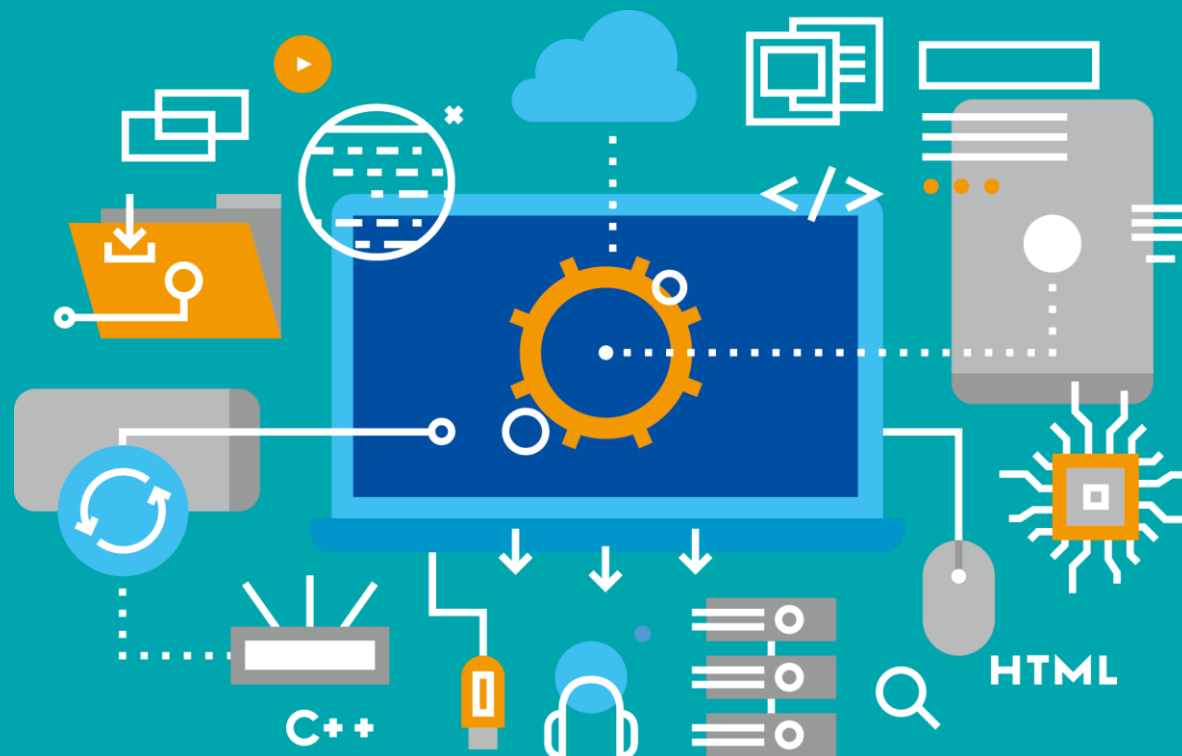


DMMU

동양미래대학교 전문기술 석사과정

클라우드와 네트워크 보안

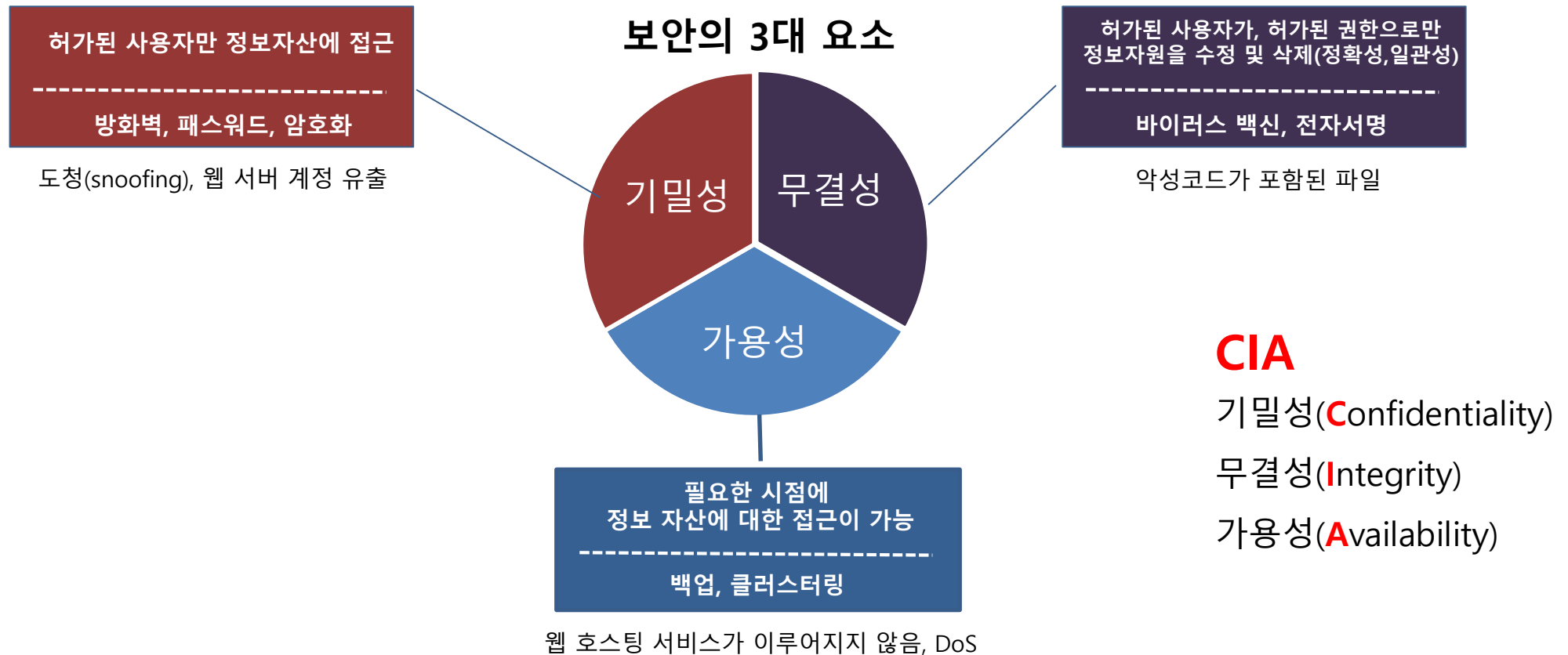
Dongyang Mirae University



- 보안의 개념과 정의
- 시스템 보안
- 네트워크 보안
- 암호화

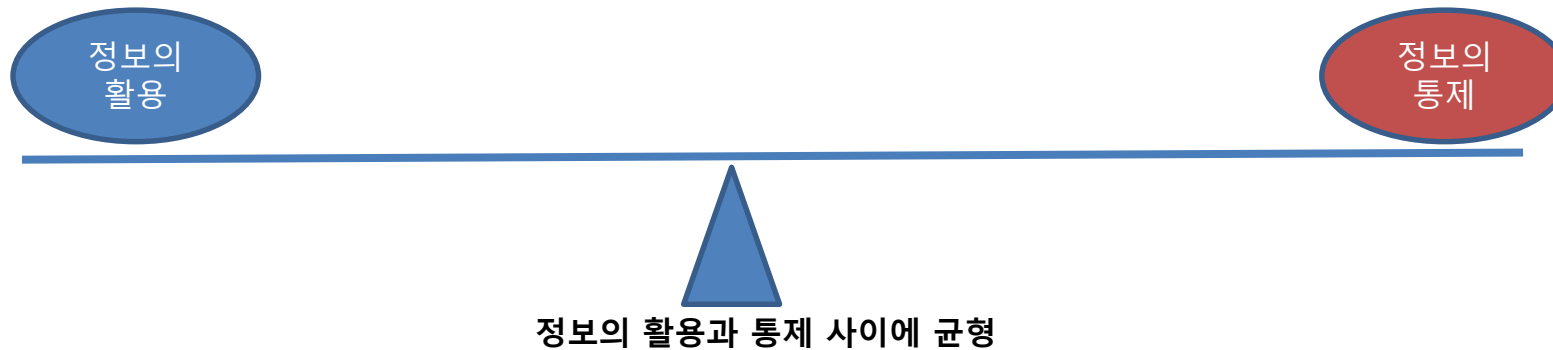
보안의 개념과 정의

1. 정보 보안의 정의



정보보안 – 정보자산(데이터, 시스템)을 내부, 외부의 위협으로 부터 **기밀성, 무결성, 가용성**을 확보하는 것

정보보호의 목표



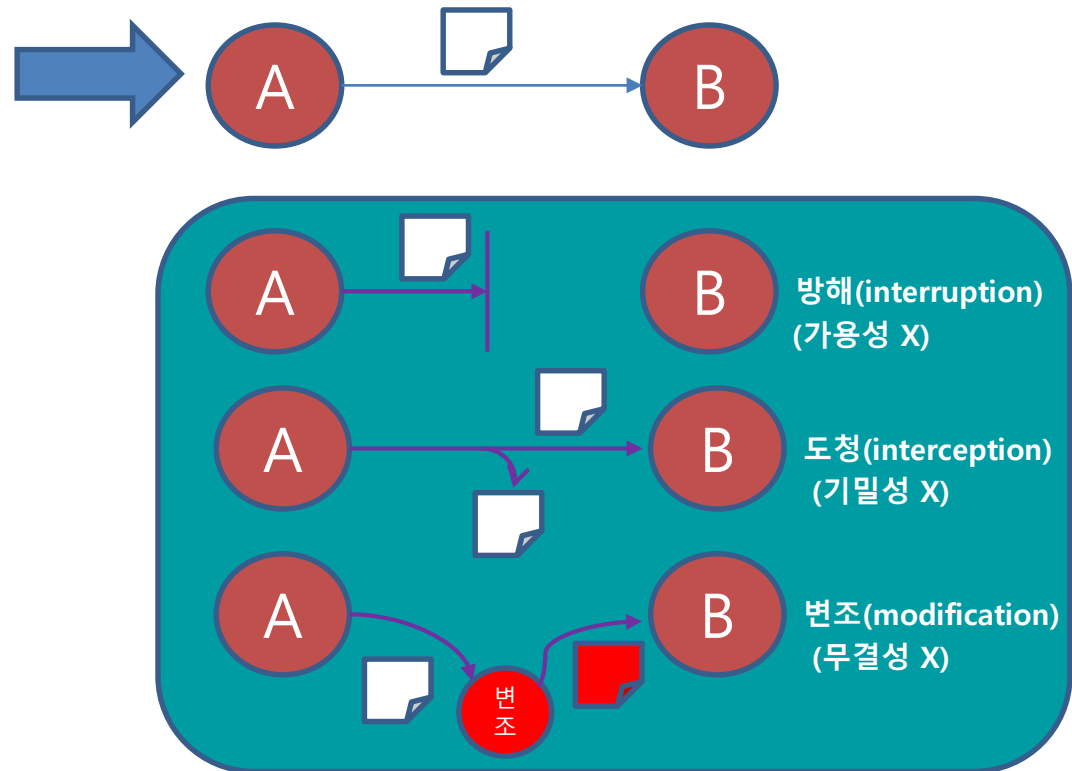
정보의
활용

정보가 필요한 사람이 쉽게 정보를 얻을 수 있도록 가용성을 극대화

정보의
통제

정보에 위협이 되는 위협요소를 줄여 안정성을 확보

해킹 해커들이 수행하는 모든 불법적인 행위



시스템 보안

권한이 없는 사용자가 파일이나 폴더, 장치 등을 사용하지 못하도록 제한하여 시스템을 보호하는 기능

계정
관리

세션
관리

접근
제어

권한
관리

로그
관리

취약점
관리

시스템 보안

권한이 없는 사용자가 파일이나 폴더, 장치 등을 사용하지 못하도록 제한하여 시스템을 보호하는 기능

시스템 보안 관리	보안 관리 내용
계정관리	아이디와 패스워드를 이용한 사용자 인증 / 사용자 아이디 패스워드 관리
세션관리	사용자와 시스템, 시스템과 시스템 사이의 활성화된 접속 / 화면보호기, 인터넷 뱅킹-지속적 암호 인증
접근제어	네트워크 안에서 다른 시스템을 보호할 수 있도록 네트워크 관점에서 접근 통제 / 특정 포트를 통해 서비스 접근
권한 관리	사용자가 적절한 권한으로 정보자산에 접근 통제 / ls -l
로그 관리	시스템 내부나 네트워크를 통한 외부 접근에 대해 활동 내용을 기록
취약점 관리	계정관리, 세션관리, 접근제어, 권한관리를 잘 하여도 시스템 자체 결함에 의한 보안 문제 발생 / 윈도우 업데이트, 패치

계정
관리

Top 25 most common passwords by year according to SplashData

Rank	2011 ^[4]	2012 ^[5]	2013 ^[6]	2014 ^[7]	2015 ^[8]	2016 ^[3]	2017 ^[9]	2018 ^[10]	2019 ^[11]
1	password	password	123456	123456	123456	123456	123456	123456	123456
2	123456	123456	password	password	password	password	password	password	123456789
3	12345678	12345678	12345678	12345	12345678	12345	12345678	123456789	qwerty
4	qwerty	abc123	qwerty	12345678	qwerty	12345678	qwerty	12345678	password
5	abc123	qwerty	abc123	qwerty	12345	football	12345	12345	1234567
6	monkey	monkey	123456789	123456789	123456789	qwerty	123456789	111111	12345678
7	1234567	letmein	111111	1234	football	1234567890	letmein	1234567	12345
8	letmein	dragon	1234567	baseball	1234	1234567	1234567	sunshine	iloveyou
9	trustno1	111111	iloveyou	dragon	1234567	princess	football	qwerty	111111
10	dragon	baseball	adobe123 ^[a]	football	baseball	1234	iloveyou	iloveyou	123123
11	baseball	iloveyou	123123	1234567	welcome	login	admin	princess	abc123
12	111111	trustno1	admin	monkey	1234567890	welcome	welcome	admin	qwerty123
13	iloveyou	1234567	1234567890	letmein	abc123	solo	monkey	welcome	1q2w3e4r
14	master	sunshine	letmein	abc123	111111	abc123	login	666666	admin
15	sunshine	master	photoshop ^[a]	111111	1qaz2wsx	admin	abc123	abc123	qwertyuiop
16	ashley	123123	1234	mustang	dragon	121212	starwars	football	654321
17	bailey	welcome	monkey	access	master	flower	123123	123123	555555
18	passw0rd	shadow	shadow	shadow	monkey	passw0rd	dragon	monkey	lovely
19	shadow	ashley	sunshine	master	letmein	dragon	passw0rd	654321	7777777
20	123123	football	12345	michael	login	sunshine	master	!@#%&^*	welcome
21	654321	jesus	password1	superman	princess	master	hello	charlie	888888

계정
관리

<https://www.security.org/how-secure-is-my-password/>

The screenshot shows the homepage of security.org. At the top, there is a navigation bar with links: Home Security, Smart Home, Digital Security, About Us, and What's My Security Score?. Below the navigation bar is a sponsored advertisement for KEEPER, featuring the text "Your passwords will always be secure with Keeper." and a "Start Free Trial" button. The main heading is "How Secure Is My Password?". Below the heading is a subheading: "The #1 Password Strength Tool. Trusted and used by millions." There is a password input field with a blue arrow on the left and a series of dots representing the password. Below the input field, the text reads: "It would take a computer about 5 seconds to crack your password". At the bottom, there is a blue button labeled "Tweet Your Result".

