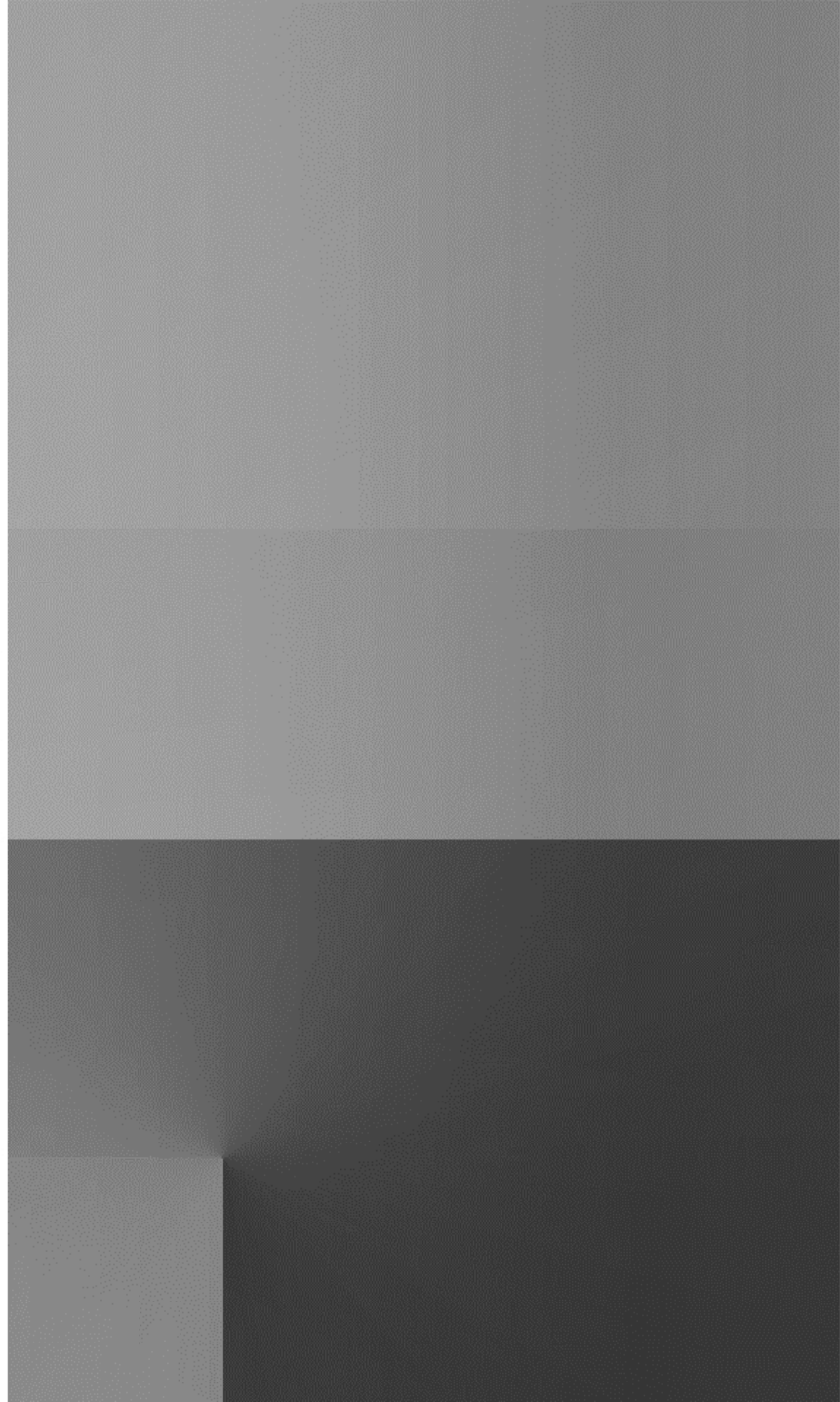
dongguk UNIVERSITY

정보보호 개론 “2주차 강의”

윤홍수

2025. 03. 13

Table of Contents



정보보호 중요성

✓ 국가 주도

- 배경

- 1990년대 이후 디지털 범죄와 사이버 공격이 급증

(특히 디도스(DDoS) 공격과 같은 피해가 큰 사건들이 발생하기 시작)

- 당시 한국은 정보화 사회로 빠르게 진입 ➔ 이러한 변화는 디지털 범죄에 대한 대응이 중요한 국가적 과제

정보보호 중요성

※ 1990년대 이후 디지털 범죄와 사이버 공격이 급증 배경

1. 인터넷 보급과 네트워크 확산 : 1990년대 중반부터 인터넷 대중화

2. 정보화 사회로의 전환 : 정부와 기업, 금융기관, 개인들이 데이터와 정보의 디지털화에 집중

3. 범죄 수법의 진화 : 해킹 기법, 악성 소프트웨어의 진화로 인해 사이버 범죄의 방법 정교화

4. 국제적 범죄 조직의 등장 : 1990년대 후반부터 국제 해커 조직과 범죄 조직 연계

정보보호 중요성

※ 한국은 정보화 사회로 빠르게 진입

1. 한국이 정보화 사회로 빠르게 진입한 배경에는 정부 주도의 강력한 정보화 정책과 투자가 크게 작용

2. 전산망 확대와 인터넷 인프라 구축 (전산망 확대와 초고속 통신망 구축)

3. 1995년 초고속 정보통신망 구축 사업 : 정보화 촉진 기본법 제정

4. 정부 주도의 정보화 추진 정책 : 김영삼 정부

5. 정보통신부 설립 : 1994년에는 정보통신부가 설립되어 국가 차원의 정보화 추진 총괄

6. 전자정부 구축 : 1990년대 중반부터 정부는 행정 시스템을 디지털화

시스템 보안의 이해

- **시스템**
  - 시스템은 하드웨어뿐만 아니라 소프트웨어까지 매우 많은 것을 포괄
  - 시스템과 관련된 보안 주제는 훨씬 큰 범위의 보안, 조직이나 국가 단위의 보안 요소를 다루는 일과 흡사

시스템 보안의 이해

시스템 보안 주제

1. 계정 관리
   - 사용자를 식별하는 가장 기본적인 인증 수단 : 아이디와 패스워드
   - 계정 관리 : 시스템 보안의 시작
2. 세션 관리
   - 사용자가 로그인하면 시스템과 연결된 상태를 유지하는 것.
   - 예 : 은행 웹사이트 로그인 → 일정 시간이 지나면 자동 로그아웃(세션 종료)되어 다른 사람이 내 계정을 몰래 사용할 수 없도록 함
3. 접근 제어
   - 중요한 시스템이나 데이터에 허가된 사용자만 접근할 수 있도록 제한하는 것
   - 예 : Wi-Fi 비밀번호 → 특정 사용자만 네트워크에 접속할 수 있도록 제한

시스템 보안의 이해

- **시스템 보안 주제**

4. 권한 관리

  - 시스템의 각 사용자가 필요한 정보에만 접근하고, 불필요한 정보에는 접근하지 못하도록 제한하는 것.
  - 예 : 회사 내부 문서 관리 → 일반 직원은 읽기만 가능, 관리자만 수정 가능

5. 로그 관리

  - 시스템 내부나 네트워크를 통해 외부에서 시스템에 어떤 영향을 미칠 경우 그 내용을 기록하여 관리하는 것
  - 예 : 컴퓨터 로그인 기록 → 누가 언제 로그인했는지 기록

