


들어가기

CONTENTS 학습목표

- 정보 보안이란 무엇인지 설명할 수 있다.
- 악성 프로그램과 해킹에 대해 설명할 수 있다.
- 암호화 기술에 대해 설명할 수 있다.
- 인터넷 보안에 대해 설명할 수 있다.





복습하기

LEARNING 지난 주차 복습

13주차 학습내용. 클라우드 컴퓨팅

- 1 클라우드 컴퓨팅의 개요
- 2 클라우드 컴퓨팅의 특징과 장단점
- 3 클라우드 컴퓨팅 서비스 유형
- 4 클라우드 컴퓨팅 관련 이슈



지난 주차 **복습**

클라우드 컴퓨팅의 개요

- 클라우드 컴퓨팅
 - 데이터와 프로그램들이 개인의 PC에 저장되는 것이 아니라 눈에 보이지 않는 인터넷 기반의 구름들에 저장하는 것
 - 사용자는 컴퓨팅을 위해 PC, 휴대폰 등의 단말기를 통해 클라우드에 원격 접속하여 원하는 Service를 받을 수 있는 새로운 컴퓨팅 환경

지난 주차 **복습**

클라우드 컴퓨팅의 특징과 장단점

- 확장성과 탄력성(Scalability & Elasticity)
- 요구에 따른 서비스 제공(On - Demand)
- 사용한 만큼의 비용 지불(Pay - Per - Use)

LEARNING


복습하기

지난 주차 복습

클라우드 컴퓨팅 서비스 유형

- ◆ SaaS
- ◆ PaaS
- ◆ IaaS

클라우드 컴퓨팅 관련 이슈



1

정보 보안의 개요



1] 정의

학습하기

정보보안

유형, 무형의 정보 생성과 가공, 유통, 배포, 그리고 정보를 사용하는 과정에서 발생하는 여러 부작용에 대처하기 위한 모든 정보 보호 활동을 포괄하는 광의의 개념



인터넷과 모바일 등 정보 기술의 발전으로 인하여 정보를 유통하는 과정에서 정보에 대한 무단 유출 및 파괴, 변조, 전자메일의 오남용, 불건전한 정보의 대량 유통 등과 같은 부작용이 발생함

2] 정보 보안 위협의 예

학습하기

◇ 문제 발생 장소에 따른 구분

컴퓨터 보안

컴퓨터 자체의 정보를 보호하기 위한 도구들의 모임

네트워크 보안

컴퓨터 사이의 정보 전송의 보안을 위한 도구들의 모임

네트워크 상에서의 정상적인 정보 전송



2] 정보 보안 위협의 예

학습하기

전송차단
(Interruption)

가로채기
(Interception)

변조
(Modification)

위조
(Fabrication)

2] 정보 보안 위협의 예

학습하기

전송차단
(Interruption)

가로채기
(Interception)

변조
(Modification)

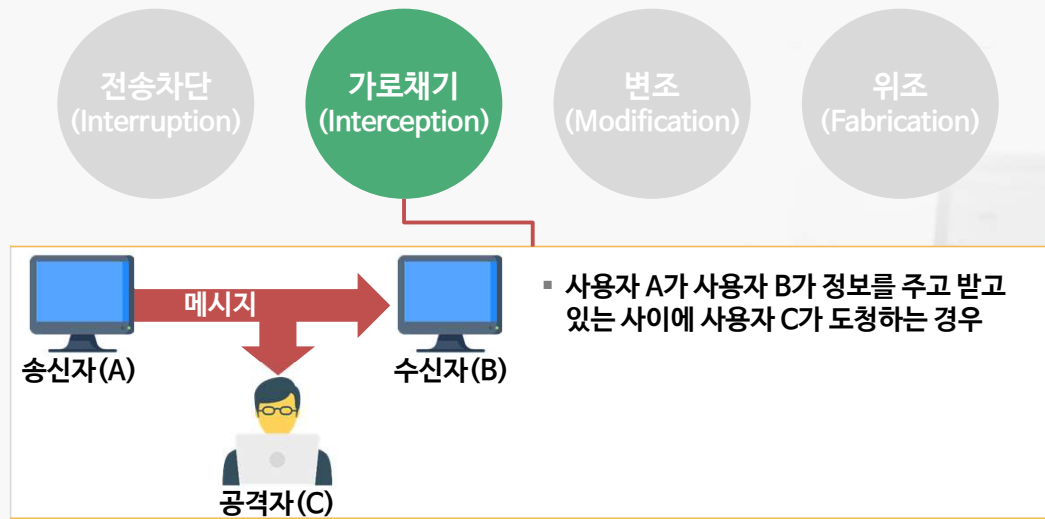
위조
(Fabrication)