계정
관리

<https://www.security.org/how-secure-is-my-password/>

dongyang

How Secure Is My Password?

● The #1 Password Strength Tool. Trusted and used by millions.

.....

It would take a computer about

5 seconds

to crack your password

dongyang1234

How Secure Is My Password?

● The #1 Password Strength Tool. Trusted and used by millions.

.....

It would take a computer about

3 years

to crack your password

Dongyang1234!

How Secure Is My Password?

● The #1 Password Strength Tool. Trusted and used by millions.

.....

It would take a computer about

12 thousand years

to crack your password

계정 관리

계정 관리 : /etc/passwd

```
[root@localhost etc]# pwd
/etc
[root@localhost etc]# cat passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
systemd-network:x:192:192:systemd Network Management:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
polkitd:x:999:998:User for polkitd:/:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
postfix:x:89:89:/:/var/spool/postfix:/sbin/nologin
chrony:x:998:996:/:/var/lib/chrony:/sbin/nologin
[root@localhost etc]#
[root@localhost etc]# ls -l passwd
-rw-r--r--. 1 root root 846 Jul 9 17:05 passwd
[root@localhost etc]#
```

로그인 아이디	User no	User name	사용자 기본 .shell
root	x : 0 : 0	root	/root : /bin/bsh
암호	Group no	Home directory	

- 암호 : 암호화되어 저장되며, 'x'는 암호가 shadow 파일에 저장되어 있음
 - 최근 시스템은 암호가 없으면 계정 비 활성화
- User name : 사용자 실제 이름을 비롯한 라벨 역할을 하는 이름
- 사용자 shell : /binsh, /bin/csh, /bin/bash, /bin/ksh

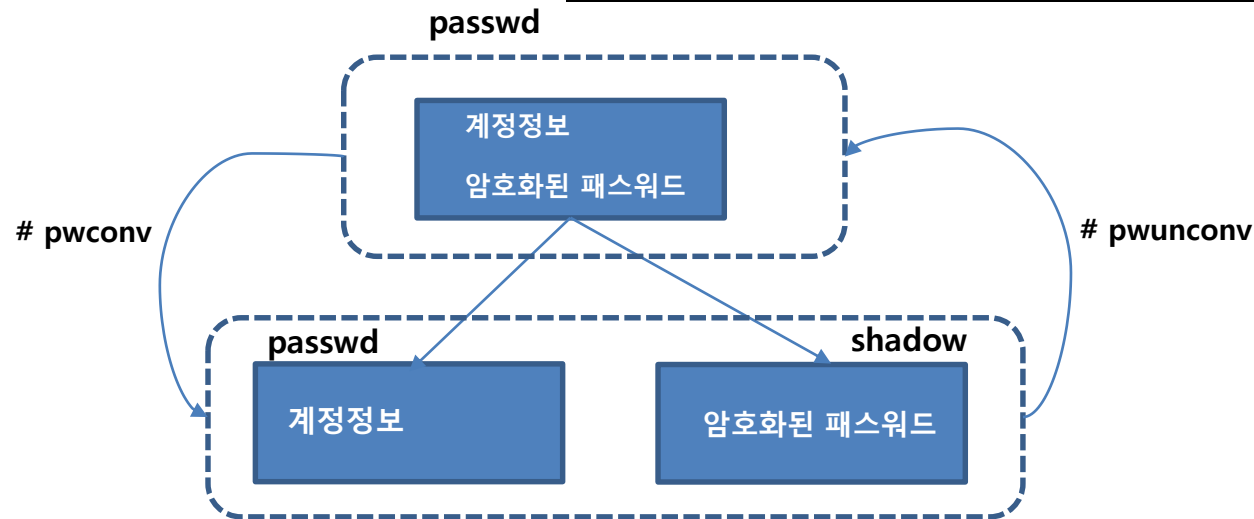
```
- rw-r--r--. root root 846 Jul 9 17:05 passwd
```

- rw- : 소유자의 권한
- r-- : 그룹의 권한
- r-- : 그 외 사용자의 권한

계정
관리

패스워드 파일 보호

```
[root@localhost etc]# pwd
/etc
[root@localhost etc]# pwunconv
[root@localhost etc]# cat passwd
root:$6$Baw0Au3uukZwWlPK$Rj/hc4Q5BU.XHs5/2P44Xu6uUuWPaTtBqrEq12kyZtdusxPMbgpMw9zu7y/oK/5/ppGiBuC1UK6UHHEmFQvyF/:0:0:root:/root:/
bin/bash
```



```
- rw-r--r--. root root 846 Jul 9 17:05 passwd
-r-----. 1 root root 846 Jul 9 17:05 shadow
```

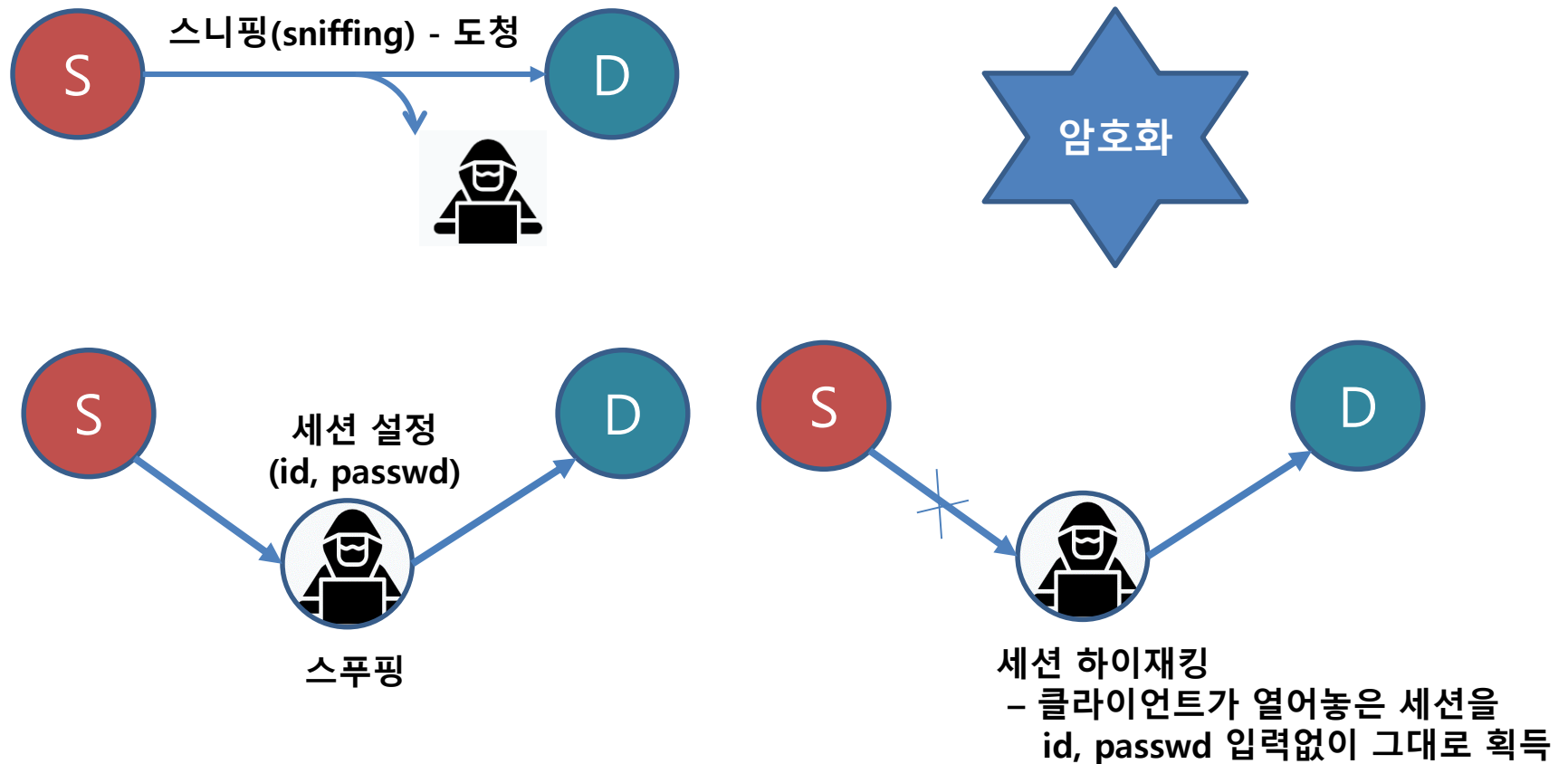
Root계만 읽기 가능

```
[root@localhost etc]# pwconv
[root@localhost etc]# cat passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
```

세션
관리

세션 : 사용자와 시스템 사이 또는 두 시스템 사이의 활성화된 접속

- 암호화 (세션하이재킹, 스니핑), 지속적 인증(윈도우 화면보호기, 인터넷뱅킹)






세션 관리

세션 : 사용자와 시스템 사이 또는 두 시스템 사이의 활성화된 접속

- 암호화 (세션하이제킹, 스니핑), 지속적 인증(윈도우 화면보호기, 인터넷뱅킹)

지속적 인증

- 시스템에 접근하는 사용자가 처음 인증에 성공한 사용자인지를 재 확인
- 세션 timeout 설정
- 윈도우 화면보호기 + 다시 시작할 때 로그인 화면 표시



지속적
인증

접근 제어

적절한 권한을 가진 인가자만 특정 시스템이나 정보에 접근할 수 있도록 통제

- 시스템 및 네트워크에 대한 기본적인 통제 수단 : IP와 Port

특정 포트를 통해서만 시스템의 서비스에 접근 가능하도록 관리

- 불필요한 서비스(포트)를 제거 : 해당 포트를 통해 공격 가능

운영체제 접근제어

서비스 이름	사용 포트	특징
ftp	21	파일 송수신
ssh	22	Secure Shell
telnet	23	암호화되지 않음
SENDMAIL	25	E-mail
http / https	80 / 443	Web server

• 포트는 2Byte (16 bit)크기로 1 – 65535 ($2^{16} - 1$)의 값을 갖는다.

✓ Well-known port : 1 – 1023

✓ Registered Port : 1024-49151

✓ Dynamic Port : 49152-65535

• 참조사이트 <http://www.iana.org/assignments/port-numbers>

✓ 1주일 간격으로 최신버전으로 업데이트

• Windows : %WINDIR%\system32\drivers\etc\services 파일에 포트번호 지정됨

• Linux : /etc/services 파일에 포트번호 지정됨

• 현재 연결되어 사용중인 포트 확인 : netstat -an

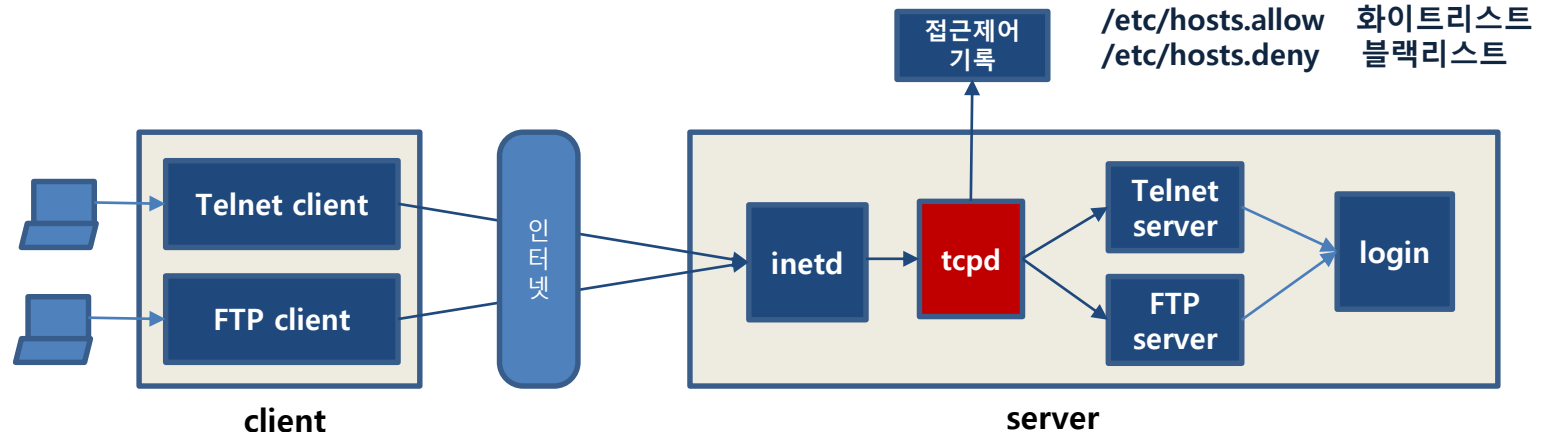
접근 제어

적절한 권한을 가진 인가자만 특정 시스템이나 정보에 접근할 수 있도록 통제

- 시스템 및 네트워크에 대한 기본적인 통제 수단 : IP와 Port

IP를 통한 시스템 접근 제어 정책 (리눅스)