6. 취약점 관리

  - 시스템 자체의 결함을 체계적으로 관리하는 것
  - 예 : 스마트폰 업데이트 / 웹사이트 보안 점검 / 비밀번호 변경

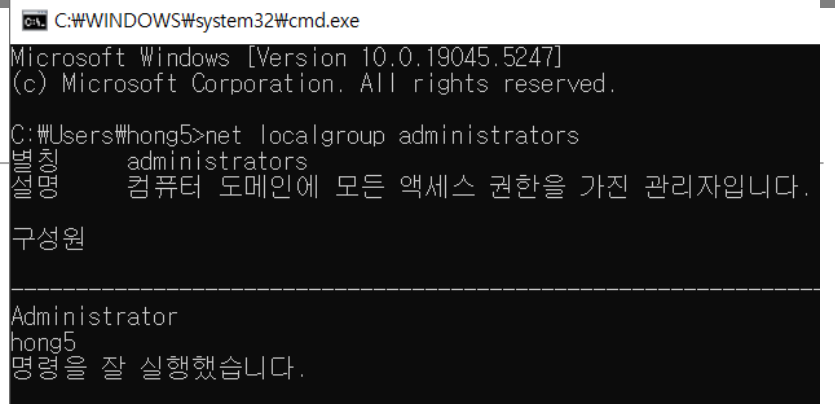
계정 관리

- **계정관리**
  - 식별과 인증
    - 식별: 어떤 시스템에 로그인하려면 먼저 자신이 누군지를 알림
    - 인증: 로그인을 허용하기 위한 확인
  - 보안의 네 가지 인증 방법
    - **알고 있는 것**
      - 머릿속에 기억하고 있는 정보를 이용하여 인증 수행
    - **가지고 있는 것**
      - 신분증이나 OTP 장치 등으로 인증 수행
    - **자신의 모습**
      - 홍채와 같은 생체 정보로 인증 수행
    - **위치하는 곳**
      - 현재 접속을 시도하는 위치의 적절성을 확인하거나 콜백을 사용해 인증 수행
      - 콜백: 접속을 요청한 사람의 신원을 확인, 미리 등록된 전화번호로 전화를 되걸어 접속을 요청한 사람이 본인인지 확인

계정 관리

- **계정관리**
  - **위치하는 곳 ➔ 콜백**
    - 현재 접속을 시도하는 위치의 적절성을 확인하거나 콜백을 사용해 인증 수행
    - 콜백: 접속을 요청한 사람의 신원을 확인, 미리 등록된 전화번호로 전화를 되걸어 접속을 요청한 사람이 본인인지 확인

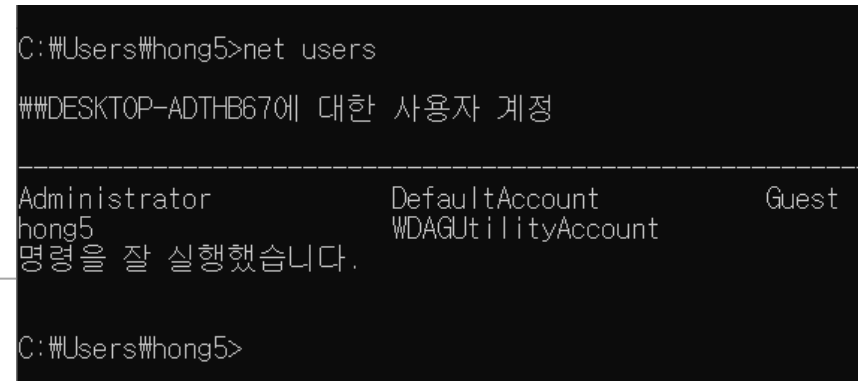
계정 관리



■ 운영체제의 계정 관리

- 운영체제
  - 시스템을 구성하고 운영하기 위한 가장 기본적인 소프트웨어
    - 운영체제에 대한 권한을 가지게 되면 해당 시스템의 다른 응용 프로그램에 대해서도 어느 정도의 권한을 가질 수 있음
    - 일반 사용자 권한의 계정도 시스템의 상당 부분에 대한 읽기 권한을 가짐

- 윈도우의 계정 관리
  - 관리자 계정: administrator / 시스템에 가장 기본으로 설치되는 계정
  - 관리자 그룹의 계정의 존재 형태를 확인하려면 윈도우에서 net localgroup administrators 명령을 사용
    - 현재 컴퓨터의 로컬 Administrators 그룹에 속한 사용자와 그룹 목록을 확인할 수 있습니다.
  - 사용자 계정을 모두 확인하려면 net users 명령을 사용
    - 현재 컴퓨터(또는 도메인)에 존재하는 사용자 계정의 목록을 표시합니다.



계정 관리

- **유닉스/리눅스의 계정 관리**
  - 리눅스/유닉스 계열의 시스템(이후 유닉스)에서는 기본 관리자 계정으로 root가 존재
  - 리눅스/유닉스에서는 /etc/passwd 파일에서 계정 목록을 확인

  - **시스템의 모든 사용자 계정 정보가 저장된 파일로, 각 사용자의 계정 정보를 한 줄씩 기록하고 있다**
  - **하지만, 보안상의 이유로 실제 암호는 포함되지 않고, 사용자 정보만 저장됨**

계정 관리

- 유닉스/리눅스의 계정 관리

명령어

cat /etc/passwd

root:x:0:0:root:/root:/bin/bash
user1:x:1001:1001:John:/home/user1:/bin/bash
guest:x:1002:1002:Guest:/home/guest:/bin/sh

셸(Shell)은 스크립트 언어로 명령어의 해석을 통해 리눅스 커널에 전달하는 중간자 역할

계정 관리

https://nearhome.tistory.com/49

- **유닉스/리눅스의 계정 관리**
  - /etc/passwd 파일의 구성

```
[root@centos7 ~]# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash              #1
bin:x:1:1:bin:/bin:/sbin/nologin             #2
daemon:x:2:2:daemon:/sbin:/sbin/nologin      #3
adm:x:3:4:adm:/var/adm:/sbin/nologin         #4
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin     #5
...
nobody:x:99:99:Nobody:/:/sbin/nologin        #6
...
ntp:x:38:38::/etc/ntp:/sbin/nologin          #7
...
gdm:x:42:42::/var/lib/gdm:/sbin/nologin      #8
```

사용자명	UID	설명
#1	0	시스템의 관리자 계정, 시스템을 관리하기 위한 특권(Privilege)을 가지고 있기 때문에 파일에 대한 권한(Permission)의 제약을 거의 받지않음
#2	1	시스템에 구동중인 바이너리 파일을 관리하기 위한 계정
#3	2	백그라운드 프로세스에 대한 작업을 제어하기 위한 시스템 계정
#4	3	시스템 관리를 위한 계정으로 시스템 로깅 같은 특정 시스템 파일을 관리
#5	4	로컬 프린트를 위한 데몬 계정
#6	99	익명 연결 계정, 웹 서비스와 같이 누구나 연결이 가능해야 하는 서비스가 있는 경우 필요한 계정
#7	38	컴퓨터 시간을 동기화 시켜주기 위하여 만들어진 Network Time Protocol 계정
#8	42	그래픽 화면 관리 계정

계정 관리

- **유닉스의 계정 관리**
  - /etc/shadow 파일의 구성

명령어

cat /etc/shadow ➔ 어떤 계정에서만 볼 수 있을 까요?

