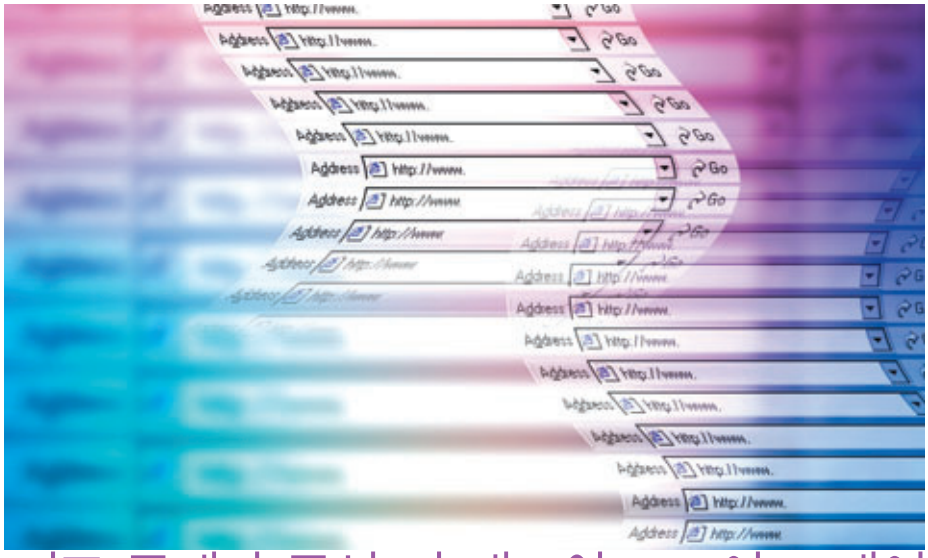
+ 허종오 · 한국 CISSP협회 연구분과 이사, 전자계산기기술사



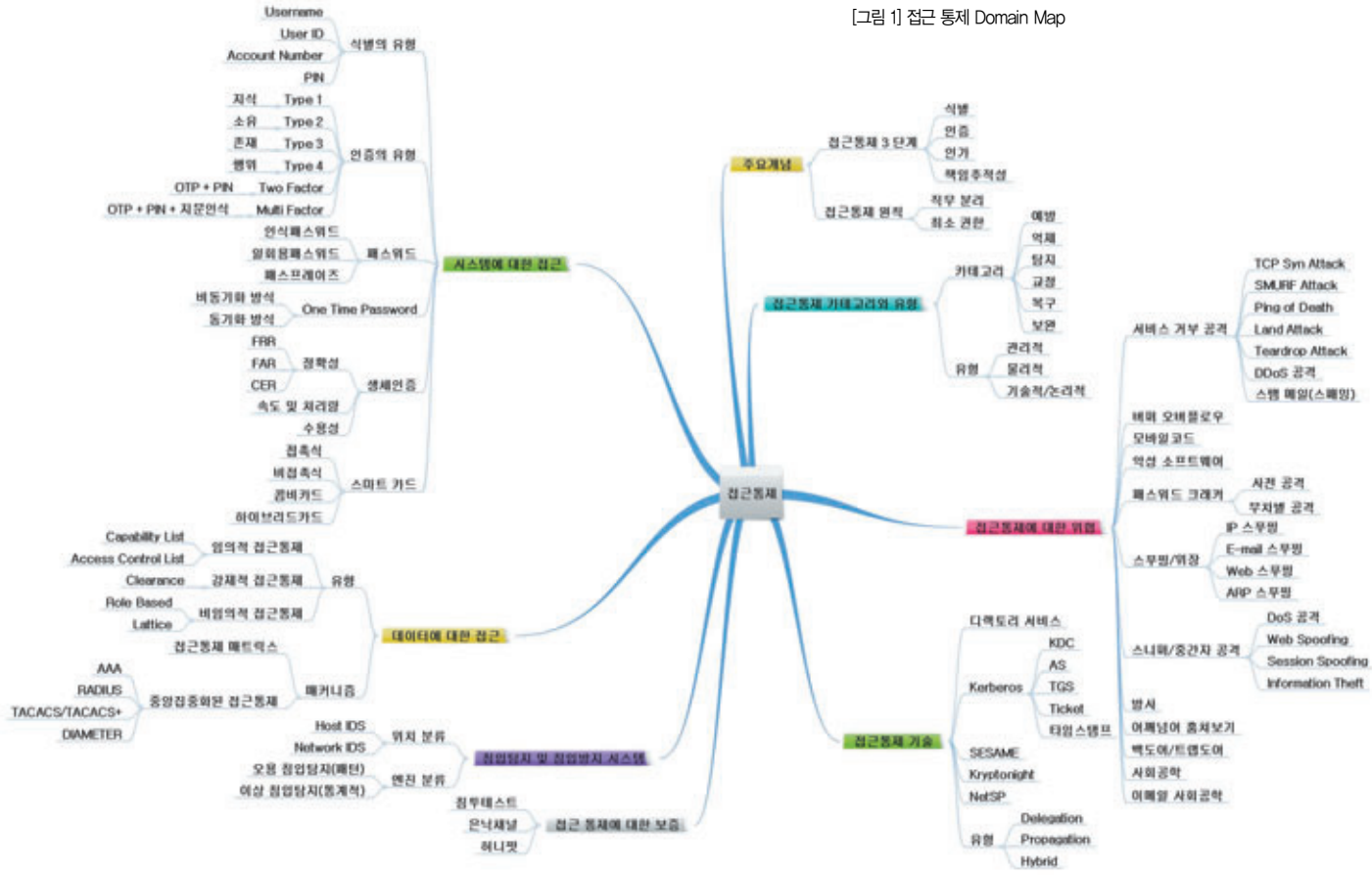
접근 통제와 통신 및 네트워크 보안 도메인

지난 호에서는 정보보호 및 위험관리, 보안 아키텍처 도메인에 대한 요점정리와 연습문제를 통해 CISSP가 되기 위해서 공부해야 될 부분과 어떤 문제가 출제될 수 있는지 알아보았다.
이번 호에서는 CISSP의 10개 도메인 중에서 기술적 부분을 설명하는 접근 통제와 통신 및 네트워크 보안 도메인에 대해서 알아보자.

1. 접근 통제(Access Control) 요점정리

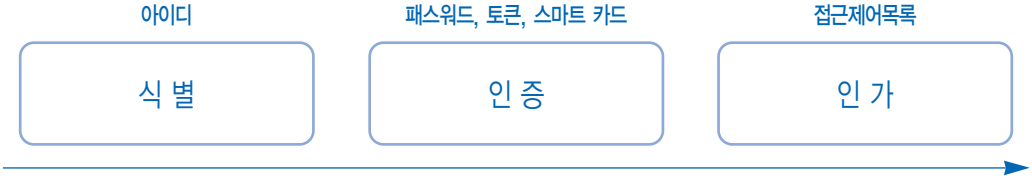
접근 통제 도메인은 CISSP가 외부 위협과 비인가자의 접근으로부터 조직의 시스템을 보호하고 접근이 승인된 사용자에 대해서는 시스템 접근 권한을 부여하는 절차를 설명하는 도메인이다. 접근 통제 도메인을 학습함으로써, 시스템 사용자(주체: Subject)와 대상 시스템(객체: Object)간에 발생하는 활동(접근: Access)간의 관계와 관련 시스템의 구성을 한 눈에 볼 수 있는 안목을 가질 수 있는 도메인이다.
접근 통제 도메인에서 학습해야 할 요점들은 다음 Domain Map을 통해 한 눈에 알 수 있다.

[그림 1] 접근 통제 Domain Map



1-1. 접근 통제의 3가지 단계

접근 통제의 3가지 중요한 단계는 식별(Identification), 인증(Authentication), 인가(Authorization)이다. 절차를 도식화 해보면 [그림 2]와 같다.



[그림 2] 접근 통제의 3 단계

최근에는 접근 통제 3단계에 사용자 행동을 기록하는 책임추적성이 추가되어 접근 통제 3단계 +1이라고 불린다. 책임추적성을 추가한 접근 통제 3단계 +1의 구성은 [표 1]을 통해 자세히 알아보자.