- TCPWrapper : 발신 IP에 대해 해당 Port의 서비스 요청을 허가할 것인지를 결정



- inetd : inetd가 관리하는 서버(telnet, ssh, FTP 등)에 대한 서비스 요청을 받는다.
- inetd는 클라이언트 연결 요청을 TCPwrapper의 tcpd로 넘겨준다.
- tcpd는 클라이언트에 적절한 접근권한이 있는지 접근제어기록을 통해 확인
- 접근권한이 있을 경우만 해당 서버로 연결

접근 제어

적절한 권한을 가진 인가자만 특정 시스템이나 정보에 접근할 수 있도록 통제

- 시스템 및 네트워크에 대한 기본적인 통제 수단 : IP와 Port

/etc/hosts.allow 허용할 서비스에 대한 요청 IP 주소

/etc/hosts.deny 차단할 요청 IP 주소



처음에는 모두 비어 있음 - 모두 허용

- ① 발신 IP가 allow에 있으면 접근허용
- ② 발신 IP가 deny에 있으면 접근 차단
- ③ 나머지는 접근 허용

```
centos7 vm-1 [실행 중] - Oracle VM VirtualBox
파일  머신  보기  입력  장치  도움말
[sy.jung@localhost ~]$ cat /etc/hosts.allow
#
# hosts.allow  This file contains access rules which are used to
#              allow or deny connections to network services that
#              either use the tcp_wrappers library or that have been
#              started through a tcp_wrappers-enabled xinetd.
#
#              See 'man 5 hosts_options' and 'man 5 hosts_access'
#              for information on rule syntax.
#              See 'man tcpd' for information on tcp_wrappers
#
[sy.jung@localhost ~]$
```

```
centos7 vm-1 [실행 중] - Oracle VM VirtualBox
파일  머신  보기  입력  장치  도움말
[sy.jung@localhost ~]$ cat /etc/hosts.deny
#
# hosts.deny  This file contains access rules which are used to
#             deny connections to network services that either use
#             the tcp_wrappers library or that have been
#             started through a tcp_wrappers-enabled xinetd.
#
#             The rules in this file can also be set up in
#             /etc/hosts.allow with a 'deny' option instead.
#
#             See 'man 5 hosts_options' and 'man 5 hosts_access'
#             for information on rule syntax.
#             See 'man tcpd' for information on tcp_wrappers
#
[sy.jung@localhost ~]$
```

접근
제어

적절한 권한을 가진 인가자만 특정 시스템이나 정보에 접근할 수 있도록 통제

- 시스템 및 네트워크에 대한 기본적인 통제 수단 : IP와 Port

/etc/hosts.allow 허용할 서비스에 대한 요청 IP 주소

/etc/hosts.deny 차단할 요청 IP 주소



/etc/hosts.allow	/etc/hosts.deny	접근제어
ALL: 10.0.2.7	ALL: ALL	10.0.2.7만 접근 허용
sshd: 10.0.2.7 sshd: 203.123.2.	sshd: ALL	sshd 서버 접근은 10.0.2.7과 203.123.2.xxx에 대해 허용하고 나 머지는 접근 불가
sshd: 10.0.2.7, 203.123.2.	sshd: ALL	

권한
관리

운영체제의 파일과 디렉터리에 대한 접근 관리

- 파일과 디렉터리에 대해 그룹이나 개별 사용자의 접근권한을 설정

(Linux) 권한관리

```
[sy.jung@localhost ~]$ ls -l  
total 4  
-rw-rw-r--. 1 sy.jung sy.jung 20 Aug 14 14:16 test.c
```

파일의 종류 : - 일반파일, d 디렉터리, l 링크

파일/디렉터리 소유자 권한

파일/디렉터리 소유자 권한

제3의 사용자 권한

-rw-rw-r-x. 1 sy.jung sy.jung 20 Aug 14 14:16 test.c

파일의 종류와 권한

파일의 소유자

파일의 그룹

로그
관리

시스템에 로그인 및 객체나 파일에 대한 접근 기록

- 해커나 악의적 사용자에 대한 추적

AAA (Authentication, Authorization, and Accounting)

- 사용자가 컴퓨터 자원을 사용하기 위해 시스템에 접속할 때 사용자 행위를 추적하기 위해 수행하는 작업
- Authentication(인증) : 등록된 사용자 여부를 아이디와 패스워드로 확인하는 과정
- Authorization(인가) : 로그인 후, 사용자에게 권한(범위)을 부여하는 과정 (일반사용자, 관리자, ...)
- Accounting(어카운팅) : 자원에 대한 접근 기록 및 통계 (과금, 악의적 사용자 추적, 트렌드 분석, 용량 설계, ...)



AAA 정보는 로그가 수행되는 대상으로 어떤 정보를 로그로 남길지를 정책 결정

- (예) 인증에 실패한 내용에 대해 로그를 남긴다.

로그
관리

시스템에 로그인 및 객체나 파일에 대한 접근 기록
- 해커나 악의적 사용자에 대한 추적

AAA (Authentication, Authorization, and Accounting)

Authentication(인증)

: syjung은 등록된 사용자임을 증명

username : syjung
Password : *****

Accounting(어카운팅) :

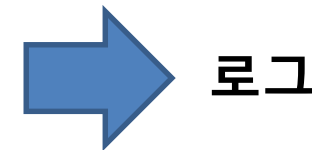
syjung의 활동 기록

syjung이 시스템에서 수행하는
활동 기록
: 읽은 파일, 머문 시간 등

syjung이 접근할 수 있는 자원

Authorization(인가) :

syjung에게 자원에 대한 접근 권한 부여



로그

윈도우

이벤트라 불리는 중앙 집중화된 형태로
로그 수집 저장

리눅스

로그를 여러 파일에 분산하여 저장
보안에 유리

로그
관리

시스템에 로그인 및 객체나 파일에 대한 접근 기록

- 해커나 악의적 사용자에 대한 추적

리눅스 로그 관리

일반적으로 /var/log 디렉터리를 비롯하여 /run 등 여러 곳에 로그가 존재

```
[root@localhost ~]# ls /var/log
anaconda      cron-20200816      maillog      messages-20200906  spooler-20200823  vmware-network.5.log
audit         cron-20200823      maillog-20200816  rhsm              spooler-20200830  vmware-network.6.log
boot.log      cron-20200830      maillog-20200823  secure           spooler-20200906  vmware-network.7.log
boot.log-20200710 cron-20200906      maillog-20200830  secure-20200816  tallylog          vmware-network.log
boot.log-20200718 dmesg             maillog-20200906  secure-20200823  tuned            vmware-vgauthsvc.log.0
btmp         dmesg.old         messages         secure-20200830  vmware-network.1.log vmware-vmtoolsd.log
btmp-20200901 firewallld        messages-20200816  secure-20200906  vmware-network.2.log wtmp
chrony       grubby_prune_debug messages-20200823  spooler          vmware-network.3.log yum.log
cron         lastlog           messages-20200830  spooler-20200816  vmware-network.4.log
[root@localhost ~]# _
```

```
[root@localhost run]# ls /run
auditd.pid  cron.reboot  dmeventd-server  initramfs  lvmlog.pid  plymouth  sudo  tuned  vmware
chrony      cryptsetup   ebttables.lock  lock       mount       sepermit  syslogd.pid  udev  xtables.lock
console     dbus        faillock        log        netreport  setrans   systemd      user
crond.pid   dmeventd-client firewallld      lvm        NetworkManager  sshd.pid  tmpfiles.d  utmp
[root@localhost run]# _
```

로그
관리

시스템에 로그인 및 객체나 파일에 대한 접근 기록

- 해커나 악의적 사용자에게 대한 추적

리눅스 로그 관리 - 로그를 확인하는 다양한 명령

```
[root@localhost log]# w
14:03:08 up 53 days, 20:32,  1 user,  load average: 0.00, 0.01, 0.05
USER    TTY      FROM          LOGIN@   IDLE   JCPU   PCPU WHAT
root    tty1          13:54      4.00s   0.06s   0.00s w
[root@localhost log]# _
```

\$ w

- 로그인 계정 이름, 로그인 디바이스, 로그인 시간 등 확인 가능
- /run/utmp에 바이어리로 저장된 로그의 내용 확인

```
[root@localhost ~]# last
root      tty1          Wed Sep  9 14:15   still logged in
reboot    system boot    3.10.0-1062.el7. Wed Sep  9 14:13 - 14:15   (00:02)
root      tty1          Wed Sep  9 14:10 - 14:10   (00:00)
root      tty1          Wed Sep  9 14:06 - 14:09   (00:03)
root      tty1          Wed Sep  9 13:54 - 14:04   (00:10)
syjung    tty1          Fri Aug 14 14:15 - 14:18   (00:02)
syjung    tty1          Fri Aug 14 13:29 - 13:46   (00:16)
syjung    tty1          Tue Jul 28 14:05 - 14:08   (00:03)
syjung    tty1          Tue Jul 28 14:02 - 14:04   (00:01)
root      tty1          Fri Jul 17 17:30 - 14:01   (10+20:31)
reboot    system boot    3.10.0-1062.el7. Fri Jul 17 17:30 - 14:13   (53+20:43)
root      tty1          Thu Jul  9 17:11 - 17:30   (8+00:18)
reboot    system boot    3.10.0-1062.el7. Thu Jul  9 17:11 - 17:30   (8+00:19)
root      tty1          Thu Jul  9 17:10 - 17:10   (00:00)
reboot    system boot    3.10.0-1062.el7. Thu Jul  9 17:10 - 17:10   (00:00)
root      tty1          Thu Jul  9 17:09 - 17:09   (00:00)
reboot    system boot    3.10.0-1062.el7. Thu Jul  9 17:07 - 17:10   (00:02)

wtmp begins Thu Jul  9 17:07:57 2020
[root@localhost ~]# _
```

\$ last

- 사용자들의 로그인과 로그아웃, 시스템 부팅 정보를 확인 가능
- /var/log/wtmp에 바이어리로 저장된 로그의 내용 확인

로그
관리

시스템에 로그인 및 객체나 파일에 대한 접근 기록

- 해커나 악의적 사용자에 대한 추적

리눅스 로그 관리 - 로그를 확인하는 다양한 명령

```
Sep 9 14:13:41 localhost kernel: vgaarb: device added: PCI:0000:00:0f.0,decodes=io+mem,owns=io+mem,locks=none
Sep 9 14:13:41 localhost kernel: vgaarb: loaded
Sep 9 14:13:41 localhost kernel: vgaarb: bridge control possible 0000:00:0f.0
Sep 9 14:13:41 localhost kernel: SCSI subsystem initialized
Sep 9 14:13:41 localhost kernel: ACPI: bus type USB registered
Sep 9 14:13:41 localhost kernel: usbcore: registered new interface driver usbfs
Sep 9 14:13:41 localhost kernel: usbcore: registered new interface driver hub
Sep 9 14:13:41 localhost kernel: usbcore: registered new device driver usb
Sep 9 14:13:41 localhost kernel: EDAC MC: Ver: 3.0.0
Sep 9 14:13:41 localhost kernel: Registered efivars operations
Sep 9 14:13:41 localhost kernel: PCI: Using ACPI for IRQ routing
Sep 9 14:13:41 localhost kernel: NetLabel: Initializing
Sep 9 14:13:41 localhost kernel: NetLabel: domain hash size = 128
Sep 9 14:13:41 localhost kernel: NetLabel: protocols = UNLABELED CIPSOv4
Sep 9 14:13:41 localhost kernel: NetLabel: unlabeled traffic allowed by default
Sep 9 14:13:41 localhost kernel: hpet0: at MMIO 0xfed00000, IRQs 2, 8, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0
Sep 9 14:13:41 localhost kernel: hpet0: 16 comparators, 64-bit 14.318180 MHz counter
```

\$ more /var/log/messages

- 하드웨어 구동, 서버의 동작, 에러 등 다양한 정보를 로깅

취약점 관리

기능명세, 설계, 구현 단계의 오류나 설치나 운영 상의 문제점으로 시스템이 지니는 보안상 약점

- 보안상 구멍

취약점 제공자

소프트웨어

- 보안 코딩이 되지 않은 소프트웨어
- 보안 패치가 제공되지 않은 소프트웨어

사용자

- 암호 공유 및 쉬운 암호 사용
- 보안 정책 무시 (패치 설치 무시)
- 악의적 코드가 담긴 메일 열람, 소프트웨어 다운로드, 웹 사이트 방문

네트워크 관리

- 잘못된 서비스 설정
- 보안 정책 무시 (패치 설치 무시)

Zero-Day Attack

- 보안 patch가 나오기 전 취약점 공격 발생
- 무방비 상태에서 공격 당함
- 알려지지 않은 취약점

cve.mitre.org

- CVE(Common Vulnerabilities and Exposure)는 공개적으로 알려진 소프트웨어의 보안 취약점을 가리키는 고유 표기
- 이전에는 각 기관이나 업체마다 각자의 보안취약점을 가리키는 이름을 붙여 사용했으나 서로 체계가 다르다 보니 일관성이 없어 혼란스럽고 비효율적
- 미국 비영리 회사인 MITRE사에서 1999년 처음 만들어 후, 미국 국립표준기술연구소(NIST)가 국가 취약성 데이터베이스(NVD)를 만들어 협력체계를 구축하면서 체계화

CVE-YYYY-NNNN...N

4-digit minimum and no maximum, provides for additional capacity each year when needed.

