NAC
- 네트워크에 접근하는 접속 단말의 보안성을 검증, 보안성을 강제화하고, 접속을 통제할 수 있는 보안 인프라
- PC 및 네트워크 장치 통제
- 접근 제어
- 해킹, 웜, 유해 트래픽 탐지 및 차단
- 접근 인증

X.509 인증서
1. 구성하는 필드
- Version : 현재 사용 중인 X.509의 버전 정보
- Serial Number : 인증기관이 부여한 고유번호
- Issuer name : 인증서를 발급한 인증기관 식별 정보
- Subject name : 공개키의 소유자 정보, 인증서에 대한 사용자의 이름
- Signature : 인증서에 대한 서명값
- Signature algorithm ID : 인증서 형식의 버전 정보
2. 인증기관의 개인 키 : 인증 기관이 사용자의 공개키에 대한 인증을 수행하기 위해 서명을 사용하는 키
3. 확장 영역
- 키 용도(Key Usage), 기관 키 식별자(Authority Key Identifier), 인증서 정책(Certificate Policies)

각종 시스템 보안 위협
1. 스택 버퍼 오버플로우
- SetUID가 설정된 루트 권한의 프로그램 공격 대상, 스택에 정해진 버퍼보다 큰 공격코드를 삽입하여 반환주소를 변경함으로써 임의의 공격코드를 루트 권한으로 실행하도록 하는 방법
2. 힙 오버 플로우
- 가변적인 양의 데이터를 저장하기 위해 프로그램의 프로세스가 사용할 수 있도록 예약되어 있는 메인 메모리의 영역, 연결리스트나 트리, 그래프 등의 동적인 데이터 구조를 만드는데 꼭 필요하다.
3. 포맷 스트링
- printf, fprintf, sprintf 와 같은 포맷 스트링을 사용하는 함수를 사용하는 경우, 외로부터 입력된 값을 검증하지 않고 입, 출력 함수의 포맷 문자열로 그대로 사용하는 경우 발생할 수 있는 취약점, 취약한 프로세스를 공격하거나 메모리 내용을 읽거나 쓸 수 있다.
4. 정수 오버플로우
- 정수 범위보다 높은 값 저장할 때 생기는 오버플로우
5. 레이스 컨디션 공격
- 둘 이상의 프로세스나 스레드가 공유자원에 동시에 접근할 때 접근하는 순서에 ᄯᅡ라 비 정상적인 결과 발생한다. (그냥 둘이 같이 겹쳐버려서 생기는 오류)
6. 대응방법
- ASLR(Address Space Layout Randomization) : 함수의 복귀 주소 위조 시, 공격자가 원하는 메모리 공간의 주소를 지정하기 어렵게 한다.

대칭키 암호

1) 대칭키 암호의 특징

- 비대칭키 암호에 비해 속도가 빠르다
- 부인 방지 기능 제공

2) 대칭키 암호의 운영모드

블록 암호의 사용 방식

1. ECB(Electronic CodeBook)
- 초기벡터(Initialization Vector)를 사용하지 않는다
- 평문 블록을 암호화한 것이 그대로 암호문 블록으로

2. CBC(Cipher Block Chaining)
- 평문 블록이 암호화되기 전에 이전 암호문 블록과 XOR
- 암호화 된 블록은 전송되지만 다음 블록을 암호화 할 때 쓰기위해 메모리에 저장
- 첫 번째는 초기벡터와 평문 블록이 암호화
- 암호문 Ci에서 에러가 발생한다면 Pi랑 Pi+1은 에러, Ci+2부터는 정상적 복호
- 생성되는 각각의 암호문 블록은 현재 평문 블록뿐만 아니라 그 이전의 평문 블록들의 영향도 받게 된다.
- 평문이 달라지면 초기 벡터는 매번 새롭게 랜덤으로 생성

3. CFB(Cipher FeedBack)
- 블록 암호화를 병렬로 처리할 수 없다.

4. CTR(Counter)
- 평문 블록마다 서로 다른 카운터 값을 사용하여 암호문 블록을 생성한다.
- 초기 벡터가 필요

5. OFB(Output FeedBack)
- 암호 알고리즘의 출력을 암호 알고리즘의 입력으로 피드백
- 키 스트림을 미리 준비할 수 있고 미리 준비한다면 암호문을 만들 때 암호 알고리즘을 더 이상 구동할 필요 없다 (키 스트림을 미리 만들어 두면 암호화를 고속으로 수행할 수 있으며, 혹은 키 스트림을 만드는 작업과 XOR를 취하는 작업을 병행하는 것도 가능하다.)
- 평문 블록은 암호 알고리즘에 의해 직접 암호화되고 있는 것이 아니며 평문 블록과 암호 알고리즘의 출력을 XOR해서 암호문 블록을 만들어 낸다.

3) 대칭키 암호의 알고리즘

=> IDEA(International Data Encryption Algorithm)

=> RC4 스트림 암호 알고리즘
- 작은 단위의 데이터를 암호화 하기 위한 스트림 암호

AES(Advanced Encryption Standard)
- DES(Data Encryption Standard)를 대신하여 새로운 표준이 된 대칭 암호 알고리즘
- SPN 기반 대칭키 암호이다
- 128 라운드 키를 사용한다
- ARIA, SEED는 우리나라 대칭키 암호이다.

Slack
- 공간은 물리적으로 파일에 할당된 공간이지만 논리적으로 사용할 수 없는 낭비 공간이기 때문에, 공격자가 의도적으로 정보를 은닉할 가능성이 있다. 또한, 이전에 저장되었던 데이터가 남아 있을 가능성이 있어 파일 복구와 삭제된 파일의 파편 조사에 활용할 수 있다.
- 카빙(Carving)과정을 통해 디스크 내 비구조화된 데이터 스트림을 식별하고 의미있는 내용을 추출할 수 있다.