[표 1] 접근 통제의 3단계 +1 구성요소

주요 용어	설명	예
식별 (Identification)	식별은 인증 서비스에 스스로를 확인시키기 위하여 정보를 공급하는 주체의 활동이다.	사용자명, 계정번호, 메모리 카드
인증 (Authentication)	주체의 신원을 검증하기 위한 사용 증명 활동이다. 인증을 위해 사용되는 네 가지 특징 – 주체는 그가 알고 있는 것을 보여주어야 한다.(Something you know : 지식) – 주체는 그가 가지고 있는 것을 보여주어야 한다.(Something you have : 소유) – 주체는 그를 나타내는 것을 보여주어야 한다.(Something you are : 존재) – 주체는 그가 하는 것을 보여주어야 한다.(Something you do : 행위) ☞ 하나의 매커니즘 사용 시 단일(one-factor) 인증, 두 가지 경우 이중(two-factor) 인증 ☞ 강한 인증으로 생각되려면 위의 세 가지 매커니즘 중에서 최소한 두 가지 사용, Multi-Factor 인증	– 패스워드, PIN – 토큰, 스마트 카드 – 생체인증(지문, 정맥) – 움직임, 음성, 터치, 서명
인가 (Authorization)	인증된 주체에게 접근을 허용하고 특정 업무를 수행 할 권리를 부여하는 과정 – 클리어런스(Clearance) : 주체가 지니고 있는 보안 수준으로서, 주체가 접근 할 수 있는 객체를 직접적 으로 규정하는 것이다. – 알 필요성(need-to-know) : 주체에 있어서 어떤 정보가 유용해야 할지의 여부와 관계가 있는 공인된 형식상의 접근 수준	접근 제어 목록(ACL), 보안 등급
책임추적성 (Accountability)	– 사용자의 이용을 추적하고 그의 행동들에 대해 기록하고 추적하는 활동 – 책임추적이 가장 어려운 경우는 하나의 계정을 여러 명이 공유하는 것이다.	접근 통제를 강화하기 위한 SW