CVE-2014-0001

CVE-2014-12345

CVE-2014-7654321

사이버공격 실황 중계



real time attack

전체 동영상 이미지 뉴스 쇼핑 더보기 설정 도구

검색결과 약 919,000,000개 (0.35초)

en.wiktionary.org > wiki > real-tim... > 이 페이지 번역하기

[real-time attack - Wiktionary](#)

NounEdit · (video games, speedrunning) A non-tool-assisted speedrun of a game that is timed using a separate timer from that of any in-game timer. · (video games, ...

threatmap.checkpoint.com > 이 페이지 번역하기

[Live Cyber Threat Map | Check Point](#)

LIVE CYBER THREAT MAP. 24,471,039 **ATTACKS** ON THIS DAY
US, United States Thailand. malware. CiscoTalos.TC...
Zero-Day Protection ThreatCloud Managed ... Live Cyber Threat Map | C

www.fireeye.com > cyber-map > th... > 이 페이지 번역하기

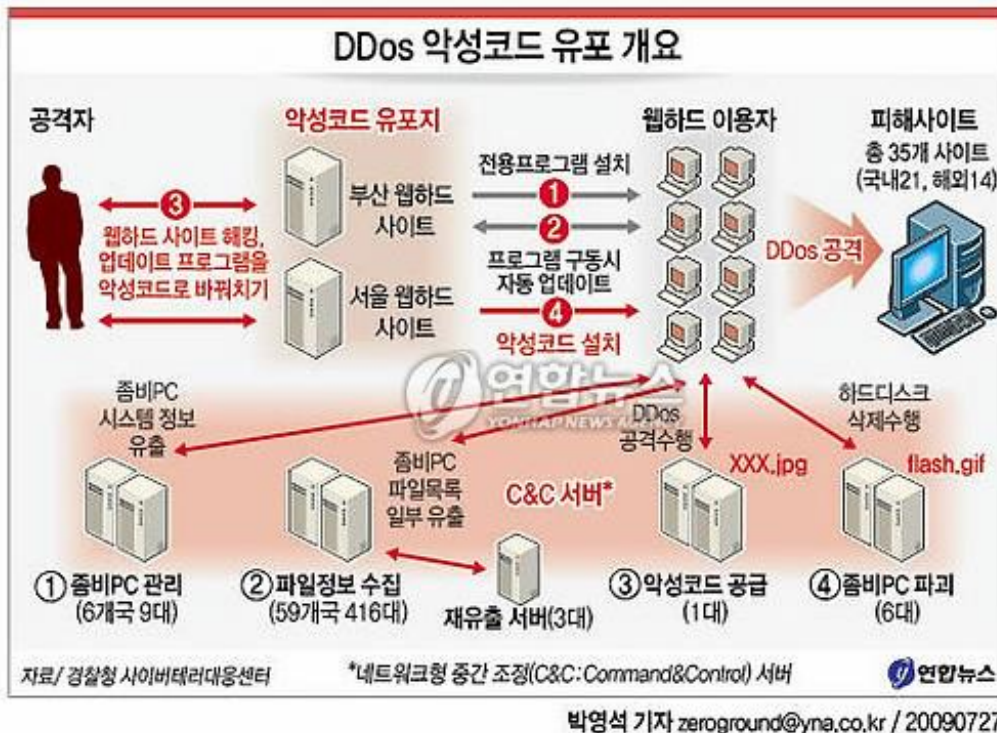
[FireEye Cyber Threat Map](#)

The "FireEye Cyber Threat Map" is based on a subset of **real attack** data, with a better visual presentation. Customer information has been ...



77 DDoS 대란 (2009.7.7)

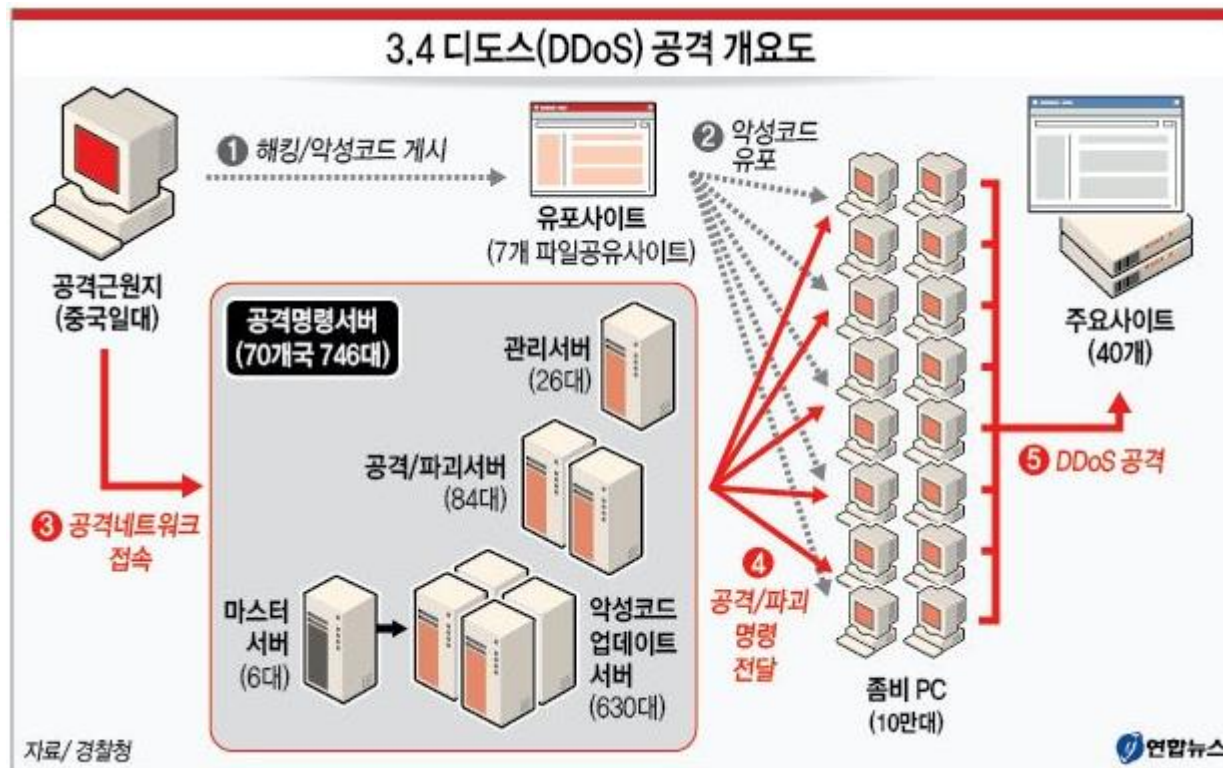
연일 뉴스 헤드라인을 장식하며 전 국민에게 DDoS(Distributed Denial of Service)라는 용어를 각인 시켜준 사건으로, 7월 7일부터 10일까지 4일간에 걸쳐, 청와대를 비롯해 주요 정부기관 홈페이지와 대형 포털, 금융권, 쇼핑몰 등 국내의 주요 홈페이지들이 타깃이 돼 장애발생



구분	기간	주요 공격대상
1차 DDoS 공격	2009.7.5.~6	미국 21개 주요 정부기관, 금융, 인터넷사이트 등 대규모 공격 발생
2차 DDoS 공격	2009.7.7~8	국내 12개, 미국 14개 주요 정부기관, 금융, 인터넷사이트 등 대규모 공격 발생
3차 DDoS 공격	2009.7.8~9	국내 15개, 미국 1개 주요 정부기관, 금융, 인터넷사이트 등 대규모 공격 발생
4차 DDoS 공격	2009.7.9~10	국내 7개 주요 정부기관, 금융, 인터넷사이트 등 대규모 공격 발생

기관유형	공격 진행 시간 (7월 7일 18시 ~ 7월 10일 18시)		
	24시간	48시간	72시간
공공기관	국회, 한나라당, 외교통상부, 국가정보원, 행정안전부	청와대, 국방부, 한미연합사령부	-
언론	-	-	조선닷컴
기업	안철수연구소, 이스트소프트	다음, 파란	네이버, 옥션
은행	외환은행, 신한은행, 농협, 우리은행, 하나은행, 기업은행	국민은행	-

34 DDoS 대란 (2011.3.4)



7.7과 3.4의 차이점과 유사점

	2009년 7월 7일	2011년 3월 4일
공격 대상 (웹사이트)	청와대 등 국내 주요 사이트 23곳	청와대 등 정부 사이트, 네이버 등 국내 주요 국가 사이트 및 주한 미군 등 40곳
공격 지속 기간	7-9일 3일간 오후 6시에서 다음날 6시까지	4일 오전 10시, 오후 6시 30분에 시작, 공격종료 시점 불확실
손상 운영체제	닷넷 프레임워크 기반 윈도우 2000/XP/2003	모든 윈도우 운영체제
파일 구성	같은 파일 구성으로 여러 차례 공격	공격 때마다 파일 구성이 달라짐.
영향 변경	변경 없이 일관되게 진행.	대응에 따라 명령을 변경함.
치료 방해	없음	호스트 변조로 백신 업데이트 및 홈페이지 접근 방해
하드 디스크 및 파일 손상 시점	마지막 디도스 공격 날인 10일 자정 손상. 당시 백신을 설치하지 않은 PC는 시스템 날짜를 이전으로 바꿔야 했음.	시스템 날짜를 감염 시작 이전으로 바꾸거나, 감염 시각을 기록한 noise03.dat 파일을 삭제할 경우, 감염 후 7일, 4일 후로 계획했다가 5일 밤 9시경을 기해 즉시 손상되는 것으로 변경.
зом비 PC 수 (발통위 발표)	약 20만여 대	5만여 대
대응 방식	제대로 준비되지 않은 상태에서 대대적 혼란 야기	7.7 디도스 이후 기업/기관의 준비가 있었고, 보안 업체와 유관 기관과의 협조로 피해 최소화

자료 : 안철수연구소

NEWSIS

서비스 거부 공격 DoS : Denial of Service

공격 유형	공격 방법	비 고
취약점 공격형	<ul style="list-style-type: none"> - 보잉크(Boink), 봉크(Bonk), 티어 드롭(TearDrop) - 랜드 공격(Land attack) 	<p>오류 제어 로직을 악용하여 시스템 자원 고갈 (단편화 조작 공격)</p> <p>출발지와 목적지 주소를 동일하게</p>
자원 고갈 공격형	<ul style="list-style-type: none"> - 죽음의 핑 공격 (ping of death) - SYN 플러딩(SYN flooding) - HTTP GET 플러딩 - HTTP CC 공격 - 스머프 공격 - 슬로우 HTTP 헤더 DoS 공격 - 슬로 HTTP POST 공격 	<p>Ping이 사용하는 ICMP 패킷을 많이 보냄</p> <p>정상적인 접속을 위장하여 3way-handshake 완료하지 않은 대량 접속 시도</p> <p>특정 페이지를 HTTP GET 메서드로 무한히 실행</p> <p>HTTP 요청 응답에 캐시를 사용하지 않도록 요구하여 웹 서비스 부하 증가</p> <p>Direct broadcast를 이용한 공격</p> <p>HTTP 헤더 정보를 조작하여 연결을 오래 유지</p> <p>HTTP 헤더 정보를 조작하여 연결을 오래 유지</p>

서비스 거부 공격 DoS : Denial of Service

공격 유형	공격 방법	비 고
취약점 공격형	<ul style="list-style-type: none"> - 보잉크(Boink), 봉크(Bonk), 티어드롭(TearDrop) - 랜드 공격(Land attack) 	<p><u>오류제어 로직</u>을 악용하여 시스템 자원 고갈 (단편화 조작 공격)</p> <p>출발지와 목적지 주소를 동일하게</p>

신뢰성 있는 데이터 전송을 위한 오류제어 기능

- 패킷의 **순서**가 올바른지 확인 (Packet ordering)
- 중간에 손실된 패킷이 없는지 확인 (Packet loss)
- 손실된 패킷의 재전송 요구 (Packet re-send request)

보잉크(Boink), 봉크(Bonk), 티어드롭(TearDrop)

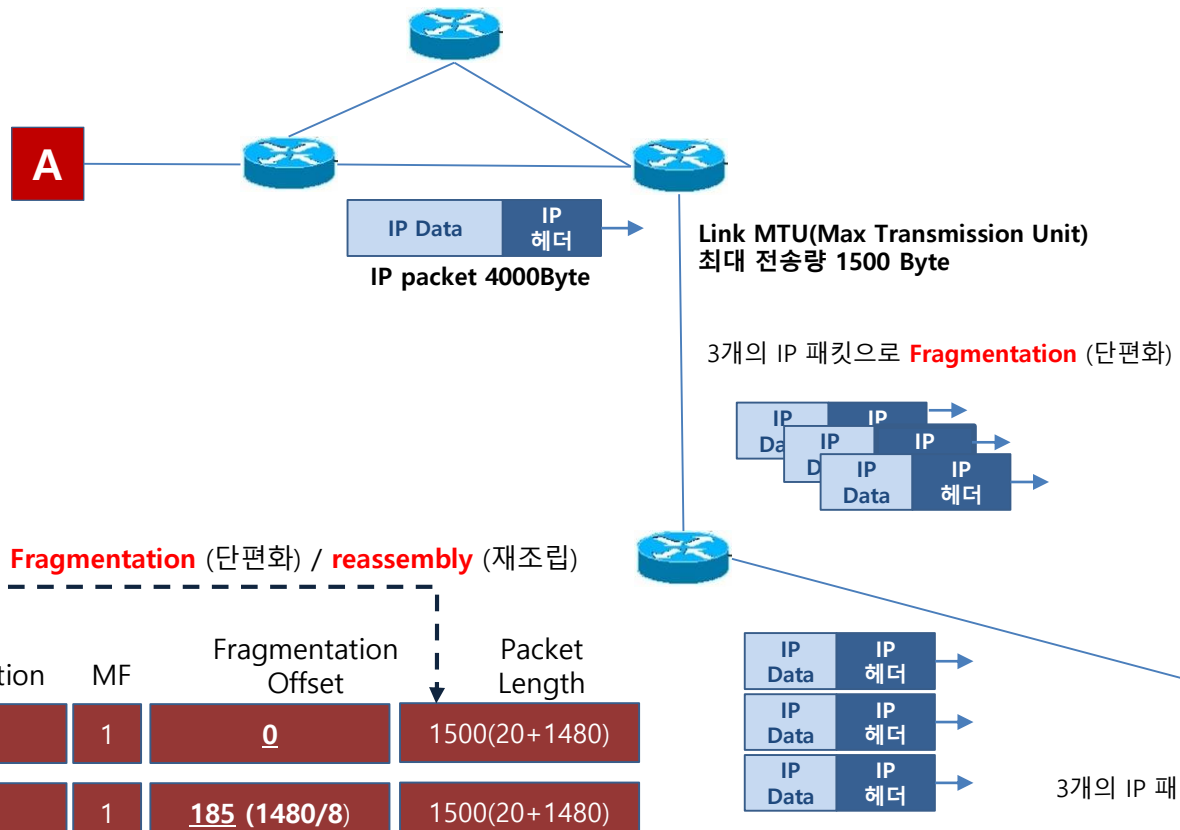
시스템의 단편화 된 데이터의 순서번호를 조작하여 재조합 과정의 오류를 발생시키는 공격