암호화 기법들
- Feistel 암호는 전치(Permutation)와 대치(Substitution)를 반복시켜 암호문에 평문의 통계적인 성질이나 암호키와의 관계가 나타나지 않도록 한다.
- Kerckhoff의 원리는 암호 해독자가 현재 사용되고 있는 암호 방식을 알고 있다고 전제한다.
- 2중 DES(Double DES) 암호 방식은 외형상으로는 DES에 비해 2배의 키 길이를 갖지만, 중간일치공격 시 키의 길이가 1비트 더 늘어난 효과밖에 얻지 못한다.

SSL/TLS 프로토콜
1. SSL 프로토콜
- Handshake 프로토콜에서 클라이언트와 서버 간에 논리적 연결 수립을 위해 클라이언트가 최초로 전송하는 ClientHello 메시지에 포함되는 정보
  1. 세션ID
  2. 클라이언트 난수
  3. 압축 방법 목록(압축 알고리즘 리스트)
- 웹 서비스 이외에 다른 응용 프로그램에도 적용 가능
- 단편화, 압축, MAC추가, 암호화, SSL레코드 헤더 추가의 과정으로 이루어짐
- 암호화 기능을 사용하면 주고받는 데이터가 인터넷상에서 도청되는 위험 줄임

Handshake
서버와 클라이언트 간 상호인증 기능을 수행하고, 암호화 알고리즘과 이에 따른 키 교환 시 사용된다.

ChangeCipherSpec
Handshake 프로토콜에 의해 협상된 암호 규격과 암호키를 이용하여 추후의 레코드 계층의 메시지를 보호할 것을 지시한다.

Record
상위계층으로부터(Handshake 프로토콜 , ChangeCipherSpec 프로토콜, Alert 프로토콜 또는 응용 층) 수신하는 메시지를 전달하며 메시지는 단편화되거나 선택적으로 압축된다.

2. TLS(Transport Layer Security) 프로토콜
- Record 프로토콜 : 운반자, 공개키 인증서를 사용하지 않는다.
- Change Cipher Spec 프로토콜 (암호명세변경 프로토콜) : 암호학적 비밀을 신속하게 보내는 데 사용
- Alert 프로토콜 (경고 프로토콜)
- Handshake 프로토콜 : TLS 세션을 처음 시작할 때 클라이언트와 서버 간에 안전한 연결을 위하여 상호 인증을 수행하고 암호 메커니즘의 정보를 교환하여 세션키를 생성하는 하부 프로토콜
- TCP 프로토콜 상에서 사용되며, DTLS는 UDP 프로토콜 상에서 사용
- TLS는 SSL을 기초로 개발
- FTPS에서는 FTP 파일 전송 프로토콜에서 안전한 전송을 위해 TLS를 사용
- TLS 프로토콜에서 대칭키 암호인 ARIA를 사용할 수 있다.

3. CoAP
- 경량 프로토콜
- DTLS를 사용하여 보안성 제공

4. MQTT
- 사물인터넷 프로토콜
- TLS 포로토콜 사용

5. HTTPS
- HTTP 프로토콜에 SSL/TLS 적용

6. SSH
- TCP 프로토콜 상에서 사용
- telnet의 안전성 보장에 사용

이메일 보안
1. PGP(Pretty Good Privacy) p524
- 송신 부인 방지는 지원하지만, 수신 부인 방지는 미지원
- 기밀성 제공을 위하여 대칭키 방식과 공개키 방식을 사용
- 인증받을 메시지나 파일에 전자서명을 생성, 확인 작업을 수행
- 공개키에는 RSA 버전과 Diffie-Hellman 버전이 존재
- 사용할 수 있는 대칭 암호 알고리즘에는 IDEA, CAST, 트리플 DES 등이 있다.
- 공개키의 취소 증명서를 발행할 수 있다.
- 데이터의 압축은 ZIP 형식을 사용한다
- RSA, MD5 등의 알고리즘을 이용하여 전자서명을 한다.
  1) Diffie-Hellman (p74)
  # 두 개의 키를 합성하면 새로운 키가 생성된다
  # 암호화와 복호화에 필요한 키를 분배하거나 교환하기 위한 것이다

2. PEM(Privacy Enhanced Mail)

리눅스 시스템 로그
- btmp : 로그인 실패를 했을 경우에 로그인 실패 정보를 기록
- utmp : 현재 로그인 한 사용자 정보를 담고있는 DB 파일, who, w, whodo, users, finger 등의 명령어
- wtmp : 사용자 로그인, 로그아웃 정보 및 시스템의 shutdown, booting 정보를 가진 파일, last 명령어로 정보 확인

보안 위협
1. 블루킵 : 원격 데스크톱 서비스를 인증 없이 조작할 수 있는 취약점
2. 다크웹
3. 딥페이크
4. 이모텟
5. 소디노키비

블록체인 네트워크
- 거래내역들의 최상위 해시값은 머클 루트로서 블록 헤더에 포함된다.
- 채굴은 주어진 난이도에 따라 해시값의 역상을 구하는 과정이다
- 공개키의 해시값이 암호화폐를 주고 받는 주소값으로 사용된다
- 이중 지불을 방지하기 위해 송신자는 자신의 주소 값에 대응하는 전자서명을 생성한다
- 각 트랜잭션에 한 개씩 전자서명이 부여된다
- 암호학적 해시를 이용한 어려운 문제를 해를 계산하여 블록 체인에 새로운 블록을 추가할 수 있고 일정량의 암호화폐로 보상받을 수 있다.
- 블록체인은 작업증명과 같은 기법을 이용하여 합의에 이른다.