1-2. 접근 통제에 대한 위협

접근 통제 시스템의 보안성을 위협하는 각종 사례들이 최근에 증가하고 있다. 하지만, 이러한 최신 공격들은 갑자기 나타난 것이 아니라, 기존에 발생한 공격들을 모방하거나, 변형하여 발생하는 공격들이다. 따라서, 기본적인 위협들을 잘 정리해두면, 새로운 공격들이 나오더라도 어떤 공격을 기반으로 변형되었는지, 어떤 방법으로 대응해야 되는지를 알 수 있다.

(1) TCP Syn Attack

– 위장(Spoofed)된 Attacker로부터 너무 많은 연결요청이 오도록 해서 대상 시스템이 Flooding(홍수) 되게 만들어 공격 대상 시스템의 메모리가 바닥나게 하여 서비스를 하지 못하도록 하는 공격

– 대응책 : Connection Time Out 시간을 단축, 네트워크 보안장비 설치(IDS, IPS 등)

(2) SMURF Attack

– 광범위한 효과로 DoS 공격 중 가장 피해가 크며, 가장 빈번하게 발생하는 공격 형태 중 하나로써 IP와 ICMP를 이용함.

– 다이렉트 브로드캐스트(Direct Broadcast)와 세 가지 구성요소인 3Player(공격자, 증폭 네트워크, 표적)를 이용

– 대응책 : 라우터를 통해 다이렉트 브로드캐스트 발생을 차단

(3) Land Attack

- 공격자가 임의로 자신의 IP Address와 Port를 대상 서버와 IP Address와 Port와 동일하게 하여 서버에 접속하는 공격 방식.
- 대응책 : 자신의 시스템 주소와 동일한 소스 주소를 가진 외부 패킷을 필터링

(4) 버퍼오버플로우

- 버퍼에 입력되는 정보에 대해 한계체크가 실행되지 않을 경우 데이터의 긴 문자열이 받아들여질 수 있으며, 이로 인해 입력된 데이터가 할당된 메모리 버퍼보다 크다면 데이터는 또 다른 메모리 세그먼트로 흘러넘치게 된다.
- 대응책 : 버퍼오버플로우는 파라미터(parameter) 체크를 통해 방지 할 수 있다.

(5) 악성 소프트웨어(Malicious Software, Malware)

- 바이러스나 웜, 트로이 목마, 스파이웨어와 같이 컴퓨터 또는 네트워크에 해를 입히거나 보안을 무력화시켜 정보를 빼내거나, 사용자가 원하지 않는 작업을 하도록 설계된 소프트웨어로서, 악성 코드(Malicious Code)라고 불리기도 한다.
- 대응책 : 악성코드 탐지 소프트웨어 사용(Anti-Virus, Anti-Software)

지금까지 주요 보안 위협에 대해서 정리해 보았다. 이외에도 스팸메일, 스푸핑, 스니퍼, 패스워드크래커, 모바일 코드를 이용한 공격, 사회공학 공격 등 다양한 위협이 존재한다.

1-3. 시스템에 대한 접근

시스템에 대한 접근 통제 기술로서 주로 사용되는 것이 앞에서 학습한 식별, 인증이다. 이렇게 식별, 인증을 거쳐 시스템에 접근한 후에는 다른 시스템에 접근하기 위해 또 다시 인증을 받지 않고, 타 시스템에 편리하게 연동하기 위해서는 단일 인증체계로 불리는 SSO(Single Sign On)가 필요하다.

즉, SSO는 식별, 인증을 한 번의 인증으로 완료하는 편리한 시스템으로서 거의 모든 조직에서 활용하고 있다. SSO는 Delegation(인증대행), Propagation(인증정보 전달) 방법으로 구분된다.

[표 2] SSO의 유형

구분	설 명
인증대행 (Delegation)	- 각 시스템의 인증정보를 한 곳에 모아두고 시스템 접근 시마다 인증을 대행하는 방식 - 대표적으로 디렉토리 서비스(Directory Service)가 있음.
인증정보 전달 (Propation)	- 각 시스템 접근 시 미리 인증된 인증 토큰 또는 티켓의 유효성만 검사하는 방식 - 대표적으로 Kerberos, SESAM가 있음.

1-4. 데이터에 대한 접근

실질적으로 모든 주체(사용자)가 객체(시스템)에 접근하여 얻고자 하는 것은 데이터이다. 하지만, 모든 주체들이 데이터에 대한 접근에서 동일한 권한을 가지는 것은 아니다. 따라서, 주체에 따라 데이터에 대한 접근 권한을 부여하는 방식에 대해 알아보자.