user1:6abc123$XYZ456...:19345:0:99999:7:::

계정 관리

- **유닉스의 계정 관리**
  - /etc/shadow 파일의 구성

user1:6abc123$XYZ456...:19345:0:99999:7:::

계정
비번 : 암호화 (SHA-512 해시)
19345 : 암호 변경 후 지난 날짜
0 : 패스워드 변경되기전 최소 사용 기간 (0이면 언제든 변경 가능)
99999 : 패스워드 변경전 최대 사용 기간
7 : 패스워드 사용 만기일 전 경고 메시지를 제공하는 일 수

계정 관리

- **유닉스의 계정 관리**
  - 유닉스에서 그룹은 /etc/group 파일에서 확인

명령어

cat /etc/group

sudo:x:27:user1,user2

그룹 이름
비밀번호
그룹 id
그룹에 속한 사용자 목록

계정 관리

✓리눅스 파일 시스템

- 리눅스 파일 권한 구조 (755 분석)

  - 리눅스 파일 권한은 파일 소유자(Owner), 그룹(Group), 모든 사용자(Other)에 대해 세 가지 권한

  - 읽기(read, r)

  - 쓰기(write, w)

  -실행(execute, x)

    - 7 5 5

      - 7 : 소유자 권한 자리

      - 5 : 그룹 권한 자리

      - 5 : 모든 사용자 권한 자리

```
root@2363f9b4464b:/# ls -al
total 84
drwxr-xr-x   1 root root 4096 Jul 16 06:08 .
drwxr-xr-x   1 root root 4096 Jul 16 06:08 ..
-rwxr-xr-x   1 root root    0 Jun 12 15:29 .dockerenv
drwxr-xr-x   1 root root 4096 Feb 14 16:24 bin
drwxr-xr-x   2 root root 4096 Apr 24  2018 boot
drwxr-xr-x   5 root root  340 Jul 17 00:22 dev
drwxr-xr-x   2 root root 4096 Feb 14 16:26 docker-entrypoint-initdb.d
```

계정 관리

✓리눅스 파일 시스템

- 숫자 권환

  - 읽기 r ➔ 4

  - 쓰기 w ➔ 2

  - 실행 x ➔ 1

➔ 755는

  - 사용자 : 읽고, 쓰고 실행 가능 ➔ 4 + 2+ 1 ➔ 7

  - 그룹 사용자 : 읽고, 실행 가능 ➔ 4 + 1 ➔ 5

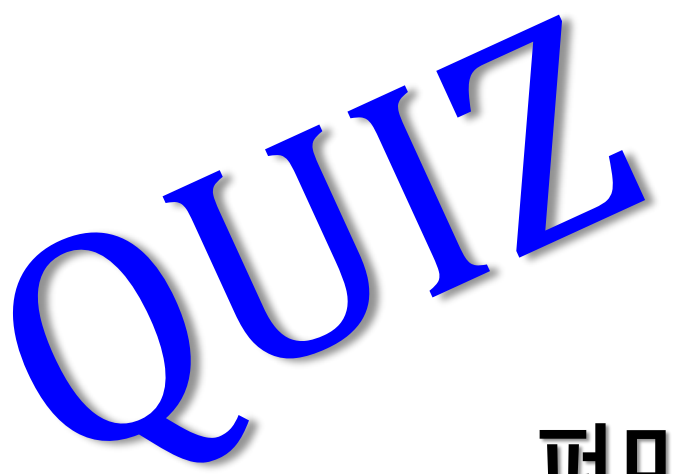
  - 모든 사용자 : 읽고, 실행 가능 ➔ 4 + 1 ➔ 5

계정 관리

✓**리눅스 파일 권한 분석 시**

- 파일 권한을 통해 **누가 파일을 사용했는지 확인 가능**
- 권한 변경 기록 확인 : **파일 권한이 갑자기 변경 되었을 경우 (악의적 접근 가능성 있음)**
- 로그 파일과의 연관성 : **특정 사용자의 비 정상적인 권한 (수정 할 수 없는 파일 수정)**
- 악성 코드 감지 : 악성 코드 흔적
- 데이터 유출 및 무단 접근 확인 : **중요한 정보가 무단으로 읽혀졌거나 복사된 것을 추적**
- 시간 기록과 권한의 연관성 : **파일이 언제 수정되었고 누가 수정했는지 확인 가능**

계정 관리



퍼미션 : 711

의미

진법

✓이산적 수치

- 2진법 : 0, 1로 표현하는 방법
- 8진법 : 0부터 7까지, 즉 8개의 숫자를 사용하는 진법
- 10진법 : 우리가 일상적으로 사용하는 숫자 체계
- 16진법 : 16진법은 0부터 9까지 숫자와 A부터 F까지 총 16개의 숫자를 사용하는 진법

진법

✓**이산적 수치 – 2진법**

네트워크 패킷이나 암호화 데이터 분석, 비트 단위의 흐름 추적

- 사용처

  - **컴퓨터 내부에서 모든 데이터는 2진법으로 표현**

  - 하드웨어(CPU, 메모리)와 기본 데이터 처리에서 2진법은 핵심

  - 비트 연산과 같은 **low level 프로그래밍이나 시스템 개발, 임베디드 시스템에서 많이 사용**

- 중요성

  - 기본적으로 모든 데이터는 2진법으로 저장

  - 파일이나 메모리 덤프를 분석할 때, 비트 수준에서의 데이터 표현을 이해하는 게 중요

  - **디스크 이미징이나 네트워크 패킷 분석에서 사용**

진법

✓**이산적 수치 – 8진법**

파일 퍼미션과 관련된 분석에 한정적, 유닉스/리눅스 시스템 포렌식에서 유용

- 사용처

  - 과거에 구형 시스템에서 메모리 주소나 퍼미션 관리에 사용

  - 특히 유닉스나 리눅스 환경에서 파일 권한을 나타낼 때 8진법이 자주 사용

  - 예를 들어, 파일 권한 755는 8진법 표현

- 중요성

  - 직접적으로 많이 사용되지는 않지만, 유닉스/리눅스 환경의 파일 권한 분석 시 중요

  - 시스템 파일의 퍼미션 정보를 확인할 때 도움

진법

✓이산적 수치 – 16진법

파일 시스템 분석, 메모리 분석, 네트워크 트래픽 분석 핵심

- 사용처

  - **컴퓨터에서 메모리 주소나 파일의 바이너리 데이터를 표현할 때 매우 자주 사용**

  - **16진법은 2진법보다 사람이 읽기 편하게 긴 이진 데이터를 짧고 간결하게 표현**

  - 네트워크 프로토콜 분석(예: Wireshark), 저수준 시스템 프로그래밍(예: 메모리 덤프, 디버깅)에서 핵심적으로 사용

- 중요성

  - 가장 중요한 진법 중 하나

  - **파일 시스템 분석, 메모리 분석, 네트워크 패킷 분석 등에서 16진 데이터를 해석해야 하는 경우가 많기 때문**

  - 파일 헤더 정보를 분석할 때, 파일 구조가 16진법으로 표현

  - 디스크 이미지나 메모리 덤프 분석에서 핵심적인 역할

진법

✓이산적 수치 – 2진법 (Binary)

- 2진법 => 10진법

$$2\text{진법 } 101 = 1\times2^2 + 0\times2^1 + 1\times2^0 = 1\times4 + 0\times2 + 1\times1$$
$$= 4 + 0 + 1 = 5\ (10\text{진법})$$