- 사용자 A가 사용자 B에게 정보를 전송할 때 사용자 C가 B와 연결할 수 없도록 하는 데이터 전송 차단

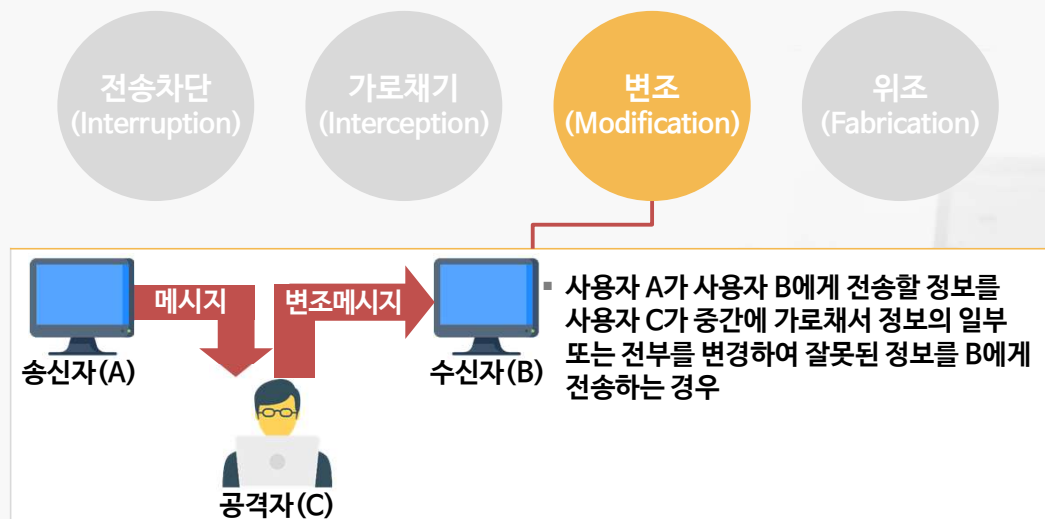
2] 정보 보안 위협의 예

학습하기



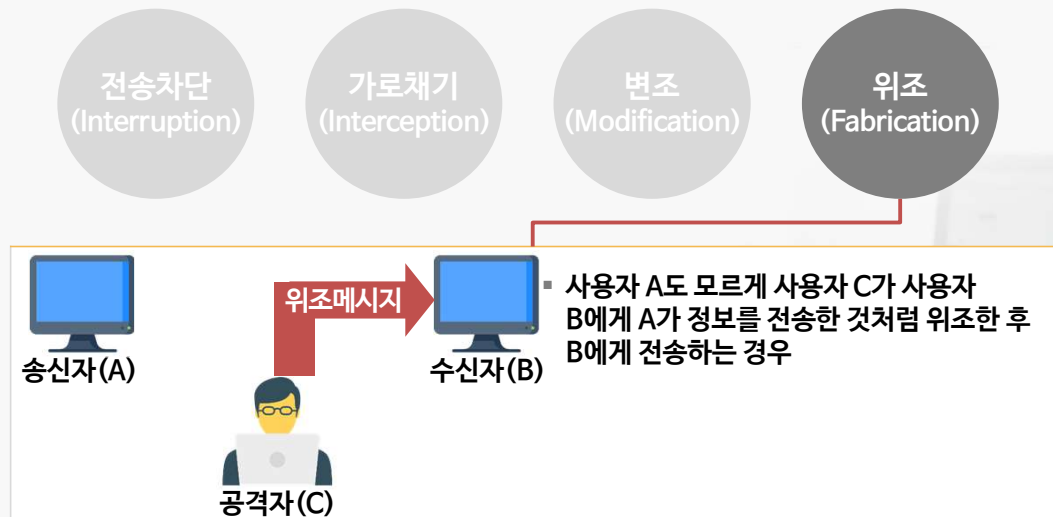
2] 정보 보안 위협의 예

학습하기



2] 정보 보안 위협의 예

학습하기



3] 정보 보안 목표

학습하기

◇ 기본적인 목표

- ✓ 내부 또는 외부의 침입자에 의해 행해지는 각종 정보의 파괴, 변조 및 유출 등과 같은 정보 범죄로부터 중요한 정보를 보호

3] 정보 보안 목표

학습하기

정보 보안 요구사항

비밀성
(Confidentiality)

무결성
(Integrity)

가용성
(Availability)



3] 정보 보안 목표

학습하기

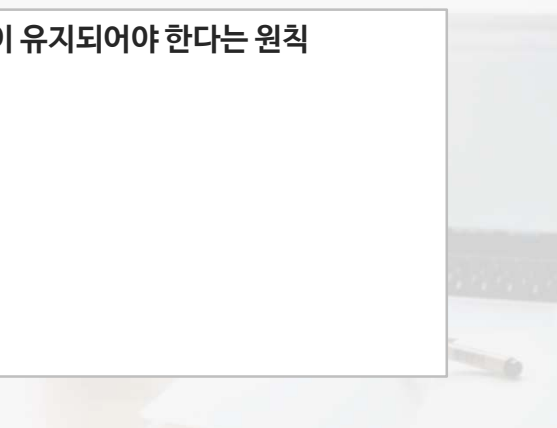
정보 보안 요구사항

비밀성
(Confidentiality)

무결성
(Integrity)

가용성
(Availability)

- 정보의 소유자가 원하는 대로 정보의 비밀이 유지되어야 한다는 원칙
- 비밀성을 보장하기 위한 메커니즘
 - 접근 통제
 - 암호화



3] 정보 보안 목표

학습하기

◇ 정보 보안 요구사항

비밀성
(Confidentiality)

무결성
(Integrity)

가용성
(Availability)

- 비인가된 자에 의한 정보의 변경, 삭제, 생성 등으로부터 보호하여 정보의 정확성, 완전성을 보장되어야 한다는 원칙
- 무결성을 보장하기 위한 정책
 - 정보 변경에 대한 통제
 - 오류나 태만 등으로부터의 예방
- 무결성을 통제하기 위한 메커니즘
 - 물리적인 통제
 - 접근 제어