[표 3] 데이터에 대한 접근 권한 부여 방식

구분	설 명
DAC	– 임의적 접근 통제(Discretionary Access Control) – 주체의 신원에 근거하여 객체에 대한 접근을 제한하는 방법으로 접근 통제 매트릭스를 통해 주체와 객체의 접근 권한을 명시함. – 주체가 증가 할 경우 관리의 어려움이 증가하는 문제가 있음.
MAC	– 강제적 접근 통제(Mandatory Access Control) – 비밀성을 갖는 객체의 비밀 등급과 대해 주체가 갖는 비밀등급을 비교하여 접근을 제어하는 방법. – 실제 시스템 구현 및 관리의 어려움이 존재함.
RBAC	– 역할 기반 접근 통제(Role Based Access Control) – DAC와 MAC의 단점을 극복하기 위해 두 방식의 장점을 발전시킨 방식임. – 관리와 구현의 편리성을 위해 역할(Role)에 권한을 부여하고, 사용자를 각 역할에 할당하는 방식임.

1-5. 접근 통제에 대한 보증

지금까지 각종 위협과 비인가자로부터의 조직의 시스템과 데이터를 보호하기 위해 시스템 접근 통제 방식과 데이터 접근 통제 방식에 대해 살펴보았다. 하지만, 실제 공격이 발생하기 전까지는 시스템 접근 통제 방식과 데이터 접근 통제 방식을 제대로 구축했는지 알 수는 없다. 따라서, 조직 내에 구축한 통제 방식들이 제대로 구축되었는지를 평가하는 방법이 접근 통제에 대한 보증이라고 할 수 있다.

주요 보증기법으로는 외부의 위협처럼, 실제 시스템을 공격하는 방법인 침투 테스트(Penetration Test)가 있으며, 이 테스트를 통해 알려지지 않은 조직 내 취약점을 사전에 발견하여 조치 할 수 있다. 그 외의 보증기법으로는 통제 시스템을 우회하는 은닉 채널(Covert Channel)을 찾아 조치하는 것과 외부의 공격을 사전에 예방하는 허니팟(Honey Pot) 또는 허니넷(Honey Net) 시스템 구축이 필요하다.

지금까지 접근 통제에 대해서 살펴보았다. 접근 통제는 기업의 정보보호 기술에 대한 내용으로서 CISSP 합격을 위해서는 꼭 필요한 기술적 지식을 제공한다. 따라서, 충분한 학습이 필요하다.