- 10진법 => 2진법

10진법 13 ➔ 2진법 1101

13 ÷ 2 = 6 (몫), 나머지 1
6 ÷ 2 = 3 (몫), 나머지 0
3 ÷ 2 = 1 (몫), 나머지 1
1 ÷ 2 = 0 (몫), 나머지 1

진법

✓이산적 수치 – 8진법 (Octal)

- 8진법 => 10진법

$$8\text{진법 } 17 = 1\times8^1 + 7\times8^0$$
$$= 1\times8 + 7\times1$$
$$= 8 + 7 = 15\ (10\text{진법})$$

- 10진법 => 8진법

10진법 65 ➔ 8진법 101

65 ÷ 8 = 8 (몫), 나머지 1

8 ÷ 8 = 1 (몫), 나머지 0

1 ÷ 8 = 0 (몫), 나머지 1

진법

A 10, B 11, C12, D 13, E 14, F 15

✓이산적 수치 – 16진법 (Hexadecimal)

- 16진법 => 10진법

16진법 1A = $1\times16^1 + A\times16^0$
= $1\times16 + 10\times1$ (A = 10)
= 16 + 10 = 26 (10진법)

- 10진법 => 16진법

10진법 125 ➔ 16진법 7D
125 ÷ 16 = 7 (몫), 나머지 13 (D)
7 ÷ 16 = 0 (몫), 나머지 7

진법

수 변환

이진수 (베이스-2)	십진수 (베이스-10)	팔진수 (베이스-8)	십육진수 (베이스-16)
0	0	0	0
01	1	1	1
10	2	2	2
11	3	3	3
100	4	4	4
101	5	5	5
110	6	6	6
111	7	7	7
1000	8	10	8
1001	9	11	9
1010	10	12	A
1011	11	13	B
1100	12	14	C
1101	13	15	D
1110	14	16	E
1111	15	17	F
10000	16	20	10
10001	17	21	11
10010	18	22	12
10011	19	23	13
10100	20	24	14

세션 관리

- **세션**
  - 세션의 개요
    - '사용자와 시스템 사이 또는 두 시스템 사이의 활성화된 접속'을 의미
    - 예) 줄서고 있을 때 친구에게 자리 맡아달라고 부탁하기
  - 동화 〈해님 달님〉의 이야기
    - 일하러 나간 어머니를 기다리던 오누이는 호랑이의 손을 확인하고 문을 열어달라고 함
    - 이 과정은 오누이 입장에서 어머니의 세션이 유효한지 확인하기 위해 '손의 모양새'를 이용한 것

세션 관리

- **세션**
  - 세션(Session)은 사용자가 시스템(웹사이트, 서버 등)과 연결된 상태를 유지하는 과정을 의미
  - 즉, 로그인해서 로그아웃할 때까지 유지되는 연결 정보라고 할 수 있다

  - 동작 원리
    - 사용자가 로그인하면, 서버에서 세션 ID를 발급
    - 사용자는 세션 ID를 이용해 계속 서버와 연결 유지
    - 일정 시간이 지나거나, 로그아웃하면 세션이 종료됨
    - 예
      - 로그인 후 장바구니에 담은 상품이 그대로 유지됨
      - 브라우저를 닫거나 세션이 만료되면 장바구니 정보가 사라짐

세션 관리

```php
<html>
<head>
<meta charset="utf-8">
</head>
<body>
<?php
    session_start();
    echo "세션 시작!!!<br>";

    $_SESSION['userid'] = "ocella";
    $_SESSION['username']  = "박영준";
    echo '세션 등록 완료!!!<br>';

    echo $_SESSION['userid']."<br>";
    echo $_SESSION['username']."<br>";
?>
</body>
</html>
```

session_use.php

```php
<?php
    session_start();

    $userid = $_SESSION["userid"];
    $username = $_SESSION["username"];
?>
<html>
<head>
<meta charset="utf-8">
</head>
<body>
<h3>등록된 세션의 사용</h3>
<ul>
    <li>등록된 세션(userid) : <?= $userid?><
    <li>등록된 세션(username) : <?= $usernam
```

접근 제어

접근 제어

- 접근 제어
  - 접근 제어: 적절한 권한을 가진 인가자만 특정 시스템이나 정보에 접근하도록 통제하는 것
  - 시스템의 보안 수준을 갖추기 위한 가장 기본적 수단
  - 시스템 및 네트워크에 대한 접근 제어의 가장 기본적인 수단은 IP와 서비스 포트

운영체제의 접근 제어

운영체제	서비스 이름	사용 포트	특징
유닉스 (리눅스 포함)	텔넷	23	암호화되지 않음
	SSH	22	SFTP 가능
	XDMCP	6000	유닉스용 GUI(XManager)
	FTP	21	파일 전송 서비스
윈도우	터미널 서비스	3389	포트 변경 가능
	GUI 관리용 툴		VNC, Radmin 등

접근 제어

- **원격 접속 프로그램 포트 관련 해킹 증가**
  - 코로나19 팬데믹 동안 재택근무와 원격 업무가 증가하면서, 원격 접속 프로그램(예: RDP, VNC, TeamViewer 등)에 대한 해킹 시도가 급격히 증가
  - 해커들은 열려 있는 포트(Port)를 스캔하여 보안이 취약한 시스템에 접근하려 했고, 특히 비밀번호가 약한 계정이나 보안 설정이 미흡한 시스템이 주요 공격 대상이 됨

프로그램	기능	기본 포트 번호
RDP (Remote Desktop Protocol)	Windows 원격 데스크톱 접속	**3389**
VNC (Virtual Network Computing)	원격 화면 공유	**5900**
SSH (Secure Shell)	원격 터미널 접속	**22**
TeamViewer	원격 제어 및 지원	**TCP/UDP 5938**
AnyDesk	원격 제어 및 지원	**TCP 7070**

권한 관리

■ 운영체제의 권한 관리

▪ 윈도우의 권한 관리

- 임의의 디렉터리를 만들고 마우스 오른쪽 버튼을 눌러 [등록정보]-[보안]을 선택하면 권한 설정 화면이 나타남

- NTFS에서 그룹 또는 개별 사용자에 대해 설정할 수 있는 권한의 종류
  1. 모든 권한: 디렉터리 접근 권한과 소유권을 변경하고 하위 디렉터리와 파일 삭제 가능
  2. 수정: 디렉터리 삭제가 가능하며 읽기, 실행, 쓰기 권한이 주어진 것과 동일
  3. 읽기 및 실행: 읽기 수행, 디렉터리나 파일 옮기기 가능
  4. 디렉터리 내용 보기: 디렉터리 내의 파일, 디렉터리 이름 보기 가능
  5. 읽기: 디렉터리 내용 읽기만 가능
  6. 쓰기: 해당 디렉터리에 하위 디렉터리와 파일 생성, 소유권이나 접근 권한의 설정 내용 확인 가능

권한 관리

리눅스의 권한 관리

- 리눅스에서는 파일과 폴더(디렉터리)마다 누가 접근하고, 수정할 수 있는지를 정하는 권한(퍼미션, Permission) 시스템이 있다
- 리눅스에서는 "모든 것이 파일이다!" → 파일이든 폴더든 모두 권한이 설정됨
- 보안 강화를 위해 사용자별로 권한을 제한하여, 허가되지 않은 접근을 차단