서비스 거부 공격 DoS : Denial of Service

단편화 조작 공격

IP 헤더

0	3	7	13	15	31			
Version Number	Header Length	DS	ECN	Packet Length				
Identification				Flag	Fragment Offset			
				DF		MF		
Time to Live		Transport	Header Checksum					
Source Address								
Destination Address								
Options/Padding								



Identification	MF	Fragmentation Offset	Packet Length
346	0	0	4000(20+3980)

Fragmentation (단편화) / **reassemble** (재조립)

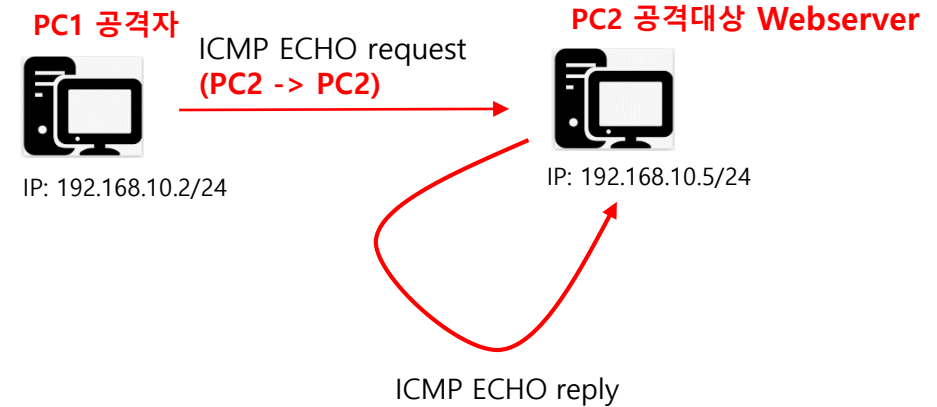
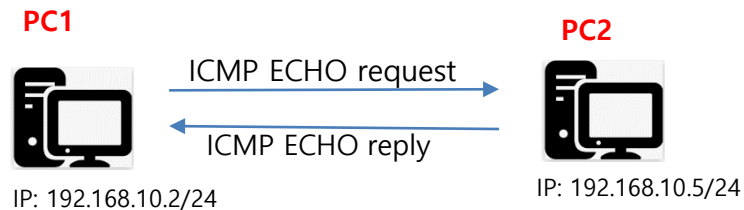
Identification	MF	Fragmentation Offset	Packet Length
346	1	0	1500(20+1480)
346	1	185 (1480/8)	1500(20+1480)
346	0	370 (2960/8)	1040(20+1020)

IP 패킷의 fragmentation offset을 조작하여
수신 호스트에서 재 조립을 어렵게 함
-> 취약점이 패치

서비스 거부 공격 DoS : Denial of Service

랜드 공격(Land attack)

\$ ping 192.168.10.5

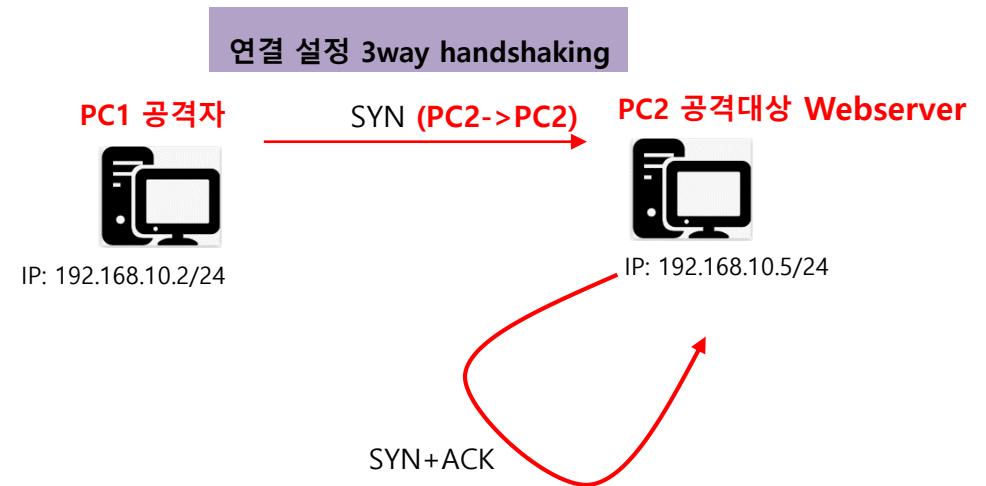
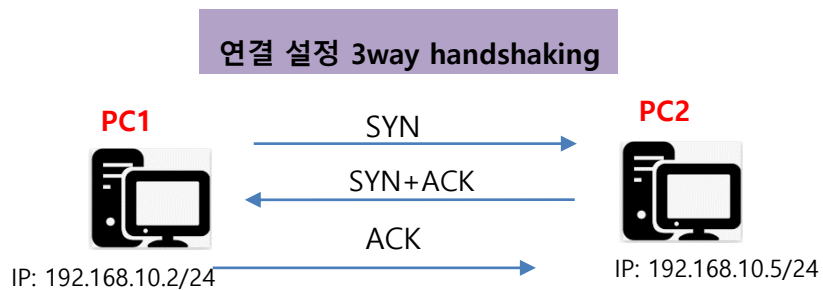


출발지 주소를 목적지 주소로 조작하는 ping of death

서비스 거부 공격 DoS : Denial of Service

랜드 공격(Land attack)

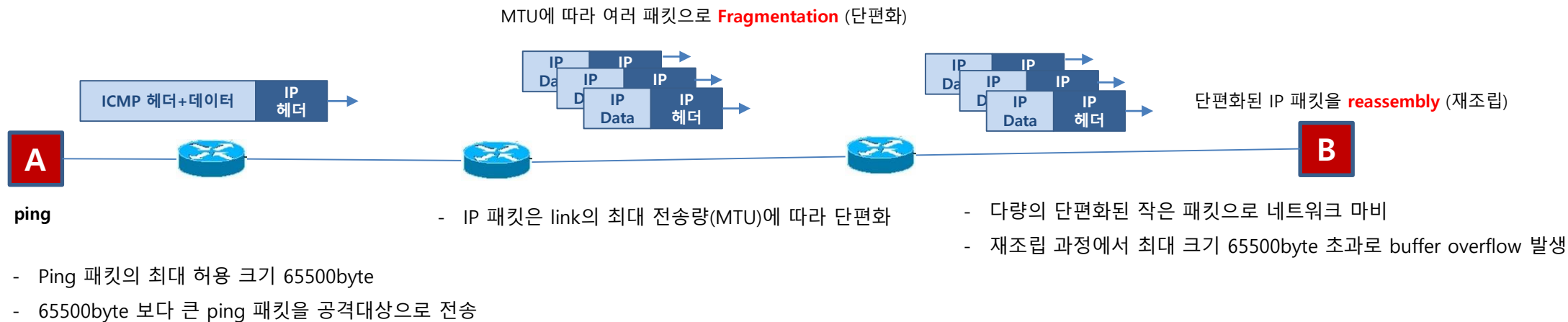
\$ telnet 192.168.10.5



출발지 주소를 목적지 주소로 조작하는 SYN flooding

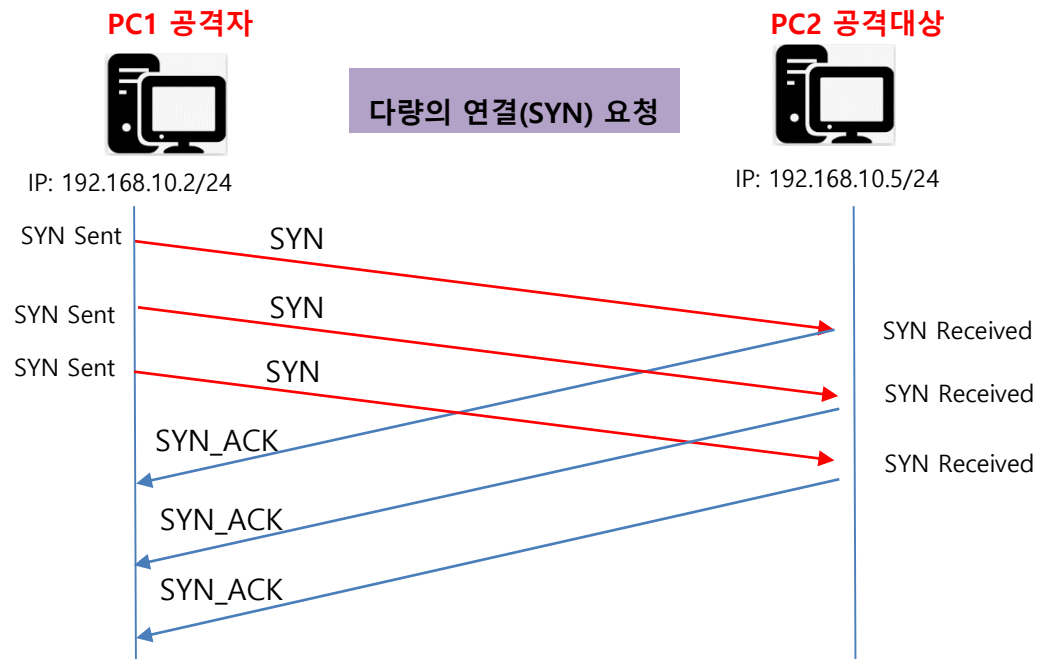
서비스 거부 공격 DoS : Denial of Service

죽음의 핑 공격 (ping of death)



서비스 거부 공격 DoS : Denial of Service

SYN 플러딩(SYN flooding)



- 클라이언트(PC1)이 서버(PC2)로 연결을 위해 SYN 패킷을 보내고,
- 서버(PC2)가 클라이언트(PC1)로 SYN+ACK을 보낼 때, **PC1은 응답 안함 (ACK 안 보냄)**



- 서버(PC2)에 연결 중인 SYN Received 상태 소켓이 다량 생성 (backlog 가득 참)
- 결국, 서버(PC2)는 추가적인 다른 클라이언트의 연결 요청을 거절하게 됨

- `listen(server_socket, 5);`

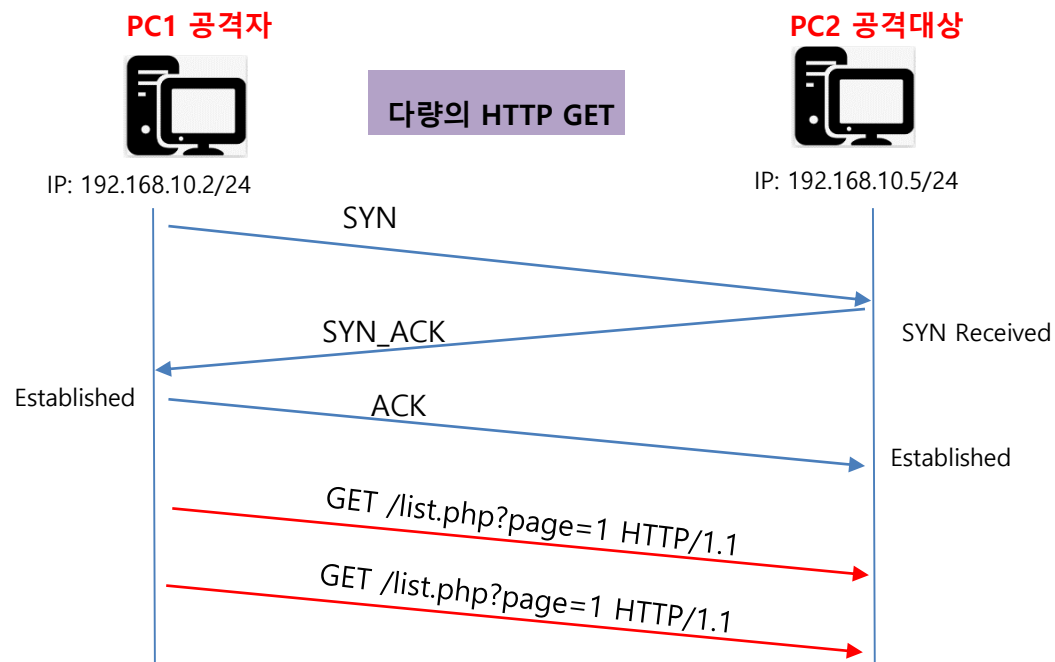
Backlog : 동시에 클라이언트 연결 요청 처리 수



SYN Received 상태는 일정 time-out후 해소됨

서비스 거부 공격 DoS : Denial of Service

HTTP GET 플러딩



- TCP 3way-handshaking 설정 완료 후
- 특정 페이지를 HTTP의 GET 메시지를 무한대로 실행

`http://192.168.10.5/list.php?page=1`

```
$ telnet 192.168.2.5
```

```
GET /list.php?page=1 HTTP/1.1
```



서비스 거부 공격 DoS : Denial of Service

HTTP CC 공격

PC1 공격자



IP: 192.168.10.2/24

캐시 기능 사용 안함

PC2 공격대상



IP: 192.168.10.5/24

```
$ telnet 192.168.2.5
```

```
GET /list.php?page=1 HTTP/1.1
```

```
Cache-Control: no-store, must-validate
```



클라이언트 요청 데이터를 디스크, 메모리, 별도의 저장 장치(Cache Server)에 저장하는 것을 금지
웹 서버가 Caching Server에게 저장된 Cache에 대한 검증을 요구하는 메시지