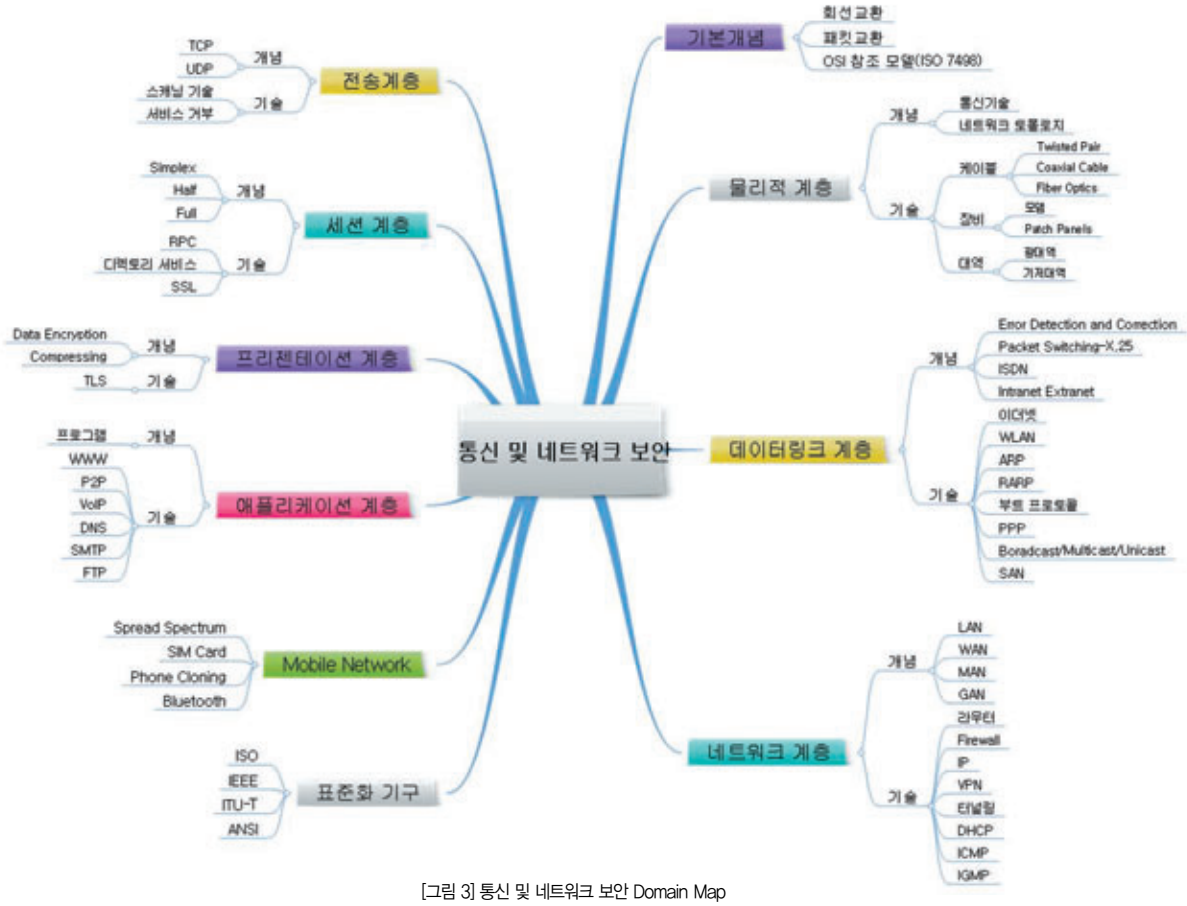
[표 4] 접근 통제 Key Factor

분야	Key Factor	출제비중
접근 통제	– 접근 통제 보안 모델에 대한 숙지 – 식별 및 인증 기술과 기법 숙지 – 접근 통제 관리 학습 – 데이터 소유권 학습 – 공격 방식 및 대응 방법에 대한 학습	높음

정리해보면, 접근 통제 부분에 주로 출제되는 주요 부분(Key Factor)은 [표 4]와 같다. 또한, 접근 통제는 전통적으로 많은 문제가 출제되는 중요한 도메인이다. 따라서, 출제비중은 "높음"이다.

2. 통신 및 네트워크 보안(Telecommunications and Network Security) 요점정리

통신 및 네트워크보안은 Mesh 형태인 인터넷의 급속한 발전으로 중요성이 증가한 도메인이다. 최근에는 이동 통신, 무선분야에 대한 보안의 중요도가 증가하고 있다. 통신 및 네트워크보안은 접근 통제와 같이 기술적인 지식을 제공하는 도메인으로서, 먼저 통신에 대한 기술적 지식을 OSI 7 Layer 모델을 통해 정리하고, 각 Layer별 위협 및 대응책에 대한 학습이 필요한 분야이다.

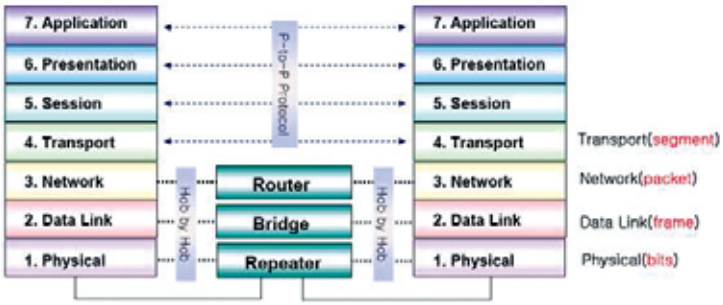


[그림 3] 통신 및 네트워크 보안 Domain Map

2-1. OSI 7 Layer 모델

OSI 7 Layer 모델은 [그림 4]를 통해 한 눈에 볼 수 있다. 참고로 모델이라는 의미는 이상적인 모습을 그려 놓은 것을 의미하는 것으로 통신 프로그램 개발자나 통신장비 제작 업체들은 OSI 7 Layer 모델에서 자신에게 필요한 계층과 필요한 프로토콜만 사용한다.

OSI 7 Layer는 Layering과 Encapsulation이라는 두 가지 키워드로 구조를 정리 할 수 있다. Layering은 각 계층들이 상호간에 독립성을 보장하면서, 계층화되는 것을 말한다. 따라서, 각 계층 구분을 통해 시스템 고장 발생 시 발생 원인을 찾을 수 있는 장점이 있다. 또한, 발신자 측에서 데이터 송신 시 상위 계층에서 하위 계층으로 이동하면서 전송하는 데이터에 추가정보인 Header와 Trailer가 데이터의 앞 · 뒤로 붙게 된다. 이것이 Encapsulation이다. 반대로 수신자 측에서는 하위계층에서 상위계층으로 올라가면서, 데이터에 붙어 있는 Header와 Trailer를 분석하고, 제거하면서 결국 발신자가 전송한 데이터는 응용 서비스를 통해 사용자에게 전달된다.