- ls -l testfile.txt

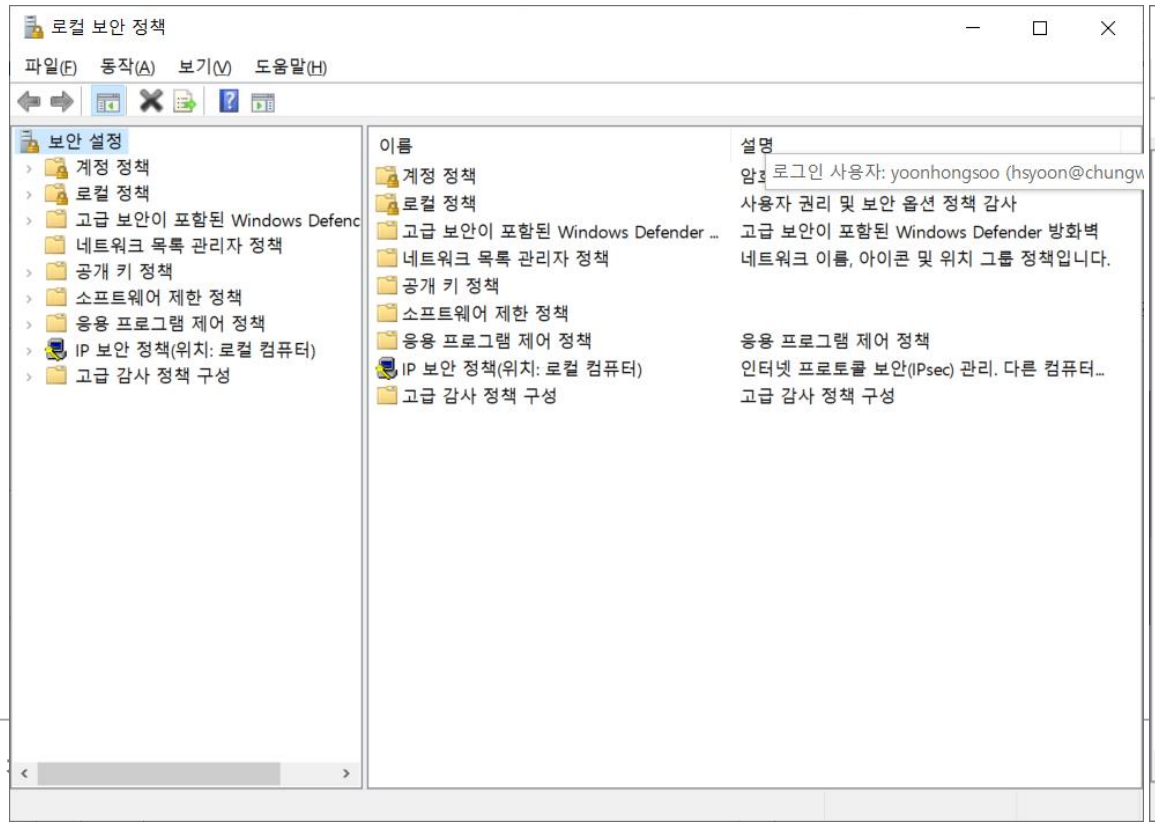
- -rw-r--r-- 1 user1 staff 1024 Mar 12 12:00 testfile.txt
- Blue color 권한 정보

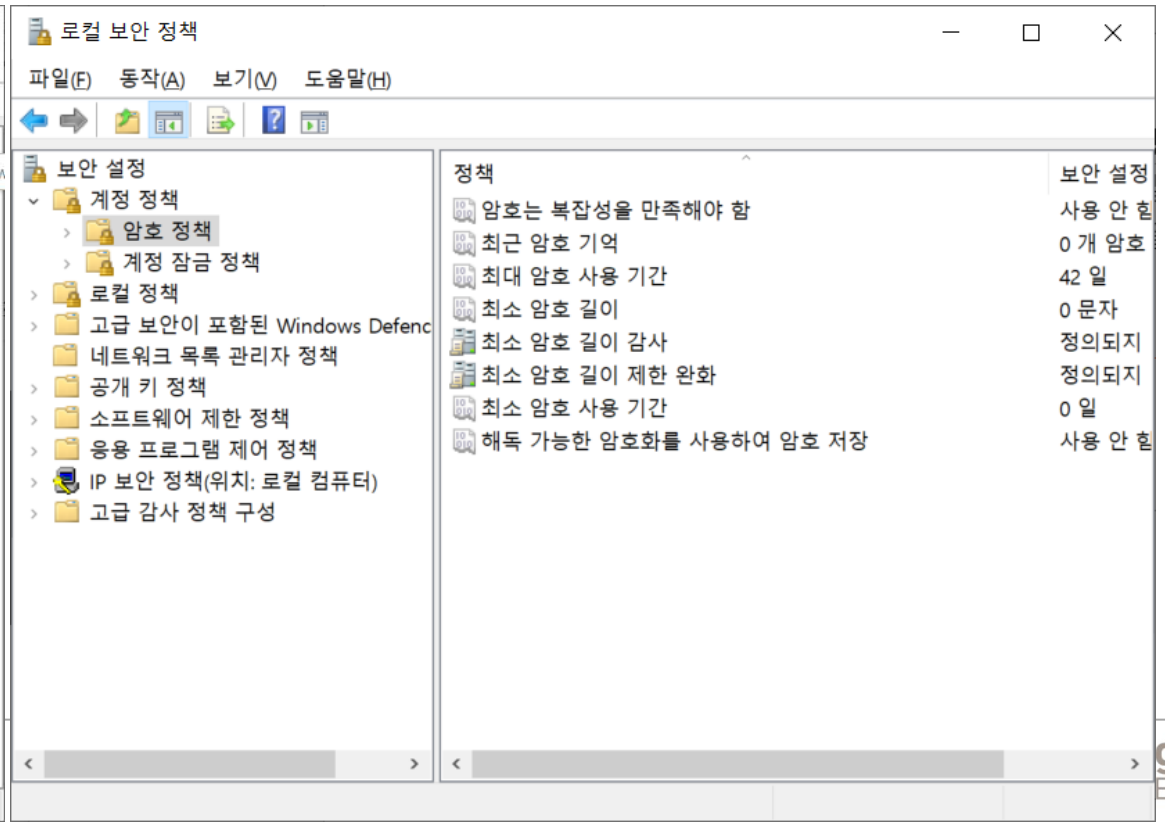
권한 관리

- **리눅스의 권한 관리**
  - -rw-r--r-- 1 user1 staff 1024 Mar 12 12:00 testfile.txt
  - 무슨 의미 인가요?