3] 정보 보안 목표

학습하기

◇ 정보 보안 요구사항

비밀성
(Confidentiality)

무결성
(Integrity)

가용성
(Availability)

- 정보 시스템은 적절한 방법으로 작동되어야 하며, 정당한 방법으로 권한이 주어진 사용자에게 정보 서비스를 거부하여서는 안된다는 것
- 가용성을 확보하기 위한 통제 수단
 - 데이터 또는 시스템의 백업
 - 중복성의 유지
 - 물리적 위협 요소로부터의 보호

4] 정보 보안 서비스

학습하기

◇ 정보 보안을 위한 서비스의 종류



2

악성 프로그램과 해킹

1] 악성 프로그램

학습하기

악성 프로그램

제작자가 의도적으로 사용자에게 피해를 주고자 만든 프로그램으로 컴퓨터 시스템을 파괴하거나 작업을 지연 또는 방해하는 프로그램



악성 프로그램의 분류

- 바이러스, **웜**, 트로이 목마 등

웜 바이러스라는 표현을 쓰기도 함

1] 악성 프로그램

학습하기

◇ 웜



실행코드 자체로 번식하는 유형을 말하며, 주로 PC상에서 실행됨



웜과 바이러스는 감염대상을 가지고 있는가와 자체 번식 능력이 있는가에 따라 분류함

웜

- 감염대상을 가지지 않음
- 자체 번식 능력 있음

바이러스

- 감염대상을 가짐
- 자체 번식 능력이 없음



웜의 번식을 위하여 웜 스스로 다른 사람에게 보내는 전자메일에 자신을 첨부함

1] 악성 프로그램

학습하기

◇ 트로이목마

트로이목마

해킹 기능을 가지고 있어 인터넷을 통해 감염된 컴퓨터의 정보를 외부로 유출하는 악성 프로그램

- ✓ 트로이목마라는 이름은 트로이 전쟁 당시 목마 속에 숨어있던 그리스 병사가 트로이를 멸망시킨 것을 비유하여 악성 프로그램이 사용자가 눈치채지 못하게 몰래 숨어든다는 의미
- ✓ 주로 인터넷에서 다운로드 파일을 통해 전파됨
- ✓ 유용한 프로그램으로 가장하여 사용자가 그 프로그램을 실행하도록 속임

1] 악성 프로그램

학습하기

◇ 트로이목마

트로이 목마의 실제 목적

“ 사용자의 합법적인 권한을 사용해 시스템의 방어체제에 침해하여 접근이 허락되지 않는 정보를 획득하는 것 ”

2] 해킹과 피싱

학습하기

◇ 해킹(hacking)이란

- 1 컴퓨터 통신망을 통하여 사용이 허락되지 않은 **다른 컴퓨터에 불법으로 접속하여**
- 2 저장되어 있는 **정보 또는 파일을 빼내거나**
- 3 마음대로 **바꾸어 놓기도 하고,**
- 4 컴퓨터 운영체제나 정상적인 **프로그램을 손상시키는 행위**

2] 해킹과 피싱

학습하기

◇ 해킹(hacking)이란

해커
(hacker)

다른 사람의 컴퓨터에 불법으로 침입, 정보를 빼내서 이익을 취하거나 파일 삭제, 전산망을 마비시키는 악의적 행위를 하는 사람



원래의 의미 : 컴퓨터 시스템 내부구조와 동작 따위에 심취하여 이를 알고자 노력하는 사람으로서 대부분 뛰어난 컴퓨터 및 통신 실력을 가진 사람들

크래커
(cracker)

다른 사람의 컴퓨터에 침입하여 악의적 행위를 하는 사람

2] 해킹과 피싱

학습하기

◇ 피싱(phishing)

✓ 개인정보(privacy)와 낚시(fishing)의 합성어

은행 또는 전자상거래
업체의 홈페이지와
동일하게 보이는 위장
홈페이지를 만들

인터넷 이용자들에게
유명 회사를 사칭하는
전자메일을 보내, 위장
홈페이지에 접속하게
함

계좌번호,
주민등록번호 등의
개인정보를 입력하도록
유도하여, 이를 이용해
금융사기를 일으킴

“ 신중 사기 수법 ”

2] 해킹과 피싱

학습하기

◇ 스파이웨어

✓ 스파이와 악성 프로그램인 소프트웨어의 합성어

✓ 컴퓨터 이용자 모르게 또는 동의 없이 설치되어 컴퓨터 사용에 불편을
끼치거나 정보를 가로채가는 악성 프로그램

2] 해킹과 피싱

학습하기

◆ 스니핑(sniffing)

- ✓ 전화의 도청 원리와 같이 특수 소프트웨어를 이용해 상대방의 ID, 비밀번호, 메일 등을 가로채는 수법

◆ 스푸핑(spoofing)

- ✓ 자기자신의 식별 정보를 속여 다른 대상 시스템을 해킹하는 기법
- ✓ 시스템 정보를 위장하여 감춤으로써 역추적을 어렵게 만들

2] 해킹과 피싱

학습하기

◆ 그레이웨어

- ✓ 허위 안티스파이웨어 프로그램, 악성 톨바, 불필요한 Active X 등과 같이 사용자의 설치 동의를 악용해 다른 프로그램을 함께 설치하거나 사용자의 불편함을 야기하는 프로그램
- ✓ 합법적인 동의 과정을 거쳐 설치했지만 교묘하게 불법적인 행위를 하는 등 합법과 불법 사이를 오고 가며 사용자들을 괴롭히고 있음