[그림 4] OSI 7 Layer 모델

[표 5] OSI 7 Layer 모델의 역할 및 기능

계층	역할	데이터 종류	기능/프로토콜
Application	각종 응용 서비스 제공	Message	FTP, SMTP, DNS, LPD, WWW, Telnet 등
Presentation	암호화, 압축 제공	Message	Mpeg, Jpg 등
Session	동기화 세션 연결/관리/종료	Message	전송모드 결정(반이중, 전이중 등)
Transport	데이터 전송	Segment	TCP, UDP
Network	통신 경로 설정(Routing)	Packet	X.25, Frame Relay, MPLS, IP
Data Link	오류제어, Frame화	Frame	BEC, FEC, 해밍코드, ARP, RARP
Physical	물리적 연결설정, 전기적 신호	Bit Stream	전기적 신호

[표 5]를 이해하고 암기하고 있다면, 네트워크 보안 도메인 학습은 거의 끝났다고 볼 수도 있다. 그 만큼 해당 표는 중요하다고 할 수 있다.

2-1-1. Layer 1 : 물리적 계층

(1) 역할

- 통신회선으로 Data를 나타내는 '0'과 '1' 비트의 정보를 회선에 내보내기 위한 전기적 변환이나 기계적 작업을 담당

(2) 주요 기술

- 네트워크 토폴로지 : 네트워크의 구성을 뜻하는 것으로 Bus형, Star형, Ring형, Tree형, Mesh형 등이 있다.
- 케이블 : 1계층에서 네트워크를 구성하는 가장 중요한 장치로서 각 네트워크 장비들 간의 연결을 하는 장치이다. 케이블은 전기적 또는 광 신호를 전달하는 장치로서, Twisted Pair Cable(꼬임 케이블), Coaxial Cable(동축 케이블), Fiber Optics Cable(광케이블) 등이 있다.

(3) 위협

- 1계층에서 발생하는 위협으로는 전기적, 환경적 간섭으로 발생하는 Noise(잡음), Attenuation(감쇄), Crosstalk(혼선) 등이 있다.

(4) 대응책

- 위협에 대한 대응책으로는 전기적, 환경적 간섭을 차단하기 위해 차폐막을 설치하는 Shield(차폐)와 케이블을 길이를 단축하는 것이다. 또한, 전기적 장애에 강하고, 먼 거리까지 신호를 전달하는 광케이블로 케이블을 대체하는 것이 있다.

2-1-2. Layer 2 : 데이터 링크 계층

(1) 역할

- 데이터 링크 계층은 3계층과 1계층 네트워크 내에서 물리적인 링크를 확립하고, Packet을 Frame화하며, 발생한 Frame 오류 등을 찾아 복구하는 계층이다.

(2) 주요 기술

- LLC(Logical Link Control) : 논리적 연결제어로서 물리적 계층 간의 연결을 담당.
- MAC(Media Access Control) : 전기적으로 연결된 케이블 내에서 신호 간의 충돌을 피하기 위한 규칙을 제공. 이러한 규칙으로, CSMA/CD와 CSMA/CA를 제공한다.
- 데이터 프레이밍 : 3계층과 1계층 사이에서 Packet을 작은 단위인 Frame으로 변환시킨다.
- 오류 탐지와 처리 : 순환 잉여검사(CRC) 등을 통해 데이터의 오류를 탐지하고 처리한다.
- 네트워크 연결 기술로서 X.25, Frame Relay, ATM, MPLS, ISDN, DSL 등이 관여된 계층이다.
- 프로토콜로는 ARP, RARP, BOOTP, PPP 등이 있다.

(3) 위협

- ARP Cache Poisoning, 전기적 충돌 등이 있다.

(4) 대응책

- ARP Cache Poisoning은 라우터 테이블을 Static 라우팅으로 변경함으로 해결 가능하다.
- 전기적 충돌은 CSMA/CD와 CSMA/CA를 통해 해결 가능하다.

2-1-3. Layer 3 : 네트워크 계층

네트워크 계층은 OSI 7 Layer 모델에서 4계층의 전송계층과 더불어 가장 중요한 역할을 하는 계층이다. 실질적으로 인터넷에 연결되는 계층으로 IP가 존재하는 프로토콜이기 때문이다.

(1) 역할

- 시스템 간에 Data를 전송하기 위한 최선의 통신 경로를 선택하는 Routing(라우팅)을 담당

(2) 주요 기술

- LAN : Router(라우터)를 기점으로 내부는 Local Area Network로 구분.
- WAN : Router(라우터)를 기점으로 외부는 Wide Area Network로 구분.
- MAN : LAN과 WAN에 이은 신개념으로 100Km 이내의 도시권을 연결하는 도시지역 통신망.
- GAN : 기업의 본사내 LAN을 세계 각지의 지점과 연결하는 Global Area Network
- Router : 수신된 패킷을 어느 선로에 실어 보낼지를 결정하고 전송하는 역할을 담당.
- Firewall(방화벽) : 외부로부터의 불법 침입과 내부의 불법 정보 유출을 방지하고, 내 · 외부 네트워크의 상호 간 영향을 차단하기 위하여 설치한 보안 시스템
- IP(Internet Protocol) : 인터넷과 연결하기 위한 네트워크 언어, IPv4는 32bit 길이의 주소를 가지며, IPv6는 128bit의 주소 길이를 가진다.
- VPN(Virtual Private Network) : 가상사설망으로서 Tunneling(터널링) 기법을 사용하여 인터넷에 접속해 있는 두 네트워크 사이의 연결을 마치 전용선을 이용해 연결한 것과 같은 효과를 내는 가상 네트워크. VPN의 요소기술로 가장 중요한 것은 터널링과 암호화이다.

