정보보호론	국가 전산 7급	2021년 9월 11일

♠ 필기합격인원/합격선(52명/84점) - 선발예정인원 42명 ♠

1. 사용자 인증에 사용되는 기술로 옳지 않은 것은? [2021년 국가 7급]

① Smart Card
② Single Sign On
③ One Time Password
④ Supervisory Control And Data Acquisition

♤ **사용자 인증에 사용되는 기술**

- 사용자 인증 : Smart Card, Single Sign On, One Time Password, 지문 등을 이용

// 스카다(Supervisory Control And Data Acquisition, SCADA) - 감독 제어 및 데이터 수집

- 스카다는 감독 제어 및 데이터 수집의 약자이다.
- 스카다 시스템은 광범위한 산업 분야에서 시용되어 중요한 역할을 수행한다.
- 기업은 스카다 시스템을 사용하여 작업 현장에 투입된 모든 **장비를 제어**하고 **데이터를 수집**한다.
- 스카다는 프로그램 로직제어기와 원격단말장치 같은 하드웨어의 조합으로 구성된다.

정답 : ④

2. 제로 데이 공격에 대한 설명으로 옳은 것은? [2021년 국가 7급]

① 서버의 성능을 크게 떨어뜨리거나 서버를 정지시키는 방법으로 서버의 정상적인 작동을 방해하는 공격 방법이다.
② 패스워드 사전 파일을 이용해 미리 지정한 아이디에 대입하여 접속계정을 알아내는 공격 방법이다.
③ 패치가 나오지 않은 시점에 이루어지는 공격 방법이다.
④ 버퍼에 일정 크기 이상의 데이터를 입력하여 프로그램을 공격하는 방법이다.

♤ **제로 데이 공격**

- 제로 데이 공격은 소프트웨어 취약점에 대한 **패치가 나오기 전**에 이루어지는 공격이다.
- 사람들이 많이 사용하는 소프트웨어일수록, 의외로 많은 제로 데이 공격이 발생된다.
- 제로 데이 공격 탐지에는 **이상탐지기법**이 적합하다.

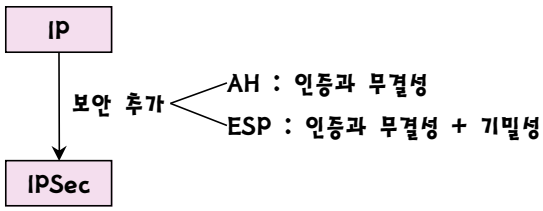
정답 : ③

3. IPSec 프로토콜의 기능이 아닌 것은? [2021년 국가 7급]

① Pretty Good Privacy ② Authentication Header
③ Internet Key Exchange ④ Encapsulating Security Payload

♤ IPSec 프로토콜

• IPSec은 개방형 IP(internet protocol)에 보안 기능을 첨가한 것이다.



• **인터넷 키 교환(internet key exchange)**는 IPsec에서 보안 연관(SA) 생성을 위한 프로토콜이다.

• PGP는 안전한 **전자우편**을 위해 Phil Zimmermann에 의해 개발되었다.

정답 : ①

4. 다음 설명에 해당하는 악성코드는? [2021년 국가 7급]

○ 사용자 동의 없이 설치되어 컴퓨터의 정보를 수집하고 전송하는 악성소프트웨어
○ 신용카드와 같은 금융정보 및 주민등록번호와 같은 신상정보, 암호를 비롯한 각종 정보를 수집

---

① ransomware ② spyware
③ backdoor ④ dropper

♤ 악성코드 – 스파이웨어(Spyware)

• Spyware는 사용자 동의 없이 설치되어 정보를 수집하고 전송하는 악성 소프트웨어이다.
• Spyware는 금융정보, 신상정보, 암호 등을 비롯한 각종 정보를 수집한다.

// 드로퍼(dropper)
• 드로퍼는 악성코드(백도어 등)를 대상 시스템에 설치하기 위해 설계된 악성 프로그램이다.
• **단계 1** : 악성코드는 **드로퍼 내에 압축된 형태로 포함**되어 바이러스 백신에 의한 **탐지**를 피하고
• **단계 2** : 드로퍼가 실행될 때, **악성코드가 생성**되어 시스템을 감염시킨다.

정답 : ②

5. 다음 설명에 해당하는 블루투스 공격을 옳게 짝지은 것은? [2021년 국가 7급]

(가) 공격이 가능한 블루투스 장치들을 검색하고 모델을 확인하는 공격
(나) 블루투스 장치 내 저장된 데이터에 대한 접근을 허용하는 공격
(다) 블루투스 지원 장치에 대한 접근권한을 획득하는 공격

	(가)	(나)	(다)
①	bluesnarf	bluebug	blueprinting
②	bluesnarf	blueprinting	bluebug
③	blueprinting	bluebug	bluesnarf
④	blueprinting	bluesnarf	bluebug

♤ **블루투스 공격**

// 블루버그(bluebug)

- 블루버그는 **장비 연결 인증 취약점**을 이용한 공격이다.**(장비에 대한 접근권한을 획득)**
- 블루버그는 블루투스 장비 사이의 취약한 연결 관리를 악용한 공격이다.
- 블루투스 장비들은 한 번 연결되면, 이후에는 자동으로 서로 연결된다.