VPN의 구성(p491)
1. 2계층 터널링(암호화) 프로토콜
- PPTP(Point to Point Tunneling Protocol)

- L2F(Layer 2 Forwarding Protocol)
  전송 계층 프로토콜로 TCP가 아닌 UDP를 사용한다.
- L2TP(Layer 2 Tunneling Protocal)
  PPTP+L2F로, 호환성이 뛰어남

접근통제 보안 모델(p169)

1. 강제적 접근 통제(MAC, Mandatory Access Control)

- 객체의 소유자가 변경할 수 없는 주체들과 객체들 간의 접근통제 관계를 정의
- 주체와 객체의 등급을 비교하여 접근 권한을 부여하는 접근 통제이며, 모든 객체는 기밀성을 지니고 있다고 보고 객체에 보안 레벨을 부여한다.

2. 임의적 접근 통제

- 주체가 소유권을 가진 객체의 접근 권한을 다른 사용자에게 부여할 수 있으며, 사용자 신원에 따라 객체의 접근을 제한한다.
- 주체 또는 소속 그룹의 아이디(ID)에 근거하여 객체에 대한 접근 제한을 설정한다. 객체별로 세분화된 접근 제어가 가능하고, 유연한 접근 제어 서비스를 제공할 수 있어 다양한 환경에서 폭넓게 사용되고 있다.
- 주체가 속해 있는 그룹의 신원에 근거하여 객체에 대한 접근을 제한하는 방법으로 객체의 소유자가 접근 여부를 결정한다.

3. 역할 기반 접근 통제

- 주체와 객체 사이에 역할을 부여하여 임의적, 강제적 접근통제 약점을 보완한 방식이다. 사용자가 적절한 역할에 할당되고 역할에 적합한 접근권한(허가)이 할당된 경우만 사용자가 특정한 모드로 정보에 접근할 수 있는 방법이다.

4. 규칙 기반 접근 통제

전자 서명 보안 매커니즘(p113)

- 근원 인증
- 메시지 무결성
- 부인 방지
- privacy를 보장해주지 않는다, 프라이버시가 필요하다면, 암&복호화 할 수 있는 또다른 수단이 적용되어야 한다.

타원곡선 전자서명 구조(Elliptic curve DSA)

- 타원곡선 상에서 이산대수 문제가 어렵다는 사실에 안전성의 근거를 둔다
- 서명할 메시지를 해싱 한 후, 그 해시값을 ECDSA 서명 알고리즘에 입력
- 동일한 비도에서 RSA 전자서명보다 공개키 길이가 짧고 복호화가 빠르다는 장점
- 블록체인 환경에서 거래의 진위 여부를 검증하기 위해 사용
- 타원곡선에서 정의된 연산
- 타원곡선을 이용하여 디피-헬먼 키 교환을 수행할 수 있다.
- 공개키 암호에 사용

OWASP(Open Web Application Security Project)

- Injection
- Broken Authentication
- Sensitive Data Exposure
- XML External Entities(XXE)
- Broken Access Control
- Security Misconfiguration
- Cross Site Scripting
- Insecure Deserialization
- Using Componets with Known Vulnerabilities

2계층(Datalink Layer) 공격 기법 : ARP Spoofing, PPTP, L2TP
4계층(Transport Layer) 공격 기법 : SYN Flooding

전자서명 활용 사례(p112)
- 서명자 인증 : 인증서 로그인을 통해 사용자의 신원 증명
- 위조 불가 : 다운로드하는 소프트웨어의 위변조 여부를 확인
- 유효성 검증 : 웹브라우저로 통신하는 서버의 사이트가 유효한지 검증
- 재사용 불가 : 폐기된 인증서들을 모아 인증서 폐기 목록 발행

IPsec 보안 프로토콜(p497)
- IPsec 설정시 송,수신자가 상대방의 IP주소를 입력해야 한다.
- ESP 프로토콜은 IP패킷을 암호화하고 무결성, 인증을 증명
- IKE 프로토콜은 인증된 Diffie-Hellman 키 교환 방식을 사용한다
- VPN(Virtual Private Network)을 구성하는 한 가지 방법이다.
- 보안 페이로드 헤더에서(ESP) 암호화되는 필드는 Payload Data, Padding, Next Header
- ESP 프로토콜
  암호화를 통한 기밀성 제공
  인증 기능 포함
  터널 모드의 ESP는 Authentication Data를 생성하기 위해 인증 알고리즘을 사용한다.
- 전송모드에서는 전송에서 온 데이터만 보호하고 IP헤더는 보호하지 않는다
- 인증 헤더(Authentication Header) 프로토콜은 발신지 호스트를 인증하고 IP패킷으로 전달되는 페이로드의 무결성을 보장하기 위해 설계
- 일반적으로 호스트는 보안 연관 매개변수들을 보안 연관 데이터베이스에 저장하여 사용

웹 공격 유형(p561)
- SQL Injection
  1) 사용자의 요청이 웹 서버의 애플리케이션을 거쳐 데이터베이스에 전달되고 그 결과가 반환되는 구조에서 주로 발생
  2) 공격이 성공하면 데이터베이스에 무단 접근하여 자료를 유출하거나 변조시키는 결과가 초래될 수 있다.
  3) 사용자의 입력값으로 웹 사이트의 SQL 질의가 완성되는 약점을 이용

- XSS(Cross Site Scripting), CSS
  1) 게시판의 글에 원본과 함께 악성코드를 삽입하여 글을 읽을 경우 악성코드가 실행되도록 하여 클라이언트 정보를 유출하는 공격 기법, 웹 페이지가 사용자로부터 입력 받은 데이터를 필터링 하지 않고, 그대로 동적으로 생성된 웹 페이지에 포함하여 사용자에게 재전송할 때 발생
  2) 저장 XSS 공격, 반사 XSS 공격, DOM 기반 XSS공격으로 분류되며, 이에 대응하기 위해서는 웹 어플리케이션의 개발 단계에서 XSS에 대비한 입출력값을 검증하고 적절하게 인코딩하는 방법을 선택하자
- 파일 업로드 취약점
- CSRF(Cross Site Request Forgery)
  취약한 웹 사이트에 로그인한 사용자가 자신의 의지와는 무관하게 공격자가 의도한 행위를 일으키도록 위조된 http 요청을 웹 응용 프로그램에 전송하는 공격
- 쿠키/세션 위조