[표 6] VPN의 요소 기술

구분	내용 설명
터널링	– 인터넷 상에서 가상의 정보흐름 통로 – L2F , PPTP , L2TP , IPSEC
암호화	– 기밀성을 보장하기 위한 메커니즘으로 전송 중인 정보의 유출방지 – DES , AES , SEED
키 관리	– IKE(Internet Key Exchange) 프로토콜을 사용하여 공유한 암호화키를 분배 및 관리
인증	– 사용자 식별 및 접근 허가, 송신지 식별 확인 – ID/암호 기반, 인증서, 생체인식 기반

(3) 위협

- IP Spoofing을 이용한 ICMP 공격, SMURF 공격 등이 있다.

(4) 대응책

- 네트워크 장비의 ICMP 수신기능 제한적으로 사용.
- SMURF 공격의 Direct Broadcasting이 일어나지 않도록 라우터를 사용.

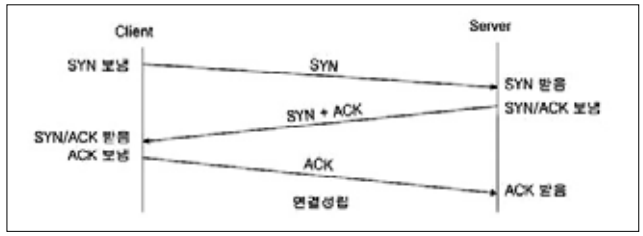
2-1-4. Layer 4 : 전송 계층

(1) 역할

- 호스트들 사이에 데이터(Payload)를 전송하는 역할을 담당한다. 이때 Connection Oriented와 Connectionless 프로토콜을 사용한다.

(2) 주요 기술

- TCP : 연결지향(Connection Oriented) 프로토콜로서 TCP 3 Way Handshake 통신을 하는 대표적인 4계층 프로토콜임.



[그림 5] TCP 3 Way Handshake

- UDP : 인터넷에서 정보를 주고받을 때, 서로 주고받는 형식이 아닌 한쪽에서 일방적으로 보내는 방식의 Connectionless 프로토콜임.

(3) 위협

- TCP의 취약점을 이용한 DoS 공격 발생

  예) TCP Syn Attack, Ping of Death, Land Attack, DDoS 등

(4) 대응책
- Connection Time이 오래된 패킷이 존재하지 않도록 Time Out 적용
- Firewall, IDS, IPS를 통한 이상 패킷 탐지 및 차단.

2-1-5. Layer 5 : 세션 계층
(1) 역할
- 두 Process 사이에 데이터가 흐를 수 있는 가상 경로의 확립이나, 해제를 수행

(2) 주요 기술
- RPC(Remote Procedure Call) : 다른 컴퓨터에 위치한 프로그림에 서비스를 요청하고 처리결과를 전달하는 프로토콜로 네트워크 기반의 분산처리 시스템을 구현하는데 사용됨.
- 그 외에 RTP, RTCP 등이 있음.

(3) 위협
- RPC는 가변포트를 사용하여 방화벽 등에 차단하는데 문제가 발생함.

(4) 대응책
- RPC Proxy를 구축하거나, Stateful Inspection 방식을 이용하여 필터링함.

2-1-6. Layer 6 : 표현 계층
(1) 역할
- 전송 시에 데이터량을 줄이기 위해 데이터를 압축하거나, 암호화하거나, 데이터를 통신에 알맞은 형태로 변경하는 역할을 담당.

(2) 주요 기술
- Codec(Compression/Decompression) : 압축 알고리즘은 프로토콜과 밀접한 관계가 있다. 압축 알고리즘의 주요 목적은 대역폭과 저장 공간을 보존한다.

(3) 위협
- 압축 암호화 기법들의 호환성 문제로 인한 활용성 저해.

(4) 대응책
- 국제적인 표준을 이용하여 호환성 강화

2-1-7. Layer 7 : 응용 프로그램 계층
(1) 역할
- 시스템을 조작하는 사람이나 데이터 통신 서비스를 수행하는 프로그램 등에 여러 서비스를 제공하는 역할

(2) 주요 기술
- SMTP(Simple Mail Transfer Protocol)
- HTTP(Hypertext Transfer Protocol)
- LPD(Line Printer Daemon)
- FTP(File Transfer Protocol)
- WWW(World Wide Web)

(3) 위협
- 서비스 취약점을 이용한 공격

(4) 대응책
- 해당 서비스의 보안 패치의 정기적이고 신속한 업데이트

2-2. 무선랜 및 이동통신 보안

2-2-1. 무선랜 보안

무선랜의 주요 기술로서 IEEE 802.11b, IEEE 802.11a, IEEE 802.11g, IEEE 802.11n이 있다. 하지만, 무선랜은 보안에 취약한 구조로서 보안 표준으로 IEEE 802.11i와 IEEE 802.1x 표준이 있다. 이와 함께 전통적인 암호화 방식으로 WEP가 있으며, 최근에는 WPA가 확대설치 되고 있다. 또한, IEEE 802.11i 표준 방식이 WPA2 등이 있다.