Cache-Control: no-store, must-validate

- 웹 서버는 **HTTP 요청에 대해 캐시를 사용하지 않고 응답해야 함**
- 웹 서버의 부하를 증가시킴

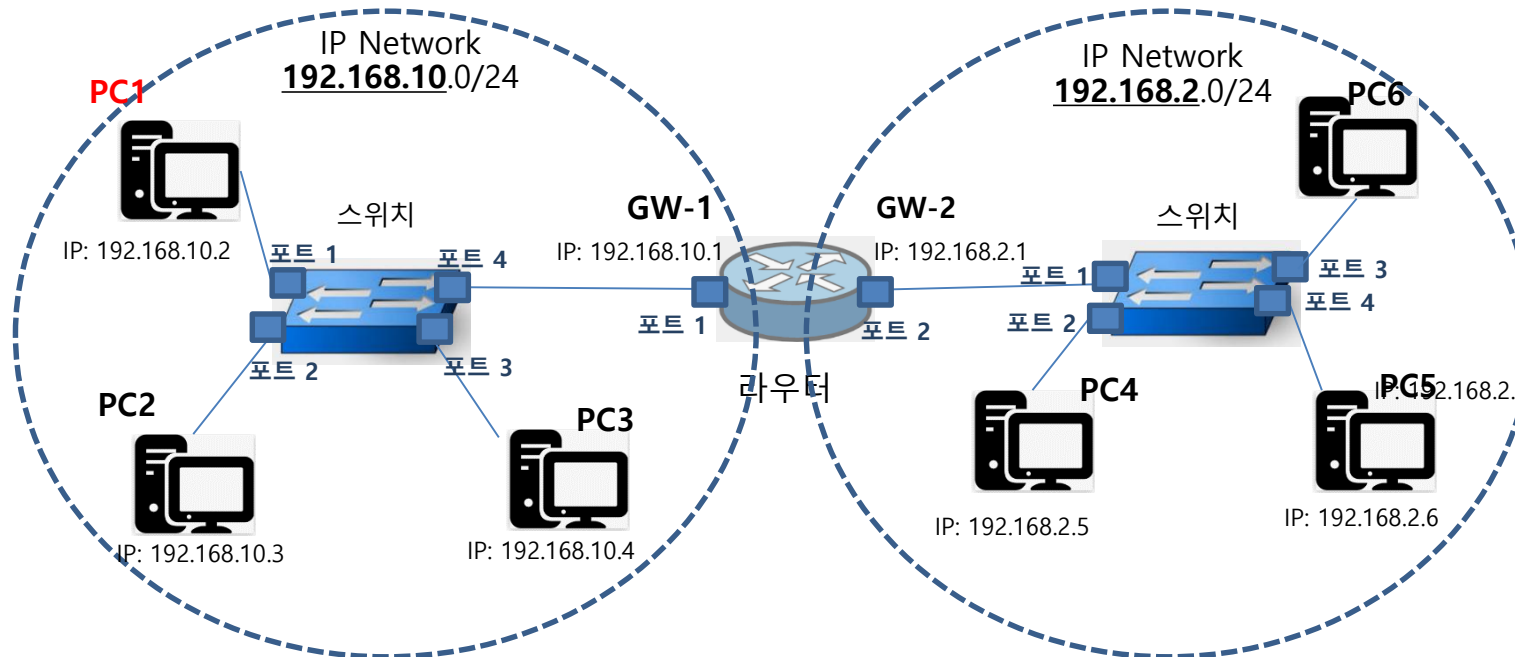
서비스 거부 공격 DoS : Denial of Service Broadcast 전송

스머프 공격

Limited Broadcast 전송 :

동일한 네트워크의 모든 호스트로 보냄
라우터에서 패킷 폐기하여 외부 망으로 안 나감

출발지 IP : 192.168.10.2
도착지 IP : 255.255.255.255



Direct Broadcast 전송

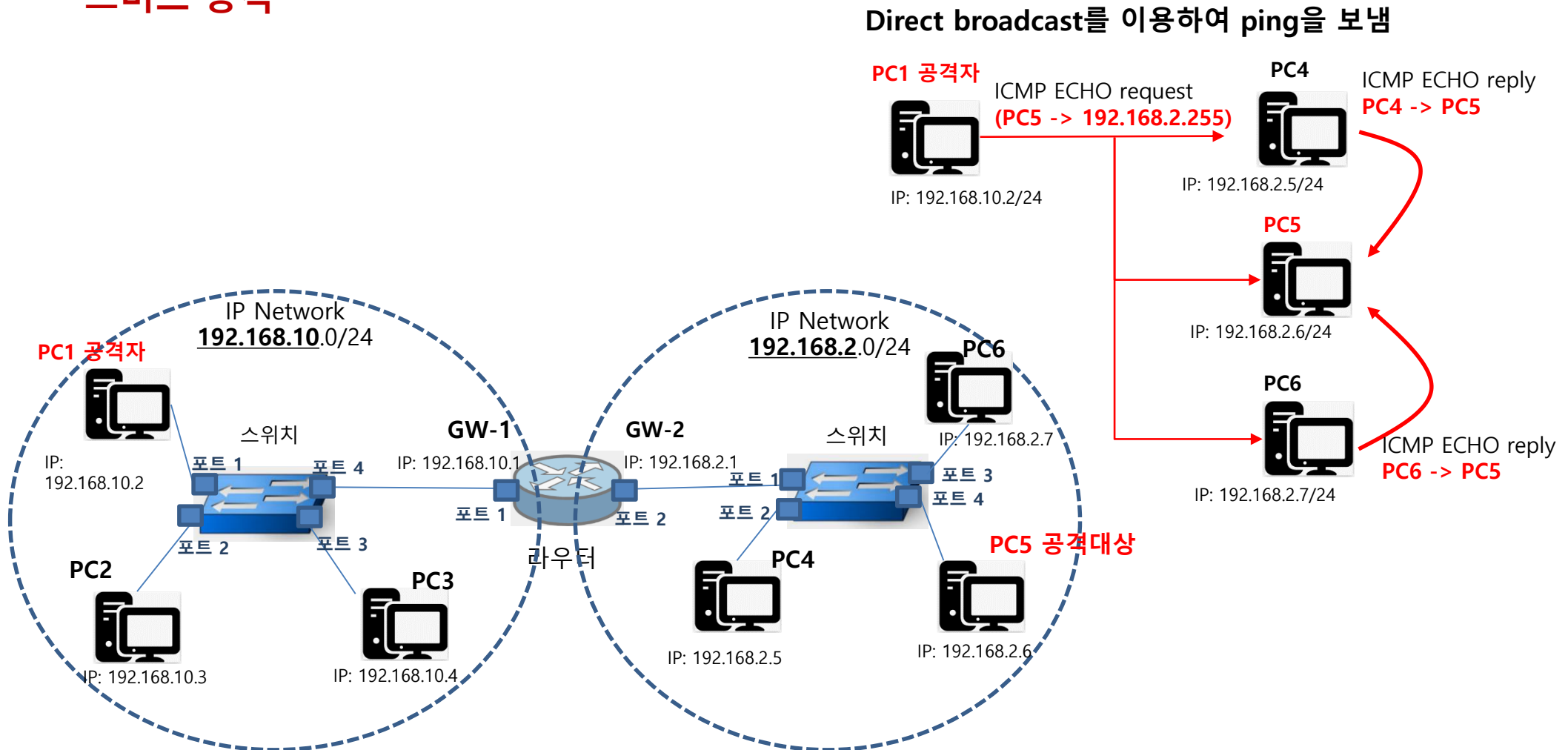
도착지 호스트가 속한 네트워크의 모든 호스트로 보냄
라우터를 거쳐 목적지 서브네트워크에 도착 후, 브로드캐스트