★ 전자서명에서는 공개키 시스템이 필요, 서명자는 자신의 개인키로 서명, 검증자는 서명자의 공개키로 서명 검증
★ 암호화 시스템에서는 수신자의 개인키와 공개키 사용, 전자서명에서는 송신자의 개인키와 공개키가 사용

공개키 암호화
- RSA
  -> 소인수분해의 어려움에 기초를 둔 알고리즘
  -> 전자문서에 대한 인증 및 부인 방지에 활용한다.
- ECC와 Rabin은 공개키 암호 방식
- 공개키 알고리즘은 암호화는 수신자의 공개키, 복호화는 수신자의 개인키
- 전자서명 할 때는 서명 작성은 송신자의 개인키, 서명 검증은 송신자의 공개키
- ElGamal은 이산대수의 문제의 어려움에 기초를 둔 알고리즘

스테가노그래피
- 민감한 정보의 존재 자체를 숨긴다
- 텍스트, 이미지 파일 등과 같은 디지털화된 데이터에 비밀이진 정보가 은닉될 수 있다
- 고해상도 이미지 내 각 픽셀의 최하위 비트들을 변형하여 원본의 큰 손상 없이 정보를 은닉하는 방법

TPM(Trusted Platform Module)
- 신뢰 컴퓨팅 그룹에서 표준화된 개념
- 신뢰할 수 있는 플랫폼 모듈, 암호화 키를 포함하여 외부의 공격이나 내부의 다른 요인에 의해 하드웨어의 변경이나 손상을 방지하는 등의 보안관련 기능을 제공하는 기술
- 개인키를 사용하여 플랫폼 설정정보에 서명하여 디지털 인증을 생성
- 키 생성, 난수 발생, 암복호화 기능을 포함한 훼손방지가 필수적인 하드웨어 칩 형태로 구현할 수 있다 소프트웨어로 구현하기도 한다.
- 기본 서비스에는 인증된 부트, 인증, 암호화가 있다.

공개키 기반 구조
- 공개키 인증서는 특정 사용자의 신원과 그 사용자의 공개키를 바인딩 시키는 기술
- CA간에는 인증 체인을 형성할 수 있기 때문에 특정 CA에 의해 서명된 인증서는 인증 체인상의 다른 CA에 의해서도 보장될 수 있다
- 공개키 인증서 서명에는 RSA나 ECDSA를 사용할 수 있다
- PKI에서 RA는 인증서 발급을 요청한 사용자의 신원을 검증한다.

일방향 해시함수
- 임의 길이의 메시지에 대해 특정 길이를 갖는 출력값을 얻을 수 있다
- 일방향 함수이다
- 동일한 출력값을 갖는 임의의 두 입력 메시지를 찾기 어렵다는 것을 강한 충돌 저항성이라 한다
- 블록체인에서 체인 형태로 사용되어 데이터의 신뢰성을 보장한다.

1) salt
- 비밀번호 사전 공격에 취약한 문제 해결 가능

정보보호 인증제도

ITSEC

- 평가등급은 최하위 레벨의 신뢰도를 요구하는 E0(부적합판정)부터 최상위 레벨의 신뢰도를 요구하는 E6까지 7등급으로 구분한다.

TCSEC(Trusted Computer System Evaluation Criteria)

- 같은 등급에서는 뒤에 붙는 숫자가 클수록 보안 수준이 높다
- TCSEC의 레인보우 시리즈에는 레드북으로 불리는 TNI가 있다.
  (Trusted Network Interpretation of the TCSEC, 네트워크용 정보 보호 시스템 평가 기준)

네트워크나 컴퓨터 시스템의 자원 고갈을 통해 시스템 성능을 저하

1. Smurf 공격
   광범위한 효과로 DoS 공격 중 피해가 가장 크다.
   공격자가 출발지 IP 주소를 목표 시스템으로 스푸핑하고, 목적지 주소를 직접 브로드캐스트 주소로 설정한 Ping 메시지를 수신한 네트워크 내의 모든 시스템이 Ping 응답 메시지를 출발지 주소인 공격 목표 시스템으로 동시에 전송
   # 쉽게 말해 공격자가 공격 대상의 IP주소로 위장하여 중계 네트워크에 다량의 ICMP Echo Request 패킷을 전송하며, 중계 네트워크에 있는 모든 호스트는 많은 양의 ICMP Echo Reply 패킷을 공격대상으로 전송하여 목표 시스템을 다운 시킨다.

2. Ping of Death
   ping을 이용하여 ICMP 패킷을 정상크기보다 아주 크게 만든다.
   # 네트워크의 연결 상태를 점검하기 위한 ping 명령을 보낼 때, 패킷을 최대한 길게하여 (최대 65,500바이트) 공격 대상에게 보내면 패킷은 네트워크에서 수백 개의 패킷으로 잘게 쪼개져 보내진다. 네트워크의 특성에 따라 한 번 나뉜 패킷이 다시 합쳐져서 전송되는 일은 거의 없으며, 공격 대상 시스템은 결과적으로 대량의 작은 패킷을 수신하게 되어 네트워크가 마비된다.
3. Land Attack
   SYN 패킷을 조작하여 출발지 IP주소와 목적지 IP주소를 일치시켜서 공격대상에 보낸다. 이때 조작된 IP 주소는 공격 대상의 주소이다.
   (송신자 IP 주소와 수신자 IP 주소, 송신자 포트와 수신자 포트가 동일하게 조작된 SYN 패킷을 공격대상에 전송하는 공격)
4. SYN Flooding Attack
   공격자가 송신자 IP 주소를 존재하지 않거나 다른 시스템의 IP 주소로 위장하여 목적 시스템으로 SYN 패킷을 연속해서 보내는 공격

위험분석 및 평가 방법

1. 델파이법 : 전문가 집단의 토론을 통해 정보시스템의 취약성과 위협 요소를 추정하여 평가하기 때문에 시간과 비용을 절약하지만 정확도가 낮다.
2. 과거자료 분석법 :
3. 시나리오법 어떤 사건도 기대하는 대로 발생하지 않는다는 사실에 근거하여 일정 조건에서 위협에 대해 발생 가능한 결과들을 예측하며, 적은 정보를 가지고 전반적인 가능성을 추론할 수 있다.