로그 관리

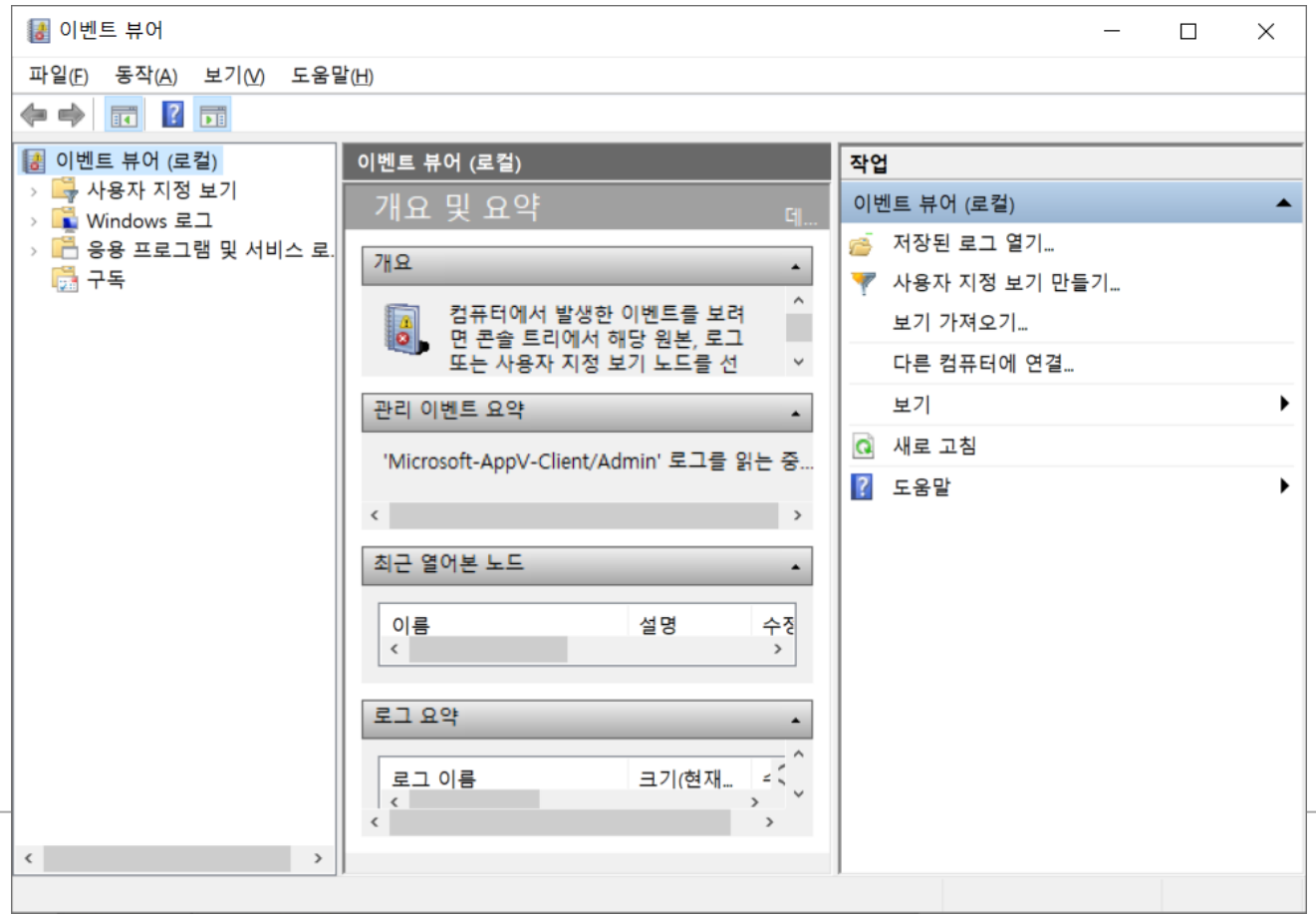
- **운영체제의 로그 관리**
  - 윈도우 보안 정책
    - 윈도우의 보안 정책은 아래 그림과 같이 확인 할 수 있다
    - 찾기 ➔ 로컬 보안 정책을 실행 시키면 확인 할 수 있다.