// 블루스나프(bluesnarf)

- 블루스나프는 블루투스의 취약점을 이용하여 **장비의 임의 파일의 데이터에 접근하는 공격**이다.
- 공격자는 블루투스의 OPP(OBEX Push Profile) 기능을 사용한다.
- OPP는 블루투스 장치끼리 인증 없이 간편하게 정보를 교환할 수 있는 기능이다.
- OBEX는 Object Exchange이다.

// 블루프린팅(blueprinting) – 청사진

- 블루프린팅은 블루투스 **공격 장치를 검색하는 활동을 의미**한다.
- 공격자는 블루투스의 서비스 발견 프로토콜(SDP, Service Discovery Protocol)을 이용
- SDP는 블루투스 장치 간 종류를 식별하기 위해 주고받는 것이다.
- 공격자는 SDP를 이용해 **공격이 가능한 블루투스 장치를 검색하고 모델을 확인**

// 블루재킹(bluejacking)

- 익명으로 블루투스 사용자에게 **스팸메시지를 보내는 기법**이다.(일명, 블루스패핑)
- 블루재킹은 보안 위협은 상대적으로 적다.
- 블루재킹은 10m 범위 내에서 가능하다.
- 블루재킹을 방지하려면 기기를 비인지 모드로 하면 된다.

정답 : ④

6. 암호화에 대한 설명으로 옳은 것은? [2021년 국가 7급]

① 대칭키 암호 방식은 암호화 키와 복호화 키가 다른 암호화 방법으로 암호화 키는 공개되고, 복호화 키는 공개되지 않는 구조로서 다수의 정보교환자 간의 통신에 적합하다.

② 공개키 암호에는 RSA, ElGamal 등이 있으며, 처리속도가 대칭키 알고리즘에 비해 매우 느린 단점이 있으나 키 전달이 편리하여 키교환 알고리즘으로 사용되며, 전자서명을 용이하게 구현할 수 있는 특징이 있다.

③ 블록 암호는 이진화된 평문과 키 이진수열을 배타적 논리합 이진 연산으로 결합하여 암호문을 생성하고, 블록 대칭 알고리즘에는 선형 쉬프트 레지스터 등이 있다.

④ 공개키 암호 방식은 암호화 키와 복호화 키가 동일한 암호화 방법으로 두 키가 동일하게 이용되며, 데이터를 변화하는 방법에 따라서 스트림암호와 블록암호로 나누어지고 기밀성용으로만 사용된다.

♤ **암호화**

---

① **대칭키 암호** 방식은 **암호화 키와 복호화 키가 다른 암호**화 방법으로 **암호화 키는 공개**되고, 복호화 키는 공개되지 않는 구조로서 다수의 정보교환자 간의 통신에 적합하다.**(×)**

→ **대칭키 암호 : 암호화 키와 복호화 키가** 같다.

③ **블록 암호**는 이진화된 평문과 키 이진수열을 배타적 논리합 이진 연산으로 결합하여 암호문을 생성하고, 블록 대칭 알고리즘에는 선형 쉬프트 레지스터 등이 있다.**(×)**

→ **스트림 암호** : 평문과 키 이진수열을 배타적 논리합 연산으로 암호문 생성

④ **공개키 암호** 방식은 **암호화 키와 복호화 키가 동일한 암호**화 방법으로 두 키가 동일하게 이용되며, 데이터를 변화하는 방법에 따라서 **스트림암호**와 **블록암호**로 나누어지고 기밀성용으로만 사용된다.**(×)**

→ **공개키 암호** : **암호화 키와 복호화 키가 서로** 다르다. **대칭키 암호 :** 스트림암호와 블록암호로 구분

정답 : ②

7. 해시에 대한 설명으로 옳지 않은 것은? [2021년 국가 7급]

① 해시 알고리즘에는 MD5, SHA 등이 있다.

② 해시는 메시지의 무결성을 확인하기 위해서 사용한다.

③ 해시 알고리즘 SHA는 유럽 RIPE 프로젝트에 의해 개발된 해시함수이다.

④ 해시는 임의의 길이 메시지로부터 고정길이의 해시값을 계산한다.

♤ **해시함수**

• 해시 알고리즘 SHA는 **유럽** RIPE 프로젝트에 의해 개발된 해시함수이다.**(×)**

→ SHA는 **미국** 국립표준기술연구소(NIST)에서 발표한 해시함수이다.

정답 : ③

8. PPTP 프로토콜에 대한 설명으로 옳은 것은? [2021년 국가 7급]

① 3계층인 네트워크 계층에서 동작한다.
② 마이크로소프트가 제안한 VPN 프로토콜로 PPP를 기반으로 한다.
③ 데이터를 스니핑한 뒤 해당 데이터를 다시 보내는 replay attack을 막을 수 있다.
④ 데이터가 전송 도중에 변조되었는지를 확인할 수 있도록 데이터 무결성을 검사한다.