통합 인증 체계

1. 커버로스(Kerberos)

- 신뢰받는 제3자인 키 배포 기관이 구성원들 중간에 개입하는 방법
- 커버로스는 세션 키를 이용한 티켓 기반 인증 기법을 제공
- 토큰을 이용한 인증 프로토콜
- 일회성 패스워드를 제공하지는 않는다
- 양방향 인증방식의 문제점을 보완하여 신뢰하는 제3자 인증 서비스를 제공
- 버전 5에서는 이전 버전과 달리 DES가 아닌 다른 암호 알고리즘을 사용할 수 있다.
- 인증 서버가 사용자에게 발급한 티켓은 유효기간 내에 재사용할 수 있다.
- 클라이언트는 사용자의 식별정보를 평문으로 인증 서버 (Authentication Server)에 전송
- 한다.
- 대칭키 암호 방식을 사용하여 분산 환경에서 개체 인증 서비스를 제공한다

침임 탐지 시스템(IDS)

- 내, 외부망의 접속점에 위치하여 방화벽의 부족한 부분을 보강하기 위해 사용
- 데이터 수집원에 의한 분류에 따라 호스트 기반 IDS와 네트워크 기반 IDS로 구분
- 오용 탐지 방법은 알려진 공격 행위의 실행 절차 및 특징 정보를 이용하여 침입 여부를 판단.
- 비정상 행위 탐지 방법은 일정 기간 동안 사용자, 그룹, 프로토콜, 시스템 등을 관찰하여 생성한 프로파일이나 통계적 임계치를 이용하여 침입 여부를 판단한다.
- 하이브리드 기반 IDS는 호스트 기반 IDS와 네트워크 기반 IDS가 결합한 형태
- 기술적 구성요소는 정보 수집, 정보 가공 및 축약, 침입 분석 및 탐지, 보고 및 조치 단계
- IDS는 공격 대응 및 복구, 통계적인 상황 분석 보고 기능을 제공
- 호스트 기반 IDS와 네트워크 기반 IDS로 구분한다.
- 오용 탐지 방법은 알려진 공격 행위의 실행 절차 및 특징 정보를 이용하여 침입 여부를 판단한다.
- 비정상 행위 탐지 방법은 일정 기간 동안 사용자, 그룹, 프로토콜, 시스템 등을 관찰하여 생성한 프로파일이나 통계적 임계치를 이용하여 침입 여부를 판단한다.

IEEE 802.11i

- WEP
- TKIP
- CCMP
  데이터 기밀성 보장을 위해 AES를 CTR 블록 암호 운용 모드로 이용한다.
- EAP

Common Criteria(공통 평가 기준)
IT 제품이나 특정 사이트의 정보시스템의 보안성을 평가하는 기준
- 인증 평가 단계
  PP(Protection Profile)-ST(Security Target)-TOE(Target Of Evaluation)
- TOE는 평가 대상을 의미(Target of Evaluation)
- 정보 시스템은 EAL로 보안 수준을 평가받는다
- CC의 EAL2 등급은 구조적 시험을 의미한다.
- PP는 Protection Profile로 보안 요구 사항을 정의
  # 구현에 독립적이다.
  # 여러 시스템 제품을 한 개의 유형으로 보호 프로파일로 수용할 수 있다.
  # 오퍼레이션이 완료되지 않을 수 있다,
- ST(Security Target)
  # 한 개의 시스템 및 제품을 한 개의 보호목표명세서로 수용해야한다.
  # 구현에 종속적
  # 모든 오퍼레이션이 완료되어야 한다.

- CCRA는 (Common Criteria Recognition Arrangement) 국제상호인정협정을 가지며, CCRA 수준으로 평가를 수행한다.

유닉스/리눅스의 파일 접근 제어
1. 접근 권한 유형으로 읽기, 쓰기, 실행 권한으로 나뉨
2. 파일에 대한 접근 권한은 소유자, 그룹, 다른 모든 사용자에 대해 각각 지정 가능
3. 파일 접근 권한 변경은 관리자인 root 사용자
4. SetUID가 설정된 파일은 실행 시간 동안 그 파일의 소유자의 권한으로 실행된다.

해시 함수
- 일방향 함수
- 임의 길이의 메시지에 대해 특정 길이를 갖는 출력값을 얻을 수 있다
- 블록체인에서 체인 형태로 사용되어 데이터의 신뢰성을 보장한다
- 동일한 출력값을 갖는 임의의 두 입력 메시지를 찾기 어렵다는 것을 강한 충돌 저항성

하이브리드 암호 시스템
- 메시지는 대칭 암호 방식으로 암호화
- 일반적으로 대칭 암호에 사용하는 세션키는 의사 난수 생성기로 생성
- 생성된 세션키는 기밀성 보장을 위해 공개키 암호 방식으로 암호화
- 메시지 송신자와 수신자가 사전에 공유하고 있는 비밀키가 없어도 사용할 수 있다
- 메시지 자체를 암호화 또는 복호화 할 때는 속도가 빠른 대칭키 암호 시스템을 사용
- 암호화에 사용된 대칭키를 상대방에게 전달할 때 상대방의 공개키를 사용
- 공개키 알고리즘을 사용하여 공개키와 개인키를 생성하고, 공개키를 상대방에게 전달한다.
- 수신자는 암호화된 대칭키를 수신자의 개인키로 복호화 할 수 있다.
해시함수의 충돌저항성을 위협하는 공격
충돌저항성? Eve로 하여금 동일한 다이제스트를 가지는 2개의 메시지를 구하지 못하도록 하는 것
- 생일 공격은 강한 충돌 내성을 깨고자 하는 공격이다
- 해시 함수의 충돌, 동일한 해시 함수가 서로 다른 두 개의 입력 값에 대해 동일한 출력 값을 내는 것을 의미

VRFY
- SMTP 클라이언트가 SMTP 서버의 특정 사용자를 확인함으로써 계정 존재 유무를 알 수 있다.