2-2-2. 이동통신 보안

이동통신도 무선랜과 마찬가지로 근본적으로 보안에 취약한 구조를 가지고 있다. 따라서, Spread Spectrum 변조 방식과 SIM Card 암호화 등을 통해 보완하고 있다.

지금까지 통신 및 네트워크 보안에 대해서 알아보았다. 통신 및 네트워크 보안은 전반적으로 많이 출제되므로, 통신 및 네트워크 기술을 각 Layer별로 확실하게 이해하고, 관련 위협과 대응책을 알고 있어야 한다.

[표 7] 통신 및 네트워크 보안 Key Factor

분야	Key Factor	출제비중
통신 및 네트워크 보안	- OSI 모델과 레이어 기술 학습 - LAN, MAN, WAN 기술 이해 - 인터넷, 인트라넷, 엑스트라넷 이해 - 가상 사설 네트워크, Firewall, Router, Bridge, Repeater - 네트워크 토폴로지와 케이블링 숙지 - 공격 방식 및 대응 방법 이해	높음

이번 호에서는 접근 통제, 통신 및 네트워크 보안을 살펴보았다. 이 두 가지 도메인은 IT 기술을 설명하고, 각종 위협과 대응책을 안내하는 기술적 분야의 도메인이다. 전통적으로 가장 많은 문제가 출제되는 도메인들이므로 충분한 학습이 필요한 도메인들이다. 다음 호에는 기술적 보안의 기반 지식인 암호학과 사용자와 가장 밀접한 분야인 응용 프로그램 보안에 대해서 알아보고자 한다.

3. 연습 문제

간단한 문제를 통해서 이번 호에서 배운 도메인에 대한 이해능력을 키우자. 중요한 것은 실제 시험에서는 이보다 어려운 문제가 출제되나, 기본을 알면 충분히 풀 수 있는 문제이니, 문제를 풀고 잘못 이해하는 부분은 요점정리를 통해 재학습이 필요하다.

▣ 접근 통제

1. 보안인증 유형 중에서 가장 보안성이 높은 것은 무엇인가?
   ① 패스프레이즈 ② OTP ③ 생체인증 ④ 2-Factor 인증

2. 생체인식시스템을 도입 시 가장 중요하게 생각해야 하는 것은?
   ① FAR(False Acceptance Rate) ② FRR(False Rejection Rate)
   ③ CER(Crossover Error Rate) ④ SLE(Single Loss Expectancy)

3. IP주소 10.1.10.2의 MAC은 xx:2f인데 10.1.10.6의 MAC도 임의로xx:2f로 ARP 테이블에 Static하게 입력하여 공격을 하는 공격기법을 무엇이라고 하는가?
   ① IP Spoofing ② ARP Spoofing ③ War Dialing ④ DoS

4. 원격시스템의 접근 시에 사용되는 프로토콜로 지속적인 시도응답을 하는 프로토콜을 무엇이라고 하는가?
   ① CHAP ② RBAC ③ PPP ④ SLIP

5. John이 휴일에 출근하여 사내 그룹웨어에 접근하려 하였으나 계정이 잠겨있었다. 해당 시스템의 로그를 확인하니 John의 계정으로 접근하여 외부 침해 흔적이 다수 발견되었다. 이 상황에서 시스템에 침입에 대한 적절한 조치를 위해 추가로 설치해야 할 시스템은 무엇인가?
   ① IPS ② Firewall ③ VPN ④ Anti Virus Program

▣ 통신 및 네트워크 보안

1. 사내 불법모뎀을 찾을 때 사용하는 방법은 무엇인가?
   ① War Driving ② War Dialing ③ Tempast ④ SCAN

2. IPSec에서 인증과 기밀성을 보장하는 방법은?
   ① AH ② ESP ③ MAC ④ IPv6

3. 전선다발이 엉켜 있을 때 발생 할 수 있는 문제점은 무엇인가?
   ① 변조 ② 도청 ③ 잡음 ④ 혼선

4. 다음 중 서비스 거부공격(DoS)이 아닌 것은?
   ① Land Attack and Teardrop Attack ② Trinoo
   ③ TFN and TFN2K ④ Race Condition and SQL Injection

5. 아래 기술들 중 암호화 통신과 관계가 없는 기술은 무엇인가?
   ① IPSec ② SSH ③ MD5 ④ PPTP

정답 : ④, ③, ②, ①, ①, ②, ②, ④, ④, ③