♤ **PPTP(Point-to-Point Tunneling Protocol) – 지점간 터널링 프로토콜**

- 마이크로소프트가 제안한 VPN 프로토콜로 PPP를 기반으로 한다.(RFC 2637로 표준화)
- PPTP는 OSI 2계층에서 동작한다.
- 현재, PPTP는 **심각한 보안 취약성**을 갖는다.**(최소한의 보안 지원) – RC4 암호(XOR 연산)** 채택
- PPTP는 **재전송 공격**(replay attack)이 가능하고, **데이터 무결성**을 보장하지 못한다.
- 지금, PPTP는 IPSec 등으로 대체되었다.

정답 : ②

9. 개인정보 보호법 제24조의2(주민등록번호 처리의 제한)에서 제24조제1항에도 불구하고 개인정보처리자가 주민등록번호를 처리할 수 있는 경우가 아닌 것은? [2021년 국가 7급]

① 수탁자가 위탁받은 해당 업무 범위를 초과하여 개인정보를 이용하거나 제3자에게 제공하는 경우
② 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 명백히 필요하다고 인정되는 경우
③ 제24조의2제1항제1호 및 제2호에 준하여 주민등록번호 처리가 불가피한 경우로서 개인정보 보호위원회가 고시로 정하는 경우
④ 법률 · 대통령령 · 국회규칙·대법원규칙 · 헌법재판소규칙 · 중앙선거관리위원회규칙 및 감사원규칙에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우

♤ **개인정보 보호법 – 제24조의2(주민등록번호 처리의 제한)**

① 제24조제1항에도 불구하고 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 주민등록번호를 처리할 수 없다. 〈개정 2016. 3. 29., 2017. 7. 26., 2020. 2. 4.〉
1. 법률 · 대통령령 · 국회규칙 · 대법원규칙 · 헌법재판소규칙 · 중앙선거관리위원회규칙 및 감사원규칙에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우
2. 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 명백히 필요하다고 인정되는 경우
3. 제1호 및 제2호에 준하여 주민등록번호 처리가 불가피한 경우로서 보호위원회가 고시로 정하는 경우

정답 : ①

10. 블록체인의 비트코인 블록 헤더구조에 대한 설명으로 옳지 않은 것은? [2021년 국가 7급]

① Nonce는 4바이트로 구성된다.
② Timestamp는 블록을 생성한 시간이다.
③ Previous Block Hash는 32바이트로 구성된다.
④ Block Header는 5가지 필드로 구성하고 크기는 60바이트로 고정되어 있다.

♤ 블록체인의 비트코인 블록 헤더구조

• 비트코인 블록은 크게 헤더(header)와 바디(body)로 이루어져 있다.

	블록해시	→ 현재 블록 해시값(hash of the block), 식별자 역할
헤더 (header)	버전(version) – **4byte**	→ 블록헤더를 만든 비트코인 프로그램 버전
	이전 블록해시 – **32byte**	→ 이전 블록헤더를 **SHA-256**으로 **2번 연속 해시**한 값
	머클루트 – **32byte**	→ 바디에 저장된 거래정보 해시값(2진트리구조에서 루트값)
	타임스탬프 – **4byte**	→ 해당 블록의 생성시간(1970년 1월 1일 이후 초단위 계산)
	난이도(bits) – **4byte**	→ bits는 난이도 조절용 수치, nonce 찾기 위한 어려운 정도
	비표(nonce) – **4byte**	→ 블록 생성을 위한 해시값을 구할 때 필요한 재료 역할
	거래 수	
바디 (body)	거래 리스트 (transaction list)	→ 해당 블록에 기재된 모든 이체내역을 담는다. → 다수의 거래정보 묶음 → 평균 약 1,800개의 거래정보가 포함될 수 있다.

• **각 블록**은 최대 1MB 크기까지 확장될 수 있다.
• 현재, 블록을 2MB로 늘려야 한다고 제안된 상태
• 헤더 80byte, 기타 17byte를 제외하고 약 1,048,479byte에 거래내역을 저장할 수 있다.
• **블록해시(hash of the block)**는 일종의 '블록' 이름 정보이다.
• 블록해시는 블록의 헤더 정보를 모두 더한 합을 구하여 SHA-256으로 변환한 값이다.
• 합 = 버전 + 이전 블록해시 + 머클루트 + 타임 + bits + 논스
• 이름은 **블록해시**이지만, 블록 전체를 해시한 값이 아니고 **블록헤더를 해시한 값**이다.
• nonce는 0에서 시작하여 난이도 조건을 만족하는 해시값을 찾을 때까지 1씩 증가시킨다.
• **작업증명(proof of work)**은 **블록해시**가 특정 값보다 **작은 값**이 나오는 **nonce를 찾는 것**이다.
• 여기서, 특정 값은 난이도 목표값이며 bits 값으로 프로그램에서 자동 제시한다.
• 난이도 목표값 조정은 평균 10분당 하나의 블록이 생성되도록 조절한다.
• 즉, 난이도 목표값 조건을 만족하는 블록해시값을 찾았을 때, **작업증명**이 성공한 것이다.
• 보상 = 새로 발행되는 비트코인 + 해당 블록에 포함되는 거래의 거래 수수료

정답 : ④