SYN 쿠키 기법
1. 서버가 여러 입력값으로 해시값을 쿠키로 구한 다음, 이를 서버 시작 순서번호로 하는 SYN+ACK패킷을 클라이언트로 회신
2. 정상적인 ACK 패킷을 수신할 때까지 연결 테이블에 자료구조 설정을 미룬다.
3. 클라이언트가 SYN 쿠키가 포함된 ACK 패킷을 보내오면 서버는 세션을 다시 열고 통신을 시작한다..

ISO 27001
Plan(조직의 상화 , 리더십, 기획) – Do(지원, 운영) – Check(성과평가) – Act(개선)

블록체인(p287)
- 합의 기법
  1. Pow(Proof of Work)
  새로 만든 블록을 앞 블록에 연결하는데 필요한 해시를 만들고 해시 연결성을 검증하여 데이터가 중간에 위변조가 되지 않았음을 확인
  2. PoS(Proof of Staking)
  작업 증명의 에너지 낭비 문제를 해결하기 위해 만들어짐, 컴퓨팅 파워가 아닌 자신이 가진 가상통화의 양, 즉 지분에 따라 블록을 생성하고 추가적으로 발생되는 코인을 받기
  # 비트코인에서 사용하는 방식이 채굴 경쟁으로 과도한 자원 소비를 발생시킨다는 문제를 해결하기 위한 대안으로 등장하였다.
  # 채굴 성공 기회를 참여자에 따라 차등적으로 부여한다.
  # 다수결로 의사 결정을 해서 블록을 추가하는 방식이 아니므로 불특정 다수가 참여하는 환경에서 유효하다.
- 관련 보안 기술
  1) 해시 함수를 사용하여 데이터에 대한 무결성을 보장한다
  2) 데이터의 신뢰성 및 투명성을 제공
  3) 한 예로 하이퍼레저 패브릭에서는 공개키 인증서를 이용하여 피어에 대한 신원 정보를 제공
  4) 블록체인 기술에서는 작업 증명이나 지분 증명 등과 같은 합의 알고리즘을 사용한다.
- 금융 분야에만 국한되지 않고 분상원장으로 각 분야에 응용할 수 있다
- 블록체인의 한 블록에는 앞의 블록에 대한 정보가 포함되어야 한다
- 하나의 블록은 트랜잭션의 집합과 헤더로 이루어져 있다.

CERT
- 정보통신망 등의 침해사고에 대응하기 위해 기업이나 기관의 업무 관할 지역 내에서 침해사고의 접수 및 처리 지원을 비롯해 예방, 피해 복구 등의 임무를 수행

ISMS

1. 정보통신망의 안전성 확보를 위해 수립하는 기술적, 물리적, 관리적 보호 조치 등 종합적인 정보보호 관리 체계 인증 제도

ISMS – P

- 국내의 기관이나 기업이 정보 및 개인정보를 체계적으로 보호할 수 있도록 통합된 관리체계 인증제도
- 정보통신망의 안전성 확보를 위해 수립하는 기술적, 물리적, 관리적 보호조치 등 정보보호관리 체계 인증 제도
- 정보보호 관리 체계의 인증만 선택적으로 받을 수도 있다
- 개인정보 제공 시 뿐만 아니라 파기 시의 보호조치도 포함
- 관리체계 수립 및 운영 영역은 Plan, Do, Check, Act의 사이클에 따라 지속적으로 반복적으로 실행되는지 평가

디지털 포렌식

- 슬랙
  물리적으로 파일에 할당된 공간이지만 논리적으로 사용할 수 없는 낭비 공간이기 때문에, 공격자가 의도적으로 정보를 은닉할 가능성이 있다. 또한, 이전에 저장되었던 데이터가 남아 있을 가능성이 있어 파일 복구와 삭제된 파일의 파편 조사에 활용할 수 있다.
- 카빙
  디스크 내 비구조화된 데이터 스트림을 식별하고 의미 있는 내용을 추출할 수 있다.

무결성을 위협하는 공격

- 메시지 변조 공격
- 위장 공격
- 재전송 공격

Bell-LaPadula 모델

- 군사용 보안 구조의 요구사항을 충족시키기 위해 개발된 최초의 수학적 모델
- 불법 파괴나

GDPR(일반개인정보보호법)

- 중요한 사항 위반 시 직전 회계연도의 전 세계 매출액 4% 또는 2천만 유로 중 높은 금액이 최대한도 부과 금액이다.