2] 해킹과 피싱

학습하기

◇ 그레이웨어



그레이웨어 피해 방법

- 특정 광고를 강제로 보게 하거나 웹 브라우저를 하이재킹해 사용자를 수익 창출 페이지로 이동시킴
- 사용자들이 쉽게 삭제할 수 없게 만들어 개인정보 유출, 시스템 성능 저하 등의 문제를 불러 일으킴

3] DDos

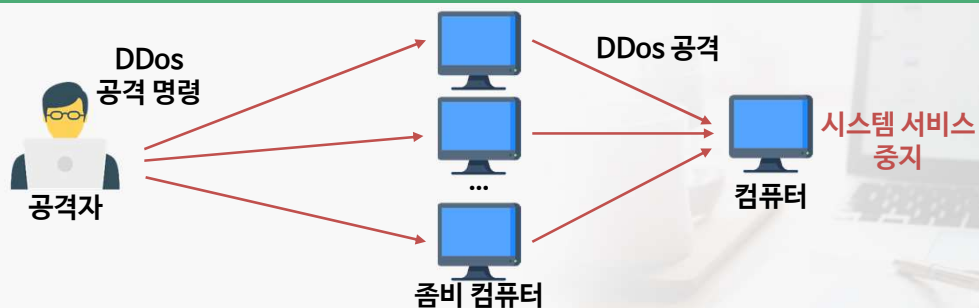
학습하기



Distributed Denial of Service의 약자로 '분산 서비스 거부' 또는 '분산 서비스 거부 공격'이라고 함



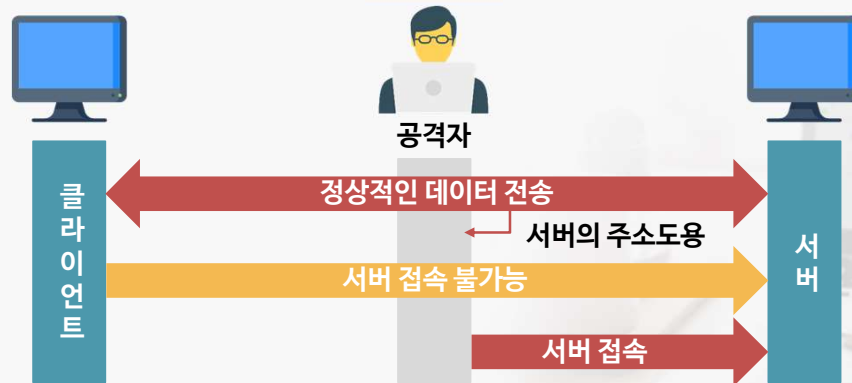
공격자는 여러 대의 좀비 컴퓨터를 분산 배치하여 동시에 공격 대상 컴퓨터나 네트워크를 공격



4] 스푸핑

학습하기

- ✓ 공격자가 MAC 주소, IP 주소, 전자메일 주소 등 자신의 정보를 위장하여 정상적인 사용자나 시스템이 위장된 가짜 사이트를 방문하도록 유도한 뒤 정보를 빼가는 수법



To. 교수님
앞에 구성된
해당 구성에
할지 확인드

5] 스니핑

학습하기

- ✓ 네트워크에서 주고받는 데이터를 도청하여 사용자의 ID, 비밀번호, 전자메일 내용, 쿠키(cookie) 등을 가로채는 수법



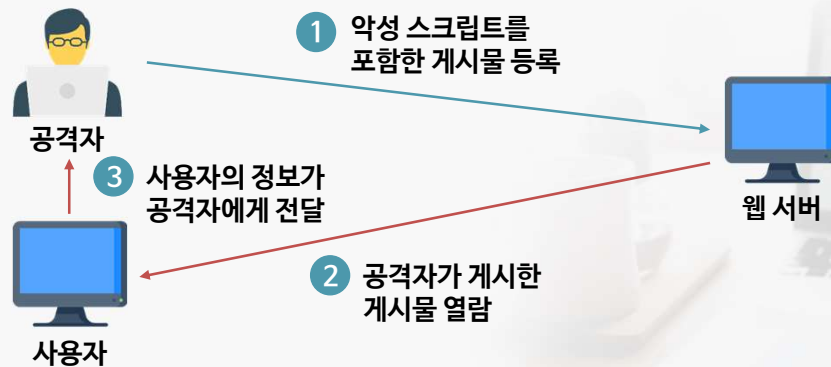
To. 교수님
앞에 구성된 스니핑
해당 구성에 함께
할지 확인드립니다

6] XSS

학습하기



공격자가 게시판에 악성 스크립트가 포함된 글을 등록하면 사용자가 게시물을 열람하고, 그 순간 악성 스크립트가 실행되어 사용자의 정보가 공격자에게 전달됨

