형태의 정보를 말한다.
3. "전자서명생성정보"란 전자서명을 생성하기 위하여 이용하는 전자적 정보를 말한다.
7. "**전자서명인증업무**"란 전자서명인증, 전자서명인증 관련 기록의 관리 등 전자서명인증서비스를 제공하는 업무를 말한다.
8. "**전자서명인증사업자**"란 전자서명인증업무를 하는 자를 말한다.
9. "가입자"란 전자서명생성정보에 대하여 전자서명인증사업자로부터 전자서명인증을 받은 자이다.
10. "이용자"란 전자서명인증사업자가 제공하는 전자서명인증서비스를 이용하는 자를 말한다.

제8조(운영기준 준수사실의 인정)

① 전자서명인증사업자(전자서명인증업무를 하려는 자를 포함한다. 이하 제8조부터 제11조까지에서 같다)는 제9조에 따른 인정기관으로부터 운영기준의 준수사실에 대한 인정을 받을 수 있다. 이 경우 제10조에 따른 평가기관으로부터 운영기준의 준수 여부에 대한 평가를 먼저 받아야 한다.

② 제1항 전단에 따른 **인정**(이하 "운영기준 준수사실의 인정"이라 한다)**을 받으려는 전자서명인증사업자**는 **국가기관, 지방자치단체** 또는 **법인**이어야 한다.

③ 임원 중에 다음 각 호의 어느 하나에 해당하는 사람이 있는 법인은 운영기준 준수사실의 인정을 받을 수 없다. 〈개정 2021. 10. 19.〉

1. 피성년후견인
2. 파산선고를 받고 복권되지 아니한 사람

:

5. 법원의 판결 또는 다른 법률에 따라 자격이 상실되거나 정지된 사람

정답 : ①

9. 위험평가 접근방법에 대한 설명으로 옳지 않은 것은? [2023년 지방 9급]

① 기준(baseline) 접근법은 기준 문서, 실무 규약, 업계 최신 실무를 이용하여 시스템에 대한 가장 기본적이고 일반적인 수준에서의 보안 통제 사항을 구현하는 것을 목표로 한다.

② 비정형(informal) 접근법은 구조적인 방법론에 기반하지 않고 전문가의 지식과 경험에 따라 위험을 분석하는 것으로, 비교적 신속하고 저비용으로 진행할 수 있으나 특정 전문가의 견해 및 편견에 따라 왜곡될 우려가 있다.

③ 상세(detailed) 위험분석은 정형화되고 구조화된 프로세스를 사용하여 상세한 위험평가를 수행하는 것으로, 많은 시간과 비용이 드는 단점이 있는 반면에 위험에 따른 손실과 보안 대책의 비용 간의 적절한 균형을 이룰 수 있는 장점이 있다.

④ 복합(combined) 접근법은 상세 위험분석을 제외한 기준 접근법과 비정형 접근법 두 가지를 조합한 것으로 저비용으로 빠른시간 내에 필요한 통제 수단을 선택해야 하는 상황에서 제한적으로 활용된다.

♤ **위험분석 방법**

• **복합(combined) 접근법**은 **상세 위험분석**을 **제외**한 기준 접근법과 비정형 접근법 두 가지를 조합한 것으로 저비용으로 빠른시간 내에 필요한 통제 수단을 선택해야 하는 상황에서 제한적으로 활용된다.(×) → **복합 접근법**은 **상세 위험분석**과 **베이스라인 접근법**을 같이 사용하는 방식이다.

// 베이스라인 접근법(baseline approach)

• **체크리스트**를 이용한 위험분석 방법이다.
• 모든 시스템에 대한 **표준** 보호대책을 체크리스트로 제공한다.

// 비정형 접근법(informal approach)

• **경험자의 지식**을 사용하여 위험분석을 수행하는 것이다.
• 이 방법은 구조적인 방법론에 기반하지 않는다.

// 상세 위험분석(detailed risk analysis)

• **모든** 정보자산에 대해 **상세**하게 위험분석을 실시한다.
• **"자산분석, 위협분석, 취약성분석"**의 각 단계를 수행하여 위험을 평가한다.

// 복합 접근법(combined approach)

• 상세 위험분석과 베이스라인 접근법을 같이 사용하는 방식이다.
• **상세** 위험분석 : **고위험(high risk) 영역** 분석
• **베이스라인** 접근법 : 그 외의 다른 영역

정답 : ④

10. ISMS-P 인증기준의 세 영역 중 하나인 관리체계 수립 및 운영에 해당하지 않는 것은? [2023년 지방 9급]

① 관리체계 기반 마련
② 위험관리
③ 관리체계 점검 및 개선
④ 정책, 조직, 자산 관리

♤ ISMS-P 인증기준

구분		영역	분야(인증기준)
ISMS-P	ISMS	1. 관리체계 수립 및 운영(16개) ↓ 필수영역, PDCA 모델 적용	1.1 관리체계 기반 마련(6) 1.2 위험관리(4) 1.3 관리체계 운영(3) 1.4 관리체계 점검 및 개선(3)
		2. 보호대책 요구사항(64개) ↓ 선택영역 해당사항이 없으면 이유를 제시 (현실적으로는 모두 인증을 받음)	2.1 **정책, 조직, 자산 관리**(3) 2.2 인적보안(6) 2.3 외부자 보안(4) 2.4 물리보안(7) 2.5 인증 및 권한 관리(6) 2.6 접근통제(7) 2.7 암호화 적용(2) 2.8 정보시스템 도입 및 개발 보안(6) 2.9 시스템 및 서비스 운영관리(7) 2.10 시스템 및 서비스 보안관리(9) 2.11 사고 예방 및 대응(5) 2.12 재해복구(2)
	–	3. 개인정보 처리단계별 요구사항(22개) ↓ 준거성(법률)	3.1 개인정보 수집 시 보호조치(7) 3.2 개인정보 보유 및 이용 시 보호조치(5) 3.3 개인정보 제공 시 보호조치(4) 3.4 개인정보 파기 시 보호조치(3) 3.5 정보주체 권리보호(3)

- **관리체계 수립 및 운영영역**은 PDCA 모델의 Plan, Do, Check, Act의 사이클에 따라 지속적이고 반복적으로 실행되는지 평가한다.
- **정책, 조직, 자산 관리**는 **보호대책 요구사항**이다.

정답 : ④