KCMVP

- 암호 알고리즘이 구현된 프로그램 모듈의 안정성과 구현 적합성을 검증하는 제도

전자화폐

- 전자적 매체에 화폐의 가치를 저장한 후 물품 및 서비스 구매시 활용하는 결제 수단
- 발행, 사용, 교환 등의 절차에 관하여 법률에서 규정하고 있으나, 가상화폐는 별도 규정 없다
- 가상화폐인 비트코인은 분산원장기술로 알려진 블록체인 활용

메시지 인증 코드(Message Authentication Code, MAC)
- 상호 인증
- 무결성 보장

One Time Password(OTP)
- 비밀번호 예측 공격을 박기 위한 방법으로 사용
- 패킷 스니핑을 통한 비밀번호 재사용 공격의 대응책으로 사용
- 동기화 방식 OTP는 시간과 인증 횟수를 기반으로 비밀번호를 동기화
- 비동기화 방식 OTP는 인증서버에 전송된 나누를 기반으로 비밀번호를 생성

ARP Spoofing
공격자가 특정 호스트의 MAC주소를 자신의 MAC 주소로 위조한 ARP Replay 패킷을 만들어 희생자에게 지속적으로 전송하면 희생자의 ARP Cache에 특정 호스트의 MAC 정보가 공격자의 MAC 정보로 변경이 된다. 이를 통해 희생자에게서 특정 호스트로 나가는 패킷을 공격자가 스니핑하는 기법

벨라파듈라 모델(BLP, Bell-LaPadula, p175)
- 비밀정보가 허가되지 않은 방식으로 접근되는 것을 방지
- 강제적 접근통제를 하고자 하는 경우 본 모델을 기반으로 통제규칙을 정의한다
- 단순 보안 규칙은 주체가 객체를 읽기 위해서는 주체의 비밀취급 허가 수준이 객체의 보안 분류 수준보다 높거나 같아야 함
- 특수 속성 규칙(강한 스타 보안 규칙)은 강한 스타 보안 규칙은 주체의 읽기/쓰기는 하위 혹은 상위가 아닌 동일한 보안 분류 수준의 객체에 대해서만 가능함

파밍 공격 (Pharming)
- 해당 사이트가 공식적으로 운영하고 있는 도메인 자체를 중간에서 탈취하는 수법
- 사용자의 컴퓨터는 공격자에게 점유되어 정상적인 URL을 입력해도 이에 해당하는 IP 주소가 공격자의 웹 서버로 연결되도록 되어 있었다.

S/MIME
- IETF의 작업 그룹에서 RSADSI(RSA Data Security Incorporation)의 기술 기반으로 개발한 전자우편 보안 기술이며, RFC 3850, 3851 등에서 정의되어 있다. 전자우편에 대한 암호화 및 전자서명을 통하여 메시지 기밀성, 메시지 무결성, 사용자 인증, 송신 사실 부인 방지, 프라이버시 보호 등의 보안 기능을 제공한다.

무선 네트워크 보안 기술
- WPA2 기술은 AES/CCMP를 사용한다
- WPA는 EAP 인증 프로토콜과 WPA-PSK를 사용한다.
- WPA-PSK는 WEP보다 훨씬 더 강화된 암호화 세션을 제공
- WEP은 64비트 WEP키가 수분 내 노출되어 보안이 매우 취약하다
- 무선 네트워크 환경에서 인증/인가를 위해 RADIUS 프로토콜을 사용하여 연결
- 무선 AP의 SSID 값 노출과 MAC주소 기반 필터링 기법은 공격의 원인이 된다.
- Diameter 프로토콜은 RADIUS보다 세션관리, 보안 측면에서 개선 및 확정된 프로토콜이다.

바이러스
- Polymorphic Virus : 감염될 때 마다 구현된 코드의 형태가 변형

DRM 구성요소
- 시큐어 컨테이너 : DRM 보호 범위에서 유통되는 컨텐츠의 배포 단위로서 암호화된 콘텐츠 메타 데이터, 전자서명 등의 정보로 구성, MPEG-21 DID 규격을 따른다.

스트림 암호
- 절대 안전도를 갖는 암호로 OTP가 존재
- LFST(Linear Feedback Shift Register)로 스트림 암호를 구현할 수 있다
- Trivium은 현대적 스트림 암호로 알려져 있다.

이더넷 상에서 전달되는 모든 패킷을 분석하여 사용자의 계정과 암호를 알아낸다
- Sniffing

리눅스 시스템에서 패스워드 정책이 포함되고, 사용자 패스워드가 암호화 되어있는 파일
- /etc/shadow

영지식 증명
- 영지식 증명은 증명자가 자신의 비밀 정보를 노출하지 않고 자신의 신분을 증명
- 최근 블록 체인 상에서 영지식 증명을 사용하여 사용자의 프라이버시를 보호하고자 하며, 이러한 기술로는 zk-SNARK가 있다.
- 완정성, 건실성, 영지식성 특성을 가져야 한다.

Dos
- 헤더가 조작된 일련의 IP 패킷 조각들을 전송
- 대상 포트 번호를 확인하여 17,135,137번, UDP 포트스캔이 아니면, UDP Flooding 공격으로 간주
- 공격자가 임의로 자신의 IP 주소를 속여서 다량으로 서버에 보냄
‘

레지스트리(Registry)
- 레지스트리 변화를 분석함으로써 악성코드 탐지 가능

침입차단시스템
- 이중 네트워크 호스트 구조는 내부 네트워크를 숨기지만, 베스천 호스트가 손상되면 내부 네트워크를 보호할 수 없다.

Meltdown 보안
- CPU를 고속하하기 위해 사용된 비순차적 명령어 처리 기술을 악용한 보안 취약점

Promiscuous
- 네트워크 인터페이스 카드가 가지고 있는 모드 중 하나인데, 네트워크 인터페이스 카드를 거치는 모든 데이터를 확인하는 스니핑 공격을 수행할 수 있다.

ifconfig
- Promiscuous 모드 설정

정보보안 요구사항
- NAT(Network Address Translation)
  # 방화벽 구축 시 내부 네트워크의 구조를 외부에 노출하지 않는 방법
- DLP

SIEM
- 조직 내에 운영되는 다양한 정보 보안 장비 및 IT 시스템들의 이벤트 로그를 수집, 분석하여 이상 징후 및 위험 사항을 파악,

setuid
- 파일을 실행시킬 때 사용자의 권한이 아닌 일시적으로 파일 소유자(특히 관리자)의 권한을 가지기 때문에 공격에 많이 사용되는 것

개인정보 비식별화 조치
- 가명 처리
- 총계 처리
- 데이터 값 삭제
- 범주화 수행

traceroute
- TCP/IP 기반의 네트워크에서 목적지 호스트까지의 경로를 파악하기 위해서 데이터그램의 TTL 값과 ICMP Time Exceeded 메시지를 기반으로 동작