출발지 IP : 192.168.10.2
도착지 IP : 192.168.2.255



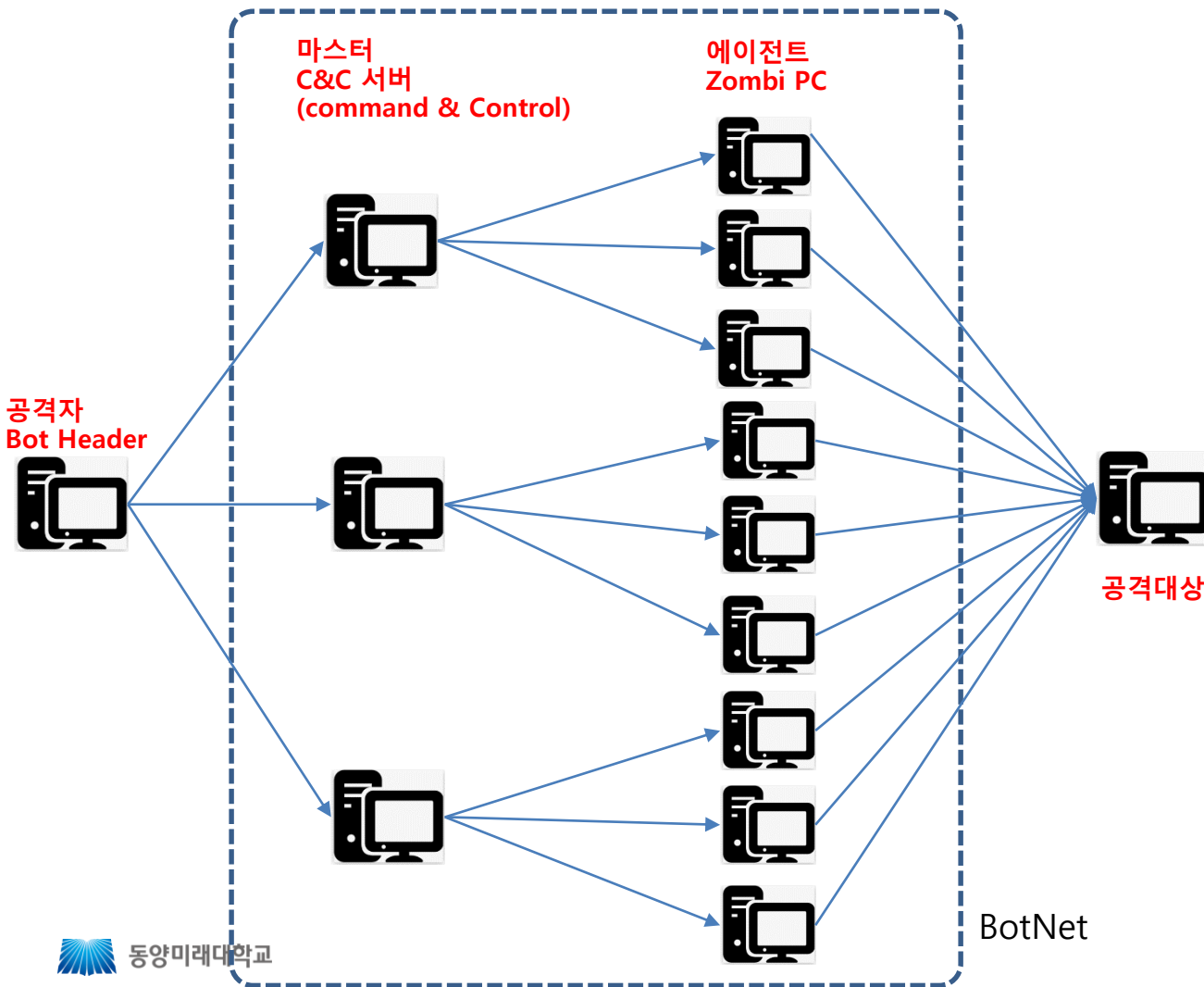
서비스 거부 공격 DoS : Denial of Service

스머프 공격



서비스 거부 공격 DoS : Denial of Service

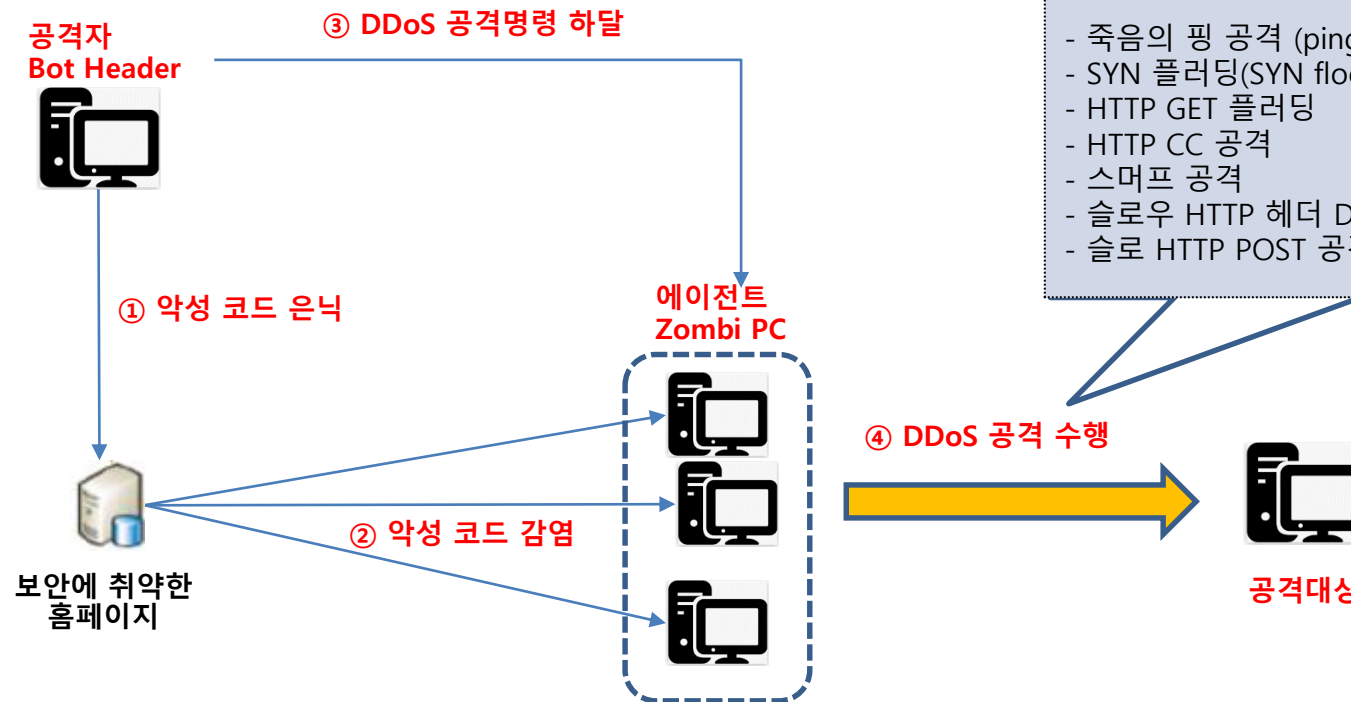
- DDoS : Distributed Denial of Service



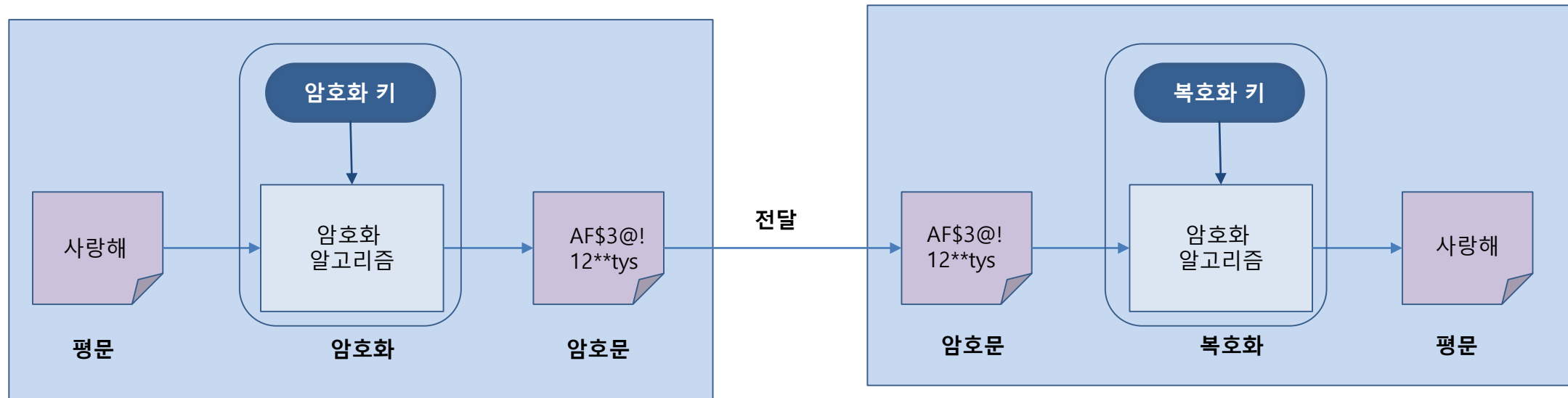
구성		설 명
공격자	Bot Header	- DDoS 공격을 수행하는 실제 공격자
마스터	C&C 서버 (command & Control)	- 공격자의 명령을 Agent(Zombie PC)에게 전달하는 시스템 - Handler 프로그램
에이전트	Zombie PC	- 공격대상에 직접 공격을 가하는 시스템 - 공격자가 유포한 Bot(악성코드)에 감염된 시스템 - Master에게 명령을 전달 받거나 Bot Header가 지정한 시점에 직접적인 공격을 동시에 수행 함 - Daemon 프로그램
봇	bot	- 분산 서비스 거부 공격에 사용되는 악성 코드
봇넷	BotNet	- 좀비 PC끼리 형성된 네트워크

서비스 거부 공격 DoS : Denial of Service

- DDoS : Distributed Denial of Service



암호의 이해



평문 (Plain Text) : 암호화 되기 전의 메시지로, 누구나 알 수 있게 쓴 일반적인 글

암호문(Cryptography) : 암호화되고 난 후 변경된 메시지로, 비밀을 유지하기 위해 당사자만 알 수 있도록 꾸민 약속 기호

암호화 (Encryption) : 평문을 암호문으로 바꾸는 과정으로, 메시지의 내용을 변형하여 원래의 내용을 알 수 없도록 변형

- 암호화 알고리즘 : 평문을 어떤 방식으로 암호문으로 변경할지 결정
- 암호화(복호화) 키 : 허락 받지 않은 외부인이 암호문을 해독하는 것을 막기 위한 암호화 과정에 사용하는 임의의 패턴

복호화 (Decryption) : 암호문을 다시 평문으로 바꾸는 과정

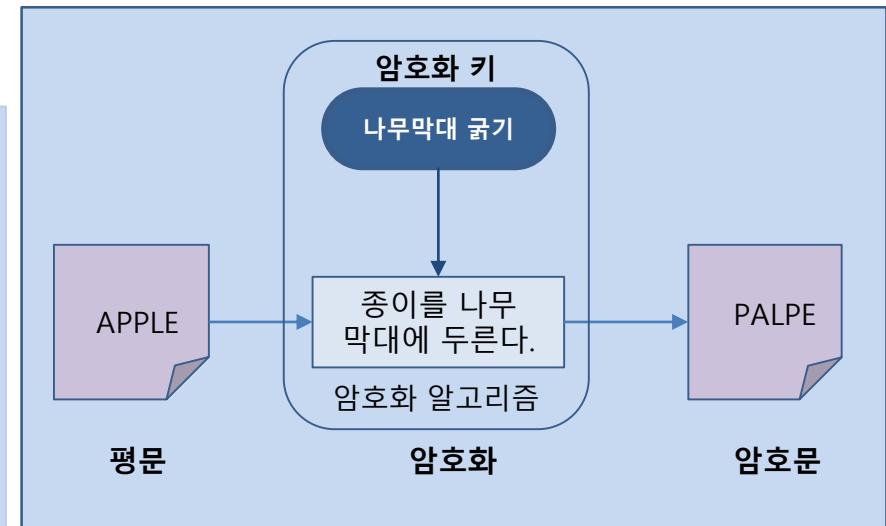
암호의 역사 – 전치법과 대체법

전치법 (Transposition) : 메시지를 구성하는 문자 위치를 바꾸는 방법

스키테일(Scytale) 암호 : 약 2,500년 전 [스파르타](#)에서 사용하던 암호방식

1. 전쟁터에 나갈 군대와 본국에 남아있는 정부는 각자, 스키테일(Scytale)이라고 하는 굵기의 원통형 막대기를 나누어 갖는다.
2. 비밀리에 보내야 할 메시지가 생기면, 본국 정부의 암호 담당자는 스키테일에 가느다란 양피지 리본을 위에서 아래로 감은 다음 옆으로 메시지를 적는다.
3. 리본을 풀어내어 펼치면 메시지의 내용은 아무나 읽을 수 없게 된다.
4. 전쟁터에 나가있는 오로지 같은 굵기의 원통막대기를 가진 사람만이 메시지를 읽을 수 있다.

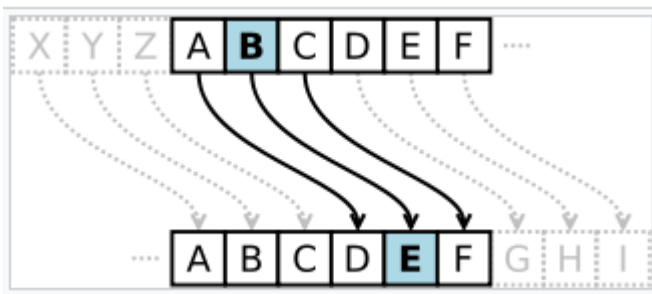
Wiki 백과



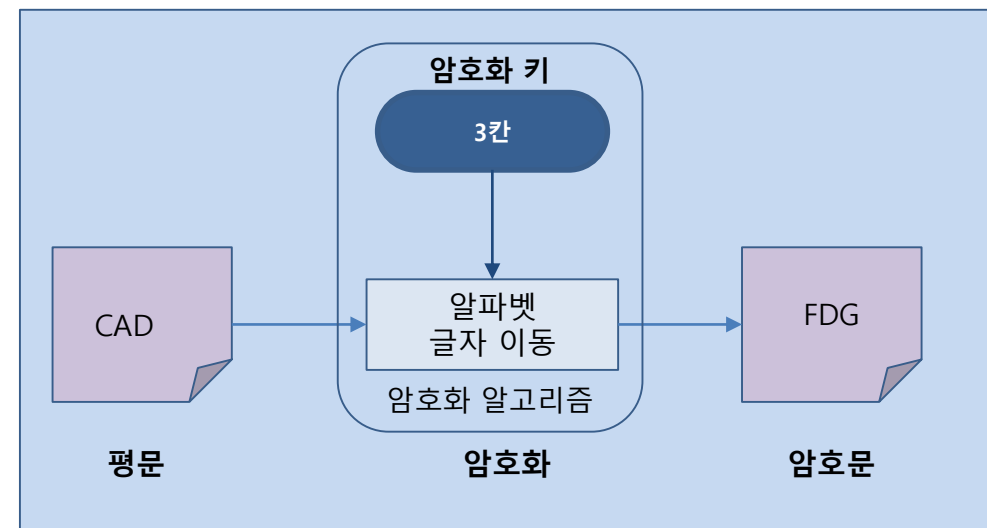
대체법 (substitution) : 메시지를 구성하는 문자를 다른 문자로 대체하는 방법

시저 암호 : 로마의 율리우스 시저가 사용하던 암호방식

1. 카이사르 암호는 각각의 알파벳을 일정한 거리만큼 밀어 글자를 치환하는 방식으로 암호화한다. 예제에서는 3글자씩 밀어서 암호화하기 때문에 B는 E로 치환된다

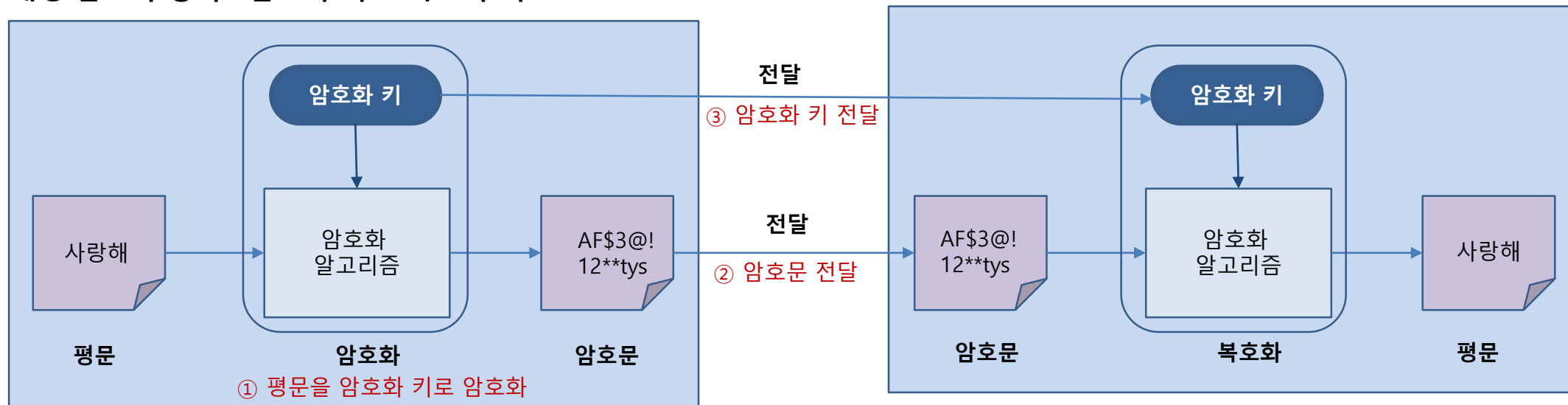


Wiki 백과



암호화 방식 - 대칭 암호화 방식 / 비대칭 암호화 방식

대칭 암호화 방식 : 암호화 키 = 복호화 키



① 평문을 암호화 키로 암호화

② 암호문 전달

③ 암호화 키 전달



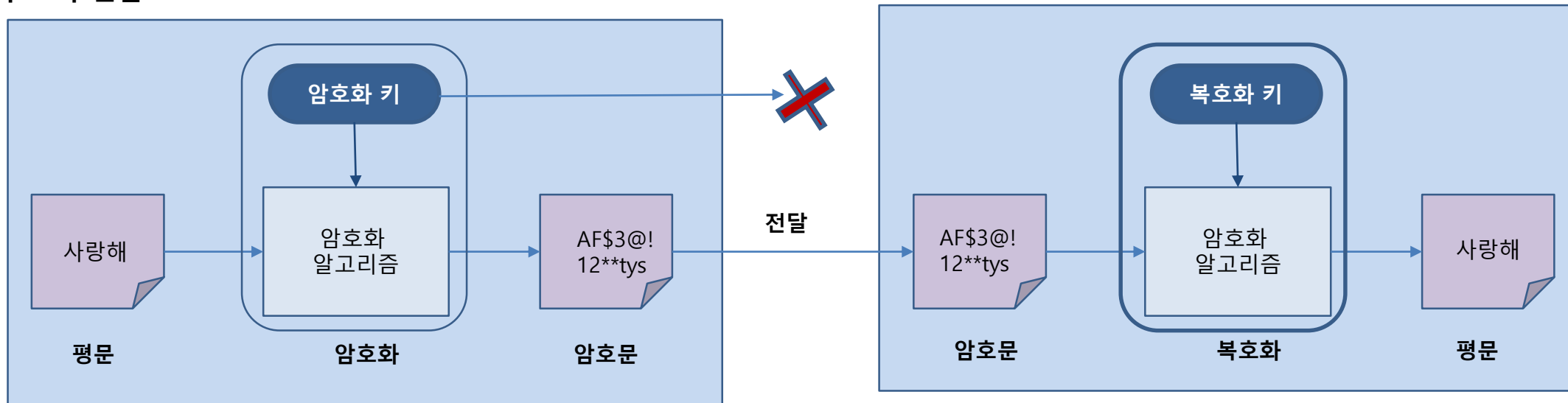
인터넷 환경에서 키를 원격지에 어떻게 안전하게 보낼까?
암호화 키를 암호화해서? 그럼 암호화된 암호화 키를 해석하는 키는 어떻게 전송?