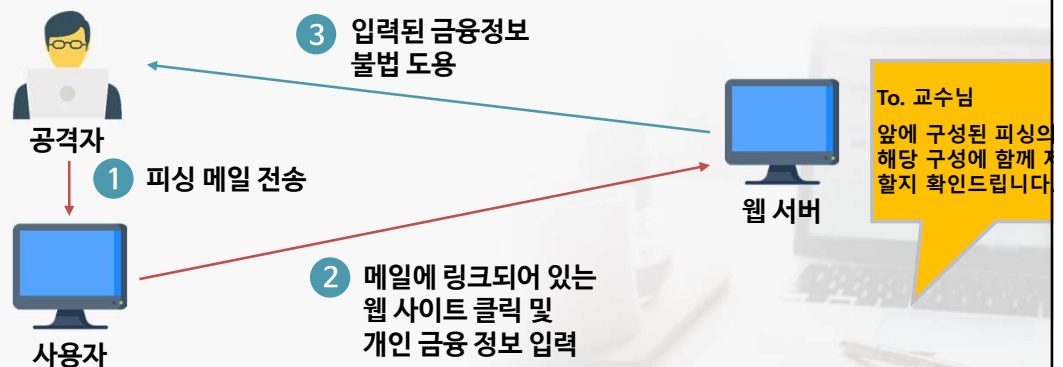


7] 피싱

학습하기



공격자가 금융 기관 등으로 위장하여 개인 정보를 알아낸 뒤 이를 이용하는 사기 수법





3 암호화 기술

1) 암호화 개요

학습하기

암호 기법

정보보호 서비스를 위한 기본적인 방법

암호 (cryptography)

평문을 해독 불가능한 형태로 변형하거나 또는 암호화된 통신문을 해독 가능한 형태로 변환하기 위한 원리, 수단, 방법 등을 취급하는 기술

암호학 (cryptology)

암호와 암호 해독을 연구하는 학문

1] 암호화 개요

학습하기

평문
(plain text)

암호화의 입력이 되는 원문인 의미 있는 메시지

암호문
(cipher text)

평문을 읽을 수 없는 메시지로 암호화(encryption)

복호화
(decryption)

암호화의 반대로, 암호문에서 평문으로 변환

1] 암호화 개요

학습하기

◇ 암호화 과정



암호화는 알고리즘과 키(key)로 되어 있음

키

평문과는 무관한 값

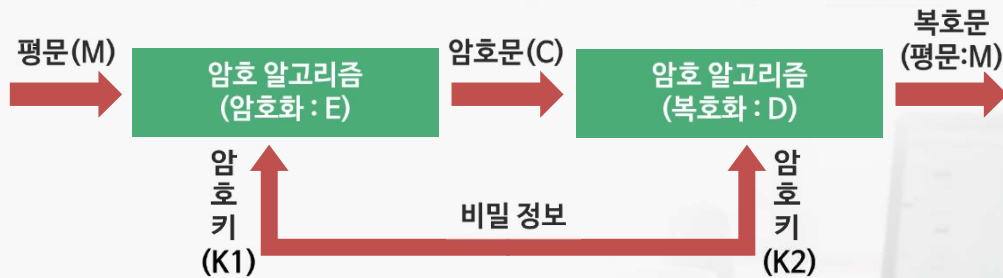
알고리즘

사용된 키에 따라 다른 출력

1] 암호화 개요

학습하기

◇ 암호화와 복호화 개념



- 암호화 : $C = E(M, K1)$
 - 비밀키 암호 시스템 : $K1 = K2$
 - 공개키 암호 시스템 : $K1 \neq K2$ ($K1$ 또는 $K2$ 는 다른 하나의 키로부터 이 계산적으로 불가능)
- 복호화 : $M = D(C, K2)$

1] 암호화 개요

학습하기



암호를 잘 사용하려면, 송신자와 수신자는 정보를 코드화된 형태로 바꿀 때 사용한 규칙이 어떠한 것인지를 알아야 함

비밀키 암호 기법

대칭키

공개키 암호 기법

비대칭키

예 암호화와 복호화의 간단한 예

	암호화(+13)	
electronic commerce		ryrpgebavp pbzzrepr
	복호화(-13)	

1] 암호화 개요

학습하기

비밀키
암호화

공개키
암호화

2] 비밀키 암호화(대칭키 암호화)

학습하기

◇ 보내는 사람과 받는 사람이 같은 키를 가지고 있는 경우

◆ 비밀키 암호화의 보안 문제

- ✓ 키의 비밀 유지에 달려 있음
- ✓ 비밀키 암호화의 보안은 암호화 알고리즘은 암호문을 해독하기 어려울수록 그 가치가 있음
- ✓ 암호화 알고리즘은 알고리즘의 보안이 아니라 키의 보안에 의존함

2] 비밀키 암호화(대칭키 암호화)

학습하기

◇ 보내는 사람과 받는 사람이 같은 키를 가지고 있는 경우

◆ 비밀키 암호화 기술 : 대체와 치환 기술

예 대체를 이용한 암호화

- 시저 암호 : 알파벳을 순서대로 나열한 다음 각 문자를 3문자 뒤에 위치에 있는 문자로 바꾸어 메시지를 암호화

2] 비밀키 암호화(대칭키 암호화)

학습하기

◇ 비밀키 암호화 시스템



2] 비밀키 암호화(대칭키 암호화)

학습하기

◇ 단점



통신하는 두 당사자가 서로 같은 키를 가지고 있어야 하므로 n 명의 상대방이 있는 경우 n 개의 비밀키가 있어야 함

- 만약 여러 상대방에게 같은 키를 사용한다면 그들은 서로의 메시지를 읽을 수 있게 됨



부인방지를 막을 수 없음

- 송신자와 수신자를 증명할 수 있는 인증을 할 수 없음
- A와 B가 같은 키를 가지고 있을 때 그 두 사람이 메시지를 만들고 암호화한 다음, 서로 다른 사람이 그 메시지를 보냈다고 주장할 수 있음