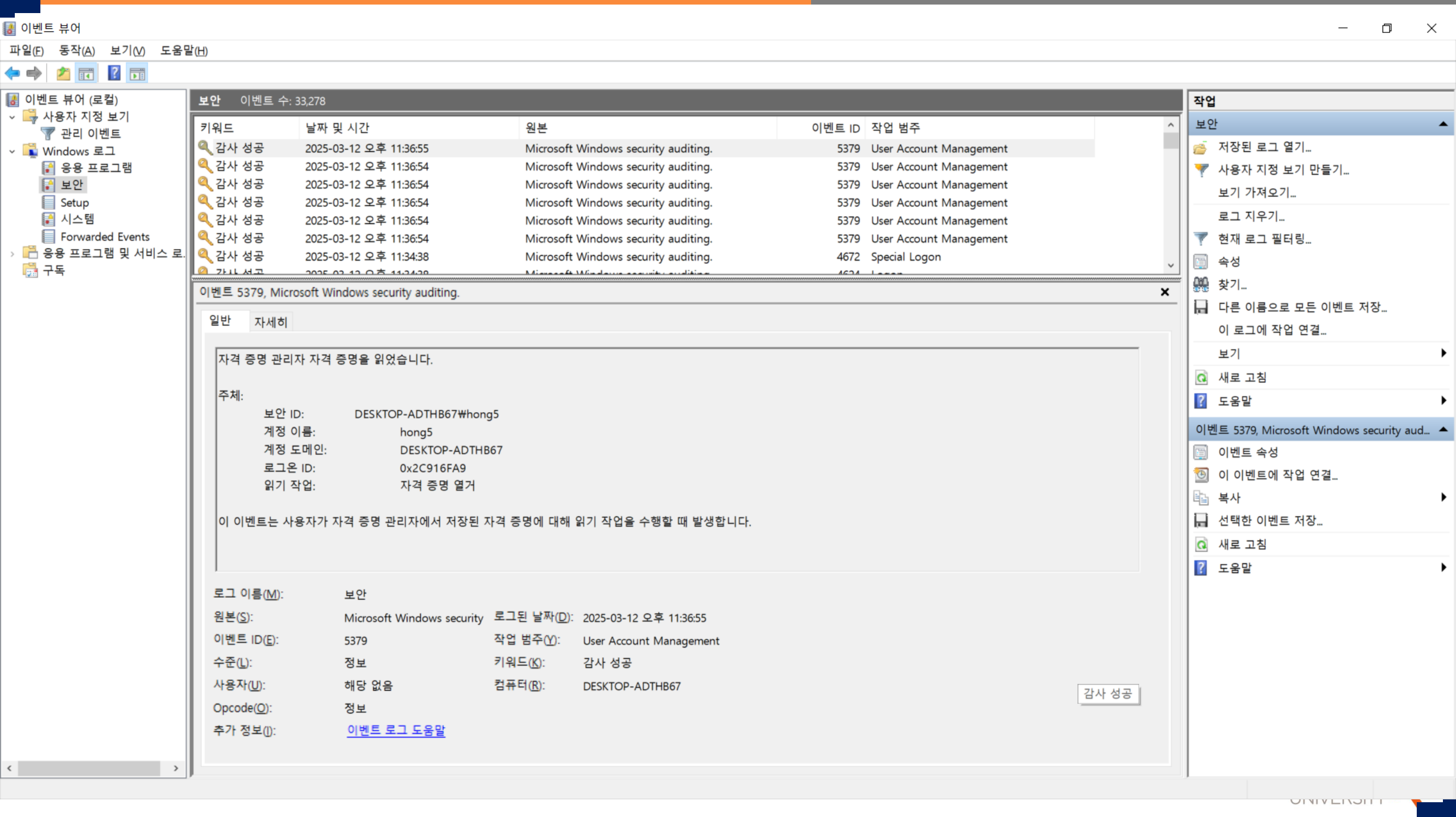




로그 관리

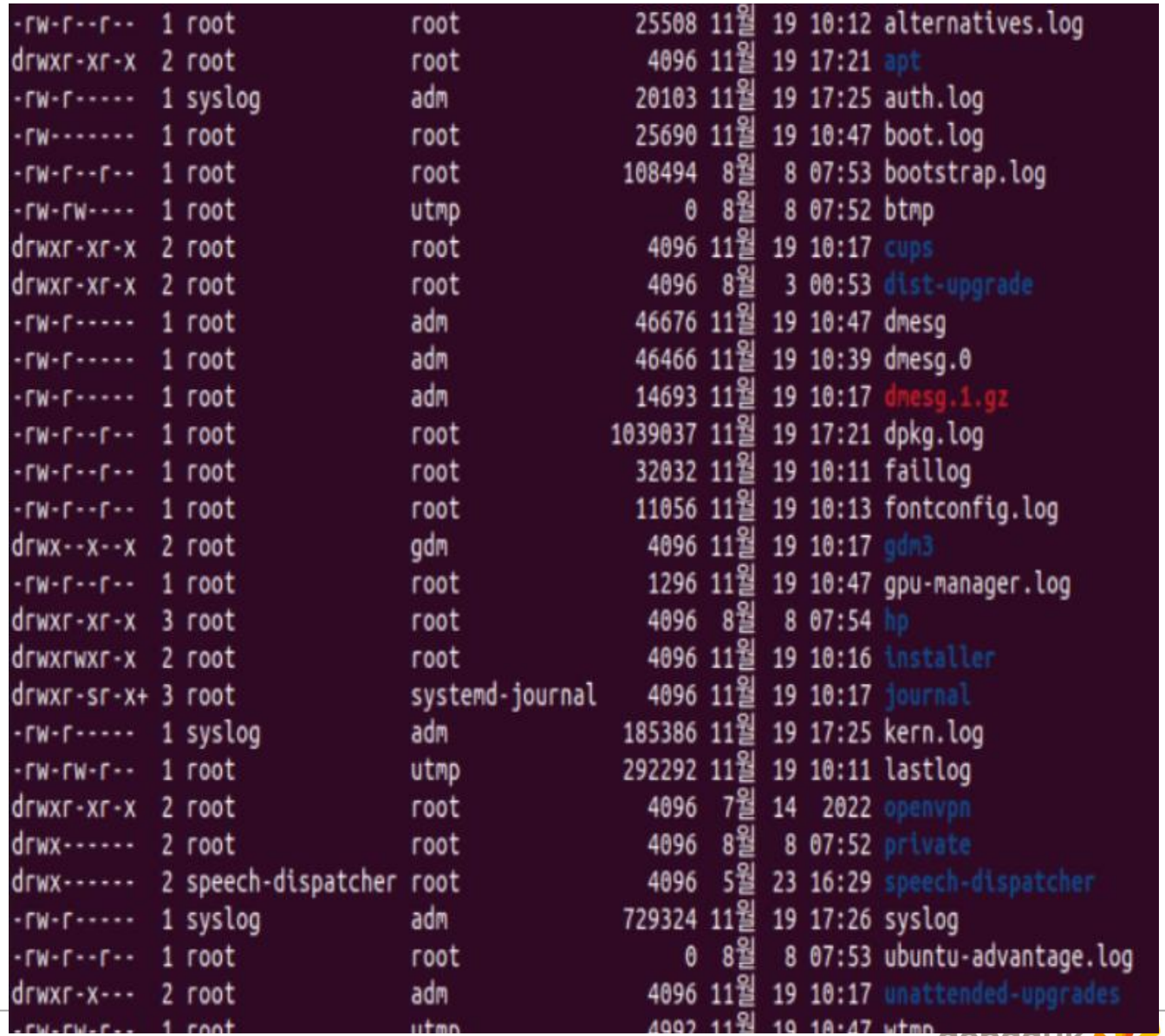
- **운영체제의 로그 관리**
  - 윈도우 로그
    - 찾기 ➔ 이벤트 뷰어를 실행 시키면 확인 할 수 있다.




이벤트 뷰어
파일(F) 동작(A) 보기(V) 도움말(H)
이벤트 뷰어 (로컬)
사용자 지정 보기
관리 이벤트
Windows 로그
응용 프로그램
보안
Setup
시스템
Forwarded Events
응용 프로그램 및 서비스 로...
구독
보안 이벤트 수: 33,278
키워드 날짜 및 시간 원본 이벤트 ID 작업 범주
감사 성공 2025-03-12 오후 11:36:55 Microsoft Windows security auditing. 5379 User Account Management
감사 성공 2025-03-12 오후 11:36:54 Microsoft Windows security auditing. 5379 User Account Management
감사 성공 2025-03-12 오후 11:36:54 Microsoft Windows security auditing. 5379 User Account Management
감사 성공 2025-03-12 오후 11:36:54 Microsoft Windows security auditing. 5379 User Account Management
감사 성공 2025-03-12 오후 11:36:54 Microsoft Windows security auditing. 5379 User Account Management
감사 성공 2025-03-12 오후 11:36:54 Microsoft Windows security auditing. 5379 User Account Management
감사 성공 2025-03-12 오후 11:34:38 Microsoft Windows security auditing. 4672 Special Logon
이벤트 5379, Microsoft Windows security auditing.
일반 자세히
자격 증명 관리자 자격 증명을 읽었습니다.
주체:
보안 ID: DESKTOP-ADTHB67₩hong5
계정 이름: hong5
계정 도메인: DESKTOP-ADTHB67
로그온 ID: 0x2C916FA9
읽기 작업: 자격 증명 열거
이 이벤트는 사용자가 자격 증명 관리자에서 저장된 자격 증명에 대해 읽기 작업을 수행할 때 발생합니다.
로그 이름(M): 보안
원본(S): Microsoft Windows security
로그된 날짜(D): 2025-03-12 오후 11:36:55
이벤트 ID(E): 5379
작업 범주(Y): User Account Management
수준(L): 정보
키워드(K): 감사 성공
사용자(U): 해당 없음
컴퓨터(R): DESKTOP-ADTHB67
Opcode(O): 정보
추가 정보(I): 이벤트 로그 도움말
작업
보안
저장된 로그 열기...
사용자 지정 보기 만들기...
보기 가져오기...
로그 지우기...
현재 로그 필터링...
속성
찾기...
다른 이름으로 모든 이벤트 저장...
이 로그에 작업 연결...
보기
새로 고침
도움말
이벤트 5379, Microsoft Windows security aud...
이벤트 속성
이 이벤트에 작업 연결...
복사
선택한 이벤트 저장...
새로 고침
도움말

로그 관리

- **리눅스의 로그 관리**
  - 로그
    - 리눅스에서는 /var/log 디렉터리에 로그가 존재



로그 관리

리눅스의 로그 관리

로그

- 리눅스에서는 /var/log 디렉터리에 로그가 존재
  - /var/log/syslog 혹은 messages
  - - 시스템 메시지와 로그 기록
  - (작동 상태, 어플리케이션 로그, 시스템 오류 등)