DES, 트리플 DES, AES, SEED, RC4

암호화 방식 - 대칭 암호화 방식 / 비대칭 암호화 방식

대칭 암호화 방식 : 암호화 키 = 복호화 키

구조적 결함



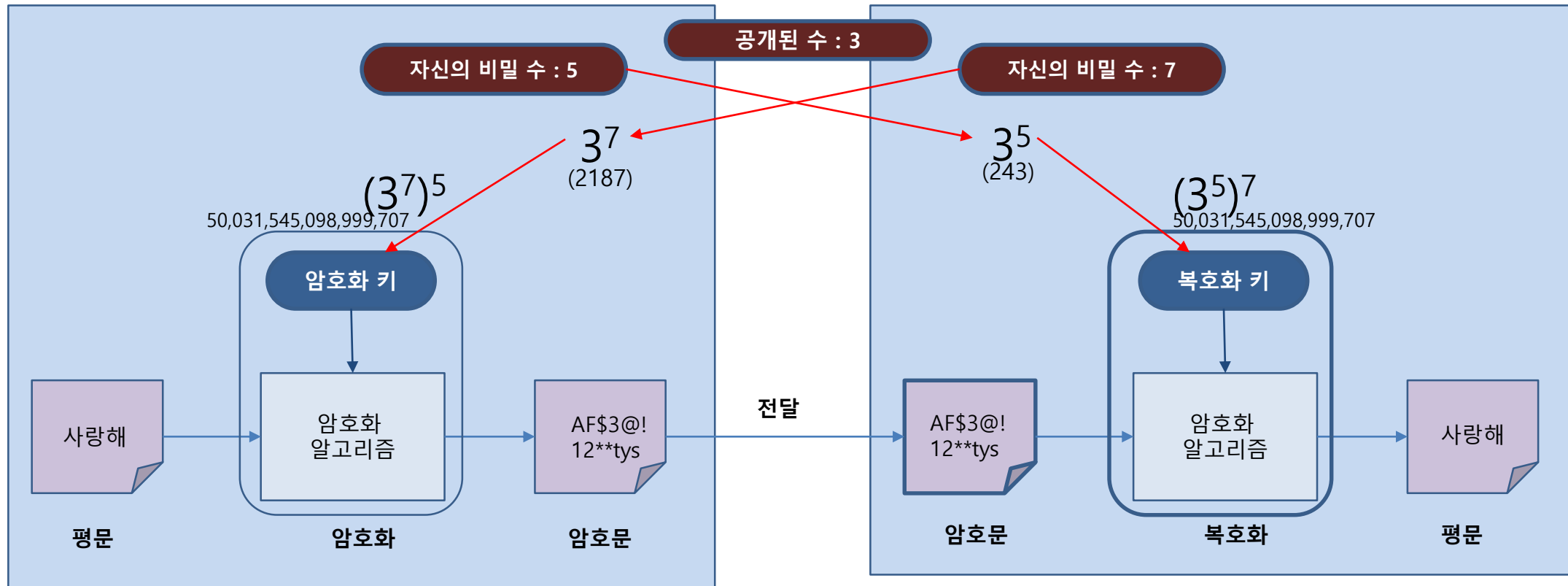
대칭 암호화 알고리즘의 구조적 한계를 극복하기 위한 방법

<- 인터넷 환경에서 키를 원격지에 어떻게 안전하게 보낼까?

암호화 방식 – 대칭 암호화 방식 / 비대칭 암호화 방식

비 대칭 암호화 방식 : 암호화 키 \neq 복호화 키

디피-헬만 키 공유 (DH 키 공유) – 비 대칭 개념의 출발

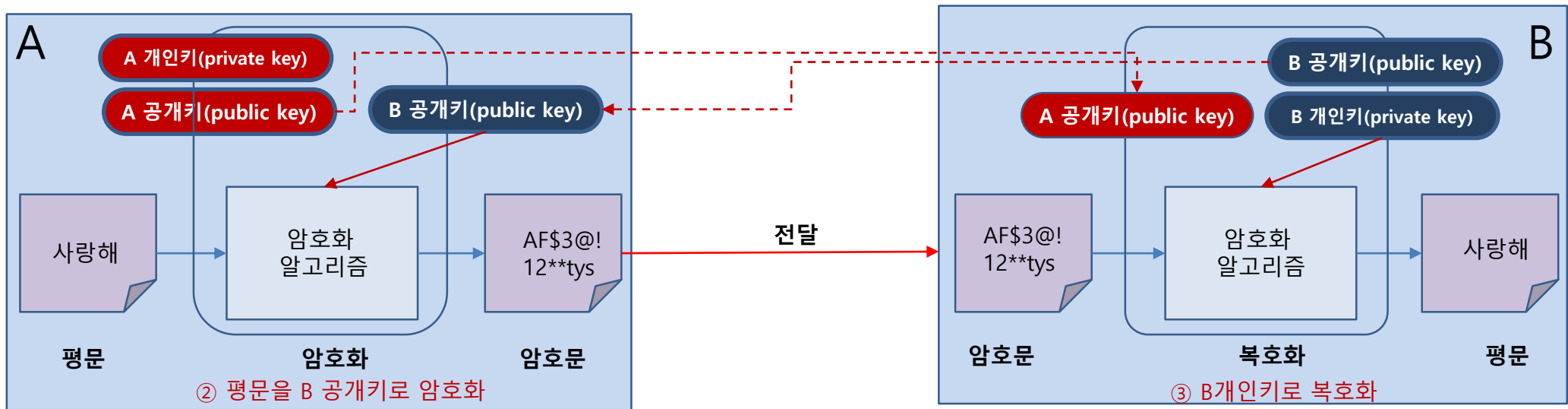


직접적인 키 교환없이, 공개된 수(공개키)를 가지고 자신의 비밀 수(개인 비밀 키)로 부터 암호화(복호화) 키 생성

암호화 방식 - 대칭 암호화 방식 / 비대칭 암호화 방식

비 대칭 암호화 방식 : 암호화 키 \neq 복호화 키

RSA : 1978년 [로널드 라이베스트](#)(Ron Rivest), [아디 샤미르](#)(Adi Shamir), [레너드 애들먼](#)(Leonard Adleman)에 의해 개발된 사실상의 표준

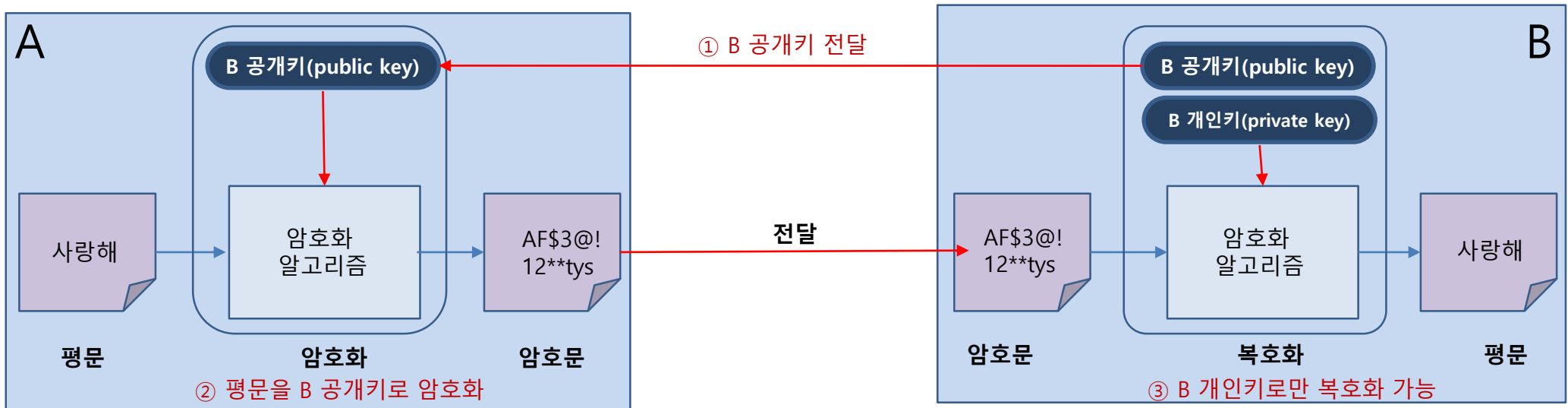


- 비밀 통신을 하기 위한 주체는 **키 쌍을 생성 (공개키, 개인키)**
- 공개키는 인터넷을 통해 상대방에게 전달하는 키이며, 개인키는 자신만 가지고 있는 키임
- 메시지 전달의 기밀성과 부인방지 기능을 제공

암호화 방식 - 대칭 암호화 방식 / 비대칭 암호화 방식

비 대칭 암호화 방식 : 암호화 키 \neq 복호화 키

RSA : 기밀성



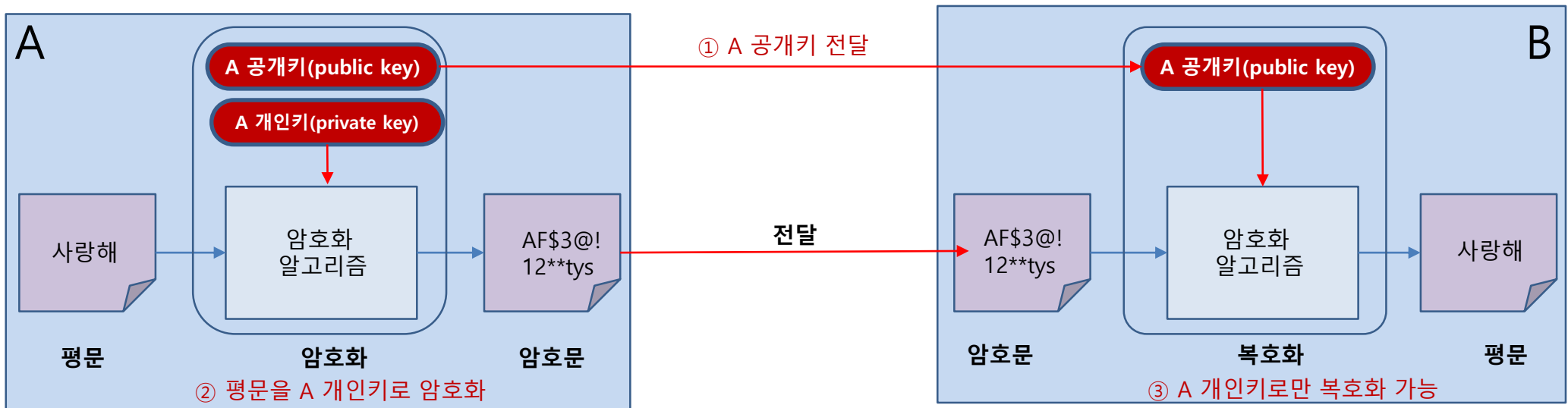
- ① (B 공개키 전달) 수신자(B)는 발신자(A)에게 자신(B)의 공개키를 전송(①)하여 암호화에 사용하도록 함
- ② (평문을 B 공개키로 암호화) 발신자(A)는 수신자(B)의 공개키로 평문을 암호문으로 만들
- ③ (B 개인키로 복호화) B 공개키로 암호화한 암호문은 B 개인키로만 복호화 가능하여 B만 수신 내용을 볼 수 있음

(기밀성) B의 공개키로 암호화한 문서는 B만(B 개인키로만) 볼 수 있음

암호화 방식 - 대칭 암호화 방식 / 비대칭 암호화 방식

비 대칭 암호화 방식 : 암호화 키 \neq 복호화 키

RSA : 부인 방지



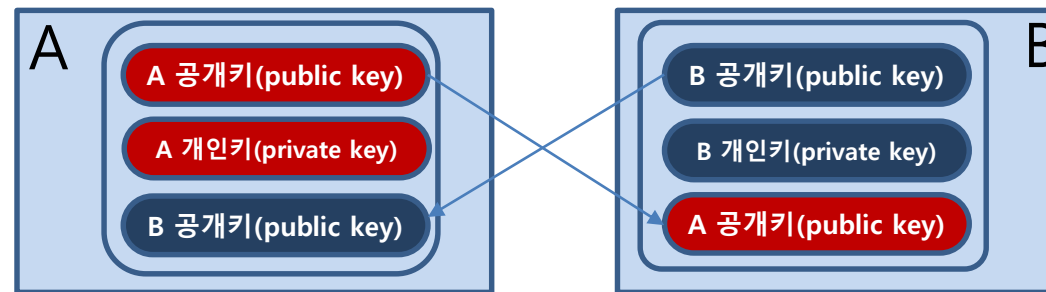
- ① (A 공개키 전달) 발신자(A)는 수신자(B)에게 자신(A)의 공개키를 전송(①)하여 복호화에 사용하도록 함
- ② (평문을 A 개인키로 암호화) 발신자(A)는 자신의 개인키로 평문을 암호문으로 만듦
- ③ (A 공개키로 복호화) A 개인키로 암호화한 암호문은 A 공개키로만 복호화 가능하여 A는 자신이 보낸 것을 부인할 수 없음(전자상거래의 계약서 등 법적 증거)

(부인방지) A의 공개키로 해독 가능하다는 것은 A가 보냈다는 것을 증명

암호화 방식 - 대칭 암호화 방식 / 비대칭 암호화 방식

비 대칭 암호화 방식 : 암호화 키 \neq 복호화 키

RSA

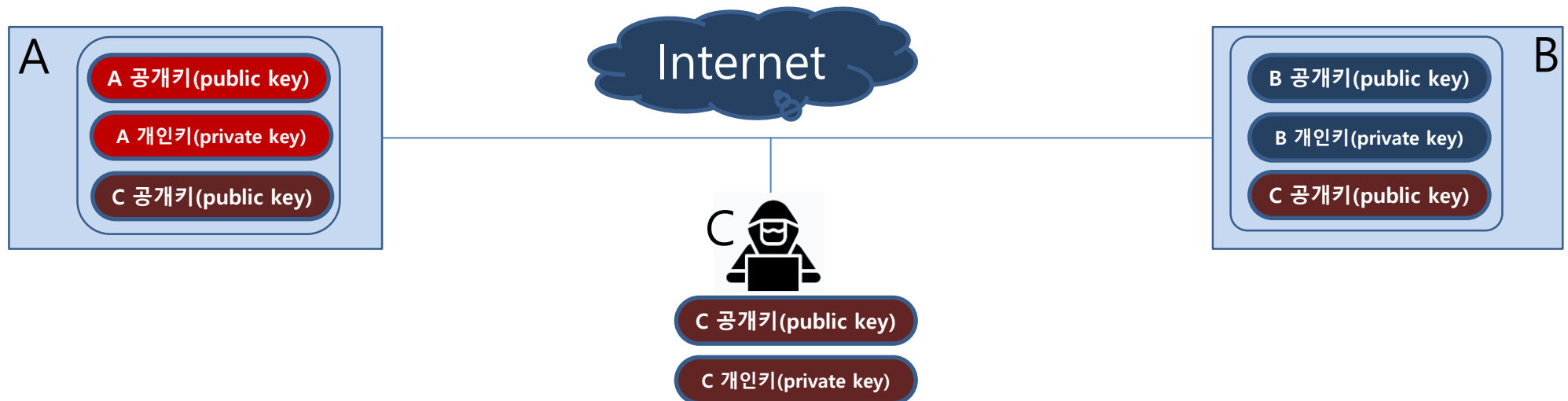


- A와 B가 비밀 통신을 하기 위해서는 각각 3개의 키를 가지고 있어야 한다.
- 자신의 공개키와 개인키, 상대방의 공개키

암호화 방식 – 대칭 암호화 방식 / 비대칭 암호화 방식

비 대칭 암호화 방식 : 암호화 키 \neq 복호화 키

RSA 해킹 공격