2] 비밀키 암호화(대칭키 암호화)

학습하기

◇ 단점



통신하는 두 당사자가 서로 같은 키를 가지고 있어야 하므로 n 명의 상대방이 있는 경우 n 개의 비밀키가 있어야 함

- 만약 여러 상대방에게 같은 키를 사용한다면 그들은 서로의 메시지를 읽을 수 있게 됨



부인방지를 막을 수 없음

- 송신자와 수신자를 증명할 수 있는 인증을 할 수 없음
- A와 B가 같은 키를 가지고 있을 때 그 두 사람이 메시지를 만들고

단점을 해결하기 위한 방법으로 비대칭 암호화 알고리즘을 사용하는
공개키 암호화 기법을 사용

3] 공개키 암호화

학습하기

◇ 개념

- ✓ 1976년 디퍼 (Diffie)와 힐만(Hellman)에 의해 제안된 공개키 암호기법의 개념
- ✓ 키에 관한 정보를 공개함으로써 키 관리의 어려움을 해결하고자 하는 방식
- ✓ 공개키 암호화 기법은 대체와 치환보다는 수학적 함수를 기본으로 함
- ✓ 한 개의 키만 사용하는 비밀키 암호화와는 달리 두 개의 분리된 키를 사용하는 비대칭 암호화

3] 공개키 암호화

학습하기

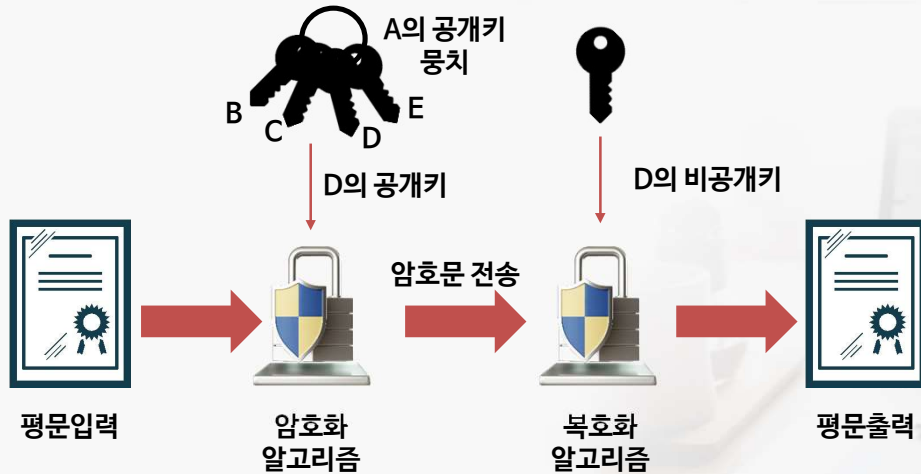
◇ 공개키와 비공개키

- | | |
|--------------------|---------------|
| 공개키 (public key) | 암호화할 때 사용하는 키 |
| 비공개키 (private key) | 복호화할 때 사용하는 키 |
- ✓ 비공개키는 당사자(소유자)만 알고 있고 다른 키는 당사자와 연결되어 있는 모든 것에 공개함
 - ✓ 한 쌍의 키는 하나의 유일한 모양을 가짐
 - 그 중 한 개의 키에 의해 암호화된 자료는 남은 다른 키에 의해서만 복호화가 가능

3] 공개키 암호화

학습하기

◇ 공개키 암호화 시스템



3] 공개키 암호화

학습하기

✓ 공개키는 암호화 기법을 메시지의 작성자 인증에 이용할 수 있음

디지털 서명(Digital Signature)

- A가 B에게 메시지를 보낼 때 A의 비공개키로 암호화하면 B는 A의 공개키로 이를 해독함
- A의 공개키로 해독이 가능하다면, 이 암호문은 A의 비공개키로 암호화한 것임이 틀림없으므로, A가 보낸 것임을 확신함



3] 공개키 암호화

학습하기

- ✓ 송신자의 메시지인 것을 확인할 수는 있어도 다른 누군가 메시지를 읽지 않았다고는 확신할 수 없음
- ✓ 송신자의 공개키를 사용하여 메시지를 해독할 경우 누구든 원하면 복호화할 수 있으므로 기밀성은 보장할 수 없음
- ✓ 기밀성 보장을 위해 방법
 - 송신자는 비공개키로 암호화하고 디지털 서명을 보장하고, 수신자는 공개키로 다시 암호화함
 - 이 메시지가 수신자에게 전달되면 이 마지막 암호문은 수신자만이 수신자의 비공개키로 해독하고 다시 송신자의 공개키로 해독할 수 있으므로 수신자의 메시지를 확인할 수 있음
 - 단점 : 복잡한 공개키 알고리즘을 네 번의 단계를 거쳐야 함

3] 공개키 암호화

학습하기

◇ 공개키 암호 기법의 특징

장점

- 안정성은 물론 편의성이 대폭 개선
- 부인방지 또는 부인봉쇄 : 메시지 내용 또는 발신원에 대한 부인을 방지할 수 있는 전자 서명 기능을 제공

단점

- 암호화의 처리속도가 비밀키 기법에 비해 비교적 느림
- 사용자의 비공개키 자체를 이용할 수 없다 할지라도 위장 공격에 취약함 : 인증기관에 대한 공격이 성공할 때 문제

3] 공개키 암호화

학습하기

공개키 시스템의 안전성에 대한 장점과
비밀키 시스템에서의 속도에 대한 장점을 모두 얻기 위하여...