  - /var/log/auth.log 혹은 secure
  - - 인증과 관련된 로그 정보

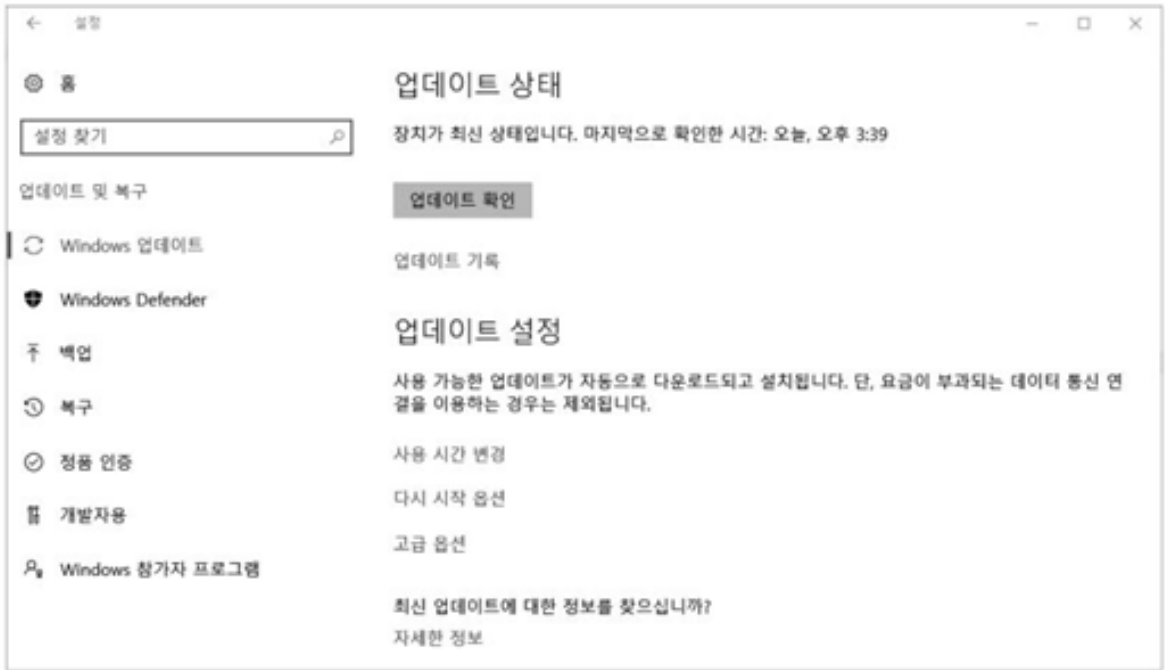
  - /var/log/boot.log
  - - 시스템 부팅 과정에서 발생하는 메시지 로그
  - (부팅 문제 진단 할 수 있음)

  - /var/log/dmesg
  - - 커널에서 발생하는 메시지, 시스템 부팅시 초기 하드웨어 감지 등의 메시지

  - /var/log/apache/access.log
  - - 웹 서버 과년 로그

취약점 관리

- **패치 관리**
  - 응용 프로그램을 만든 제작사가 배포하는 패치 또는 서비스 팩을 적용해 시스템 자체의 취약점을 보완
  - 유닉스/리눅스 시스템에도 내재된 취약점이 있지만 윈도우는 사용률이 훨씬 높고 접근하기도 쉬워 공격을 더 많이 받음
  - 윈도우 업데이트를 통해 자동으로 보안 패치를 확인하고 적용할 수 있음



모바일 보안

모바일 보안

모바일 운영체제의 역사

- 팜 OS
  - 1996년에 개발된 운영체제로 주소, 달력, 메모장, 할 일 목록, 계산기와 개인 정보를 숨기기 위한 간단한 보안 툴이 포함
- 윈도우 CE
  - PDA나 모바일 장치 등에 사용하기 위해 만든 운영체제로 1MB 이하의 메모리에 서도 동작이 가능하도록 설계
  - 1996년에 초기 버전인 윈도우 CE 1.0이 출시
- 블랙베리 OS
  - RIM이 만든 모바일 운영체제로 메시지와 이메일 전송 기능 및 보안에 초점을 두고 있음
  - 2000년에 블랙베리 5790 모델에 처음으로 블랙베리라는 명칭이 사용
- iOS
  - 애플의 아이폰과 아이패드에 사용되는 모바일 운영체제
  - 2007년 출시된 아이폰 오리지널의 운영체제를 시작으로 계속 업데이트 됨
- 안드로이드

모바일 보안

모바일 보안

모바일 운영체제의 역사

- 팜 OS
  - 1996년에 개발된 운영체제로 주소, 달력, 메모장, 할 일 목록, 계산기와 개인 정보를 숨기기 위한 간단한 보안 툴이 포함
- 윈도우 CE
  - PDA나 모바일 장치 등에 사용하기 위해 만든 운영체제로 1MB 이하의 메모리에 서도 동작이 가능하도록 설계
  - 1996년에 초기 버전인 윈도우 CE 1.0이 출시
- 블랙베리 OS
  - RIM이 만든 모바일 운영체제로 메시지와 이메일 전송 기능 및 보안에 초점을 두고 있음
  - 2000년에 블랙베리 5790 모델에 처음으로 블랙베리라는 명칭이 사용

모바일 보안

모바일 보안

모바일 운영체제의 역사

- 2007년 아이폰의 첫 번째 버전인 아이폰 오리지널의 운영체제는 맥북의 운영체제를 모바일로 바꾼 OS X
- 2008년 3월 6일 아이폰 SDK의 첫 베타 버전이 배포
- SDK 발표 이후에 iPhone OS로 명명되었다가 2010년 6월 iOS4 발표와 함께 iOS로 변경
- 안드로이드 1.1 버전은 아이폰 오리지널을 딴 코드네임을 가진 최초의 버전
- 구글은 2009년 4월을 기점으로 이후에 출시한 안드로이드 버전에 디저트 이름을 붙여서 공개

(a) 팜 OS 1.0이 탑재된 팜 파일럿 5000 (b) 윈도우 CE 1.0이 탑재된 카시오 A-11 (c) 초기의 블랙베리 5790

(d) 아이폰 오리지널 (e) HTC Dream(T-Mobile G1)

그림 2-36 다양한 운영체제를 탑재한 모바일 기기

그림 2-37 iOS와 안드로이드

모바일 보안

iOS의 취약점

- iOS는 외부 해커가 iOS에 접근할 수 있는 방법이 무척 제한적
- iOS의 보안상 문제점은 대부분 탈옥을 한 iOS 기기에서 발생
- 탈옥한 iOS 기기로는 iOS의 시스템 파일에 접근할 수 있음
- 사용자가 iOS를 탈옥할 때 반드시 적용해야 할 보안 사항은 일반 PC와 마찬가지로 기본 패스워드를 변경해야 함

(a) 탈옥한 iOS로 내부 시스템 파일에 접근

(b) 탈옥한 iOS로 SSH 서버 실행

그림 2-39 탈옥한 iOS의 활용 예

모바일 보안

안드로이드의 보안 체계

- 안드로이드는 리눅스 커널(2.6.25)을 기반으로 하는 모바일 운영체제
- 구글은 애플의 폐쇄적인 정책과 달리 공개적인 프로그램 개발을 추구

그림 2-40 안드로이드 운영체제의 구조

모바일 보안

- **안드로이드의 취약점**
  - 안드로이드는 사용자가 보안 수준을 선택할 수 있다는 점에서 iOS보다 훨씬 자유로운 운영체제
  - 앱 마켓도 다양하기 때문에 각종 바이러스와 악성 코드가 유포되며 그에 따른 백신도 보급
  - 안드로이드는 자유로운 개발과 변경이 가능한 반면 iOS에 비해 상대적으로 보안이 취약
  - iOS의 탈옥과 비슷한 개념으로 안드로이드에서는 루팅을 할 수 있음

Thank you for Listening

새로운 세상과 변화에 도전하는 동국대인이 되기를 바랍니다.