공공기관의 보안성 강화를 위한 망분리 기술
- 물리적 망분리와 논리적 망분리 기법이 존재
- 물리적 망분리가 되었다 하더라도 USB와 같이 저장 매체를 통한 악성 코드 침입이 가능
- 논리적 망분리 기법으로는 SBC 및 CBC 기반의 망분리 기법이 존재
- 데이터 다이오드 기반 데이터 일방향성을 이용해 망 분리 실현이 가능

비정형 접근법(Informal Approach)
- 전문가의 경험과 지식을 활용하여 빠르게 진행되는 위험 분석 접근법

CEK(Contents Encrypting Key)와 KEK(Key Encrypting Key)
- KEK를 이용하여 지켜야 할 키의 개수를 줄일 수 있다
- 통상적으로 CEK에는 세션 키가, KEK에는 마스터키가 사용된다.
- KEK를 이용하여 CEK를 암호화한다.
- KEK의 기밀성을 유지하기 위하여 PBE(Password Based Encryption)를 이용하기도 한다.

쿠키
- 웹사이트를 편리하게 이용하기 위한 목적으로 만들어졌으며, 많은 웹사이트가 쿠키를 이용하여 사용자의 정보를 수집하고 있다.
- 쿠키에 포함되는 내용을 웹 응용프로그램 개발자가 정할 수 있다
- 쿠키 저장시 타인이 임의로 쿠키를 읽어 들일 수 없도록 도메인과 경로 지정에 유의해야 한다.

Spyware
- 사용자의 동의 없이 설치되어 정보를 수집하고 전송하는 악성 소프트웨어로서 금융정보, 신상정보, 암호 등을 비롯한 각종 정보를 수집한다.

Keylogging
- 사용자가 키보드로 PC에 입력하는 내용을 몰래 가로채 기록하는 행위

Bot
- 인간의 행동을 흉내 내는 프로그램으로 DDoS 공격을 수행한다.

정보 보호 서비스
Authentication
- 정보교환에 의해 실체의 식별을 확실하게 하거나 임의 정보에 접근할 수 있는 객체의 자격이나 객체의 내용을 검증하는 데 사용한다.

Confidentiality
- 온오프라인 환경에서 인가되지 않은 상대방에게 저장 및 전송되는 중요정보의 노출을 방지한다.

Integrity
- 네트워크를 통하여 송수신되는 정보의 내용이 불법적으로 생성 또는 변경되거나 삭제되지 않도록 보호한다.

NULL 스캔
- 공격자가 모든 플래그가 세트되지 않은 TCP 패킷을 보내고, 대상 호스트는 해당 포트가 닫혀 있을 경우 RST 패킷을 보내고, 열려 있을 경우 응답을 하지 않는다.

xferlog
- Thu Feb 7 20:33:56 2019 1 198.188.2.2 861486 /tmp/12-67 -ftp1.bmp b _ o r freeexam ftp 0 * c 861486 0

업무연속성(BCP)
- 재해복구시스템의 백업센터 중 미러 사이트(Mirror Site)는 백업센터 중 가장 짧은 시간 안에 시스템을 복구한다.
- 업무연속성은 장애에 대한 예방을 통한 중단 없는 서비스 체계와 재난 발생 후에 경영 유지·복구 방법을 명시해야 한다.
- 재난복구서비스인 웜 사이트(Warm Site)는 구축 및 유지비용이 콜드 사이트(Cold Site)에 비해서 높다.

Sandbox

- 보호된 영역 내에서 프로그램을 동작시키는 것으로, 외부 요인에 의해 악영향이 미치는 것을 방지하는 보안 모델이다. '아이를 모래밭(샌드 박스)의 밖에서 놀리지 않는다'라고 하는 말이 어원이라고 알려져 있다. 이 모델에서는 외부로부터 받은 프로그램을 보호된 영역, 즉 '상자' 안에 가두고 나서 동작시킨다. '상자'는 다른 파일이나 프로세스로부터는 격리되어 내부에서 외부를 조작하는 것은 금지되고 있다. 가상화 기술 기반으로 악성코드의 비정상 행위를 유발하는 실험과정에서 발생할 수 있는 분석시스템으로의 침해를 방지하여 통제된 환경과 분석 기능을 제공한다.
- 가상화 기술 기반으로 악성코드의 비정상 행위를 유발하는 실험과정에서 발생할 수 있는 분석시스템으로의 침해를 방지하여 통제된 환경과 분석 기능을 제공한다.

Process Explorer

- 악성코드의 행위를 추출하기 위해 실제로 해당 코드를 실행함으로써 발생하는 비정상행위 혹은 시스템 동작 환경의 변화를 살펴볼 수 있는 동적 분석 기능을 제공한다.
- 프로세스를 관리할 수 있는 프로그램으로 악성코드의 행위를 추출하기 위해 실제로 해당 코드를 실행함으로써 발생하는 비정상 행위 혹은 시스템 동작 환경의 변화를 살펴볼 수 있는 동적 분석 기능을 제공한다.

윈도우 운영체제

- net user guest/active:no guest 계정 일시적 비활성화
- net user 시스템 내 사용자 계정정보를 나열
- net group 명령은 서버에서 글로벌 그룹을 추가, 표시 또는 수정한다
- 컴퓨터/도메인에 모든 접근 권한을 가진 관리자 그룹인 Administrators이 기본적으로 존재한다

CPO

- 정보통신망 등의 침해사고에 대응하기 위해 기업이나 기관의 업무 관할 지역 내에서 침해 사고의 접수 및 처리 지원을 비롯해 예방, 피해 복구 등의 임무를 수행하는 조직