두 기법을 상호 보완적으로 혼용하는 방법

디지털 봉투에서 편지의 내용은 비밀키 기법으로 암호화하고
이를 다시 공개키 기법으로 전자서명을 하는 경우에 해당함

4

인터넷 보안

1] 전자메일 보안

학습하기

◇ 필요성

- ✓ 컴퓨터의 사용자가 만약 불순한 의도를 가진다면 전자우편의 내용을 도청할 수 있고, 내용을 변경하여 전송하거나 전송 자체를 가로막을 수 있음
- ✓ 수신자가 이러한 공격 즉, 도청, 내용의 변경, 전송 방해 등을 감지할 수 없음

1] 전자메일 보안

학습하기

◇ 주요 기능

기밀성	사용자 인증	메시지 인증
송신 부인 방지	수신 부인 방지	재전송 공격 방지

1] 전자메일 보안



◇ 암호화 도구

1 PGP(Pretty Good Privacy)

- 필 짐머만(Phil Zimmermann)이 제작한 전자우편을 위한 암호 도구
- PGP가 제공해 주는 보안 기능 : 기밀성, 사용자 인증, 메시지 인증 및 송신부인 방지
- 공개키 인증으로서 공개키 인증에 대한 권한이 모든 사용자에게 주어져 있다는 것이 특징

1] 전자메일 보안



◇ 암호화 도구

2 S/MIME(Secure Multipurpose Internet Mail extension)

- RSA 데이터 보안 회사(RSA Data Security, Inc.)에서 제작한 도구로서 현재 넷스케이프(Netscape), 익스플로러(Explorer) 등의 메일 프로그램에서 지원
- S/MIME에서 지원하는 보안요구사항 : 기밀성, 메시지 인증, 송신 부인방지 및 사용자 인증

2] 웹 보안

학습하기

WWW는 기본적으로 안전하지 않다는 개념에서 출발함

- ✓ WWW 서비스를 지원하는 인터넷 자체가 개방성을 바탕으로 설계된 TCP/IP를 사용
- ✓ 웹은 기본적으로 인터넷과 TCP/IP 인트라넷상에서의 클라이언트/서버 응용 프로그램
- ✓ 웹은 컴퓨터와 네트워크보안에서 다루지 않은 새로운 보안의 위협에 직면

2] 웹 보안

학습하기

◇ 웹 보안의 취약성

- ✓ 인터넷에서 정보를 주고 받음
- ✓ 웹은 통일되고 새로운 정보를 볼 수 있는 창구이며, 비즈니스 거래를 위한 플랫폼의 역할 담당함
- ✓ 콘텐츠는 방대하고 웹 서버에 설치되어 운영되는 소프트웨어는 복잡함
- ✓ 초보 사용자들은 보통 웹 서비스에 대하여 클라이언트임

2] 웹 보안

학습하기

◇ 웹 보안의 취약성

- ✓ 인터넷에서 정보를 주고 받음
 - 웹은 인터넷 상의 웹 서버에서 누군가에 의해 공격 받기 쉬움
- ✓ 웹은 통일되고 새로운 정보를 볼 수 있는 창구이며, 비즈니스 거래를 위한 플랫폼의 역할 담당함
- ✓ 콘텐츠는 방대하고 웹 서버에 설치되어 운영되는 소프트웨어는 복잡함
- ✓ 초보 사용자들은 보통 웹 서비스에 대하여 클라이언트임

2] 웹 보안

학습하기

◇ 웹 보안의 취약성

- ✓ 인터넷에서 정보를 주고 받음
- ✓ 웹은 통일되고 새로운 정보를 볼 수 있는 창구이며, 비즈니스 거래를 위한 플랫폼의 역할 담당함
 - 웹 서버가 파괴되면 심각한 문제가 발생함
- ✓ 콘텐츠는 방대하고 웹 서버에 설치되어 운영되는 소프트웨어는 복잡함
- ✓ 초보 사용자들은 보통 웹 서비스에 대하여 클라이언트임

2] 웹 보안

학습하기

◇ 웹 보안의 취약성

- ✓ 인터넷에서 정보를 주고 받음
- ✓ 웹은 통일되고 새로운 정보를 볼 수 있는 창구이며, 비즈니스 거래를 위한 플랫폼의 역할 담당함
- ✓ 콘텐츠는 방대하고 웹 서버에 설치되어 운영되는 소프트웨어는 복잡함
 - 복잡한 소프트웨어는 많은 보안 약점을 숨기고 있을 수 있음
- ✓ 초보 사용자들은 보통 웹 서비스에 대하여 클라이언트임

2] 웹 보안

학습하기

◇ 웹 보안의 취약성

- ✓ 인터넷에서 정보를 주고 받음
- ✓ 웹은 통일되고 새로운 정보를 볼 수 있는 창구이며, 비즈니스 거래를 위한 플랫폼의 역할 담당함
- ✓ 콘텐츠는 방대하고 웹 서버에 설치되어 운영되는 소프트웨어는 복잡함
- ✓ 초보 사용자들은 보통 웹 서비스에 대하여 클라이언트임
 - 사용자들은 존재하는 보안의 위험은 알 필요가 없고 효과적으로 대응할 도구나 지식을 가지고 있지 않음

2] 웹 보안

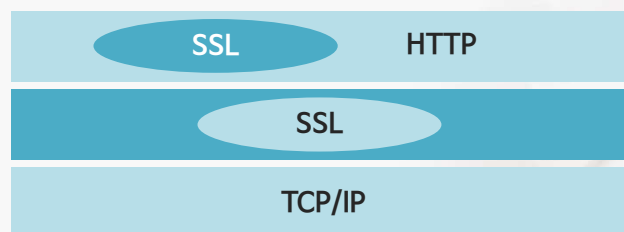
학습하기

◇ 웹 응용 프로그램에 대한 보안 프로토콜

✓ 서버와 브라우저의 인증을 제공하고 서버와 브라우저 사이의 통신의 비밀성과 무결성을 보장함

✓ S-HTTP와 SSL

웹 보안 구현 방법의 계층



2] 웹 보안

학습하기

◇ S-HTTP(Secure HTTP)

✓ 서류의 인증과 보안을 보장하는 HTTP를 지원하도록 구성됨

✓ 1994년 미국의 EIT(Enterprise Integration Technologies)사에서 HTTP 보안 요소를 첨가한 웹 보안 프로토콜로서 범용으로 사용될 수 있도록 설계됨

✓ 통신의 기밀성, 인증, 무결성 등을 지원함

2] 웹 보안

학습하기

◇ SSL(Secure Socket Layer)

- ✓ 통신망 스택 (응용프로그램 계층, TCP 전송 계층, IP 통신 계층 사이)에서 HTTP보다 하위에 작용하여 통신채널의 비밀을 보장함
- ✓ 넷스케이프사에서 개발한 웹 보안 프로토콜로서 응용 계층과 TCP/IP 사이에 위치함
- ✓ 내용의 암호화, 서버의 인증, 메시지 내용의 무결성을 제공함

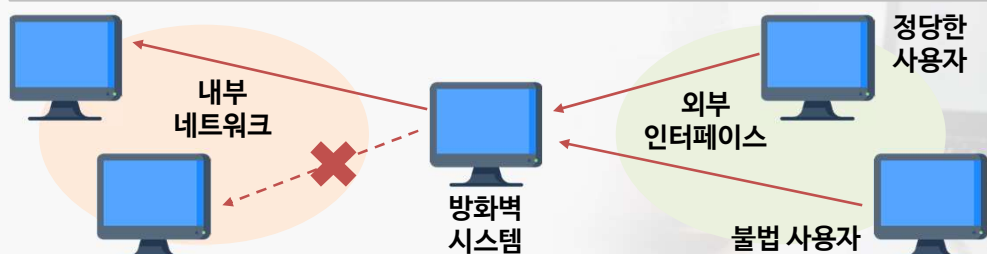
3] 방화벽

학습하기

◇ 개념

방화벽 : 침입차단시스템

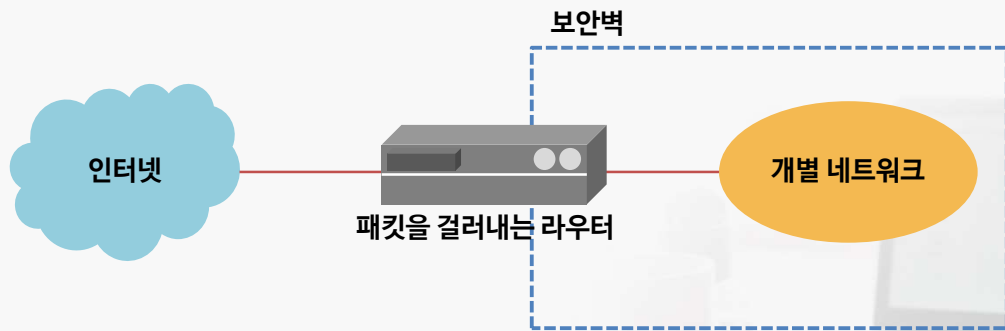
인터넷 같은 외부 네트워크에 연결된 LAN과 같은 내부 네트워크를 외부의 불법적인 사용자의 침입으로부터 안전하게 보호하기 위한 정책 및 이를 지원하는 하드웨어 및 소프트웨어를 총칭



3] 방화벽

학습하기

◇ 패킷을 걸러내는 라우터



정리하기

정리하기

정보 보안의 개요

- ◆ 정보보안
 - 모든 정보 보호 활동을 포괄하는 광의의 개념
- ◆ 정보보안의 요구사항
 - 비밀성, 무결성, 가용성

악성 프로그램과 해킹

- ◆ 컴퓨터 바이러스는 컴퓨터의 운영을 방해하는 악성 프로그램
 - 웜, 바이러스, 트로이 목마

SUMMARY


정리하기

암호화 기술

- 다양한 정보보호 서비스를 위한 기본적인 방법이 암호 기법
- 암호화 기법 분류
 - 비밀키 암호화, 공개키 암호화

인터넷 보안

- 전자 메일 보안
- 웹 보안
- 방화벽



ANNOUNCEMENT

차시예고

8주차 9주차 10주차 11주차 12주차 13주차 14주차 기말고사

- 한 학기 동안 수고하셨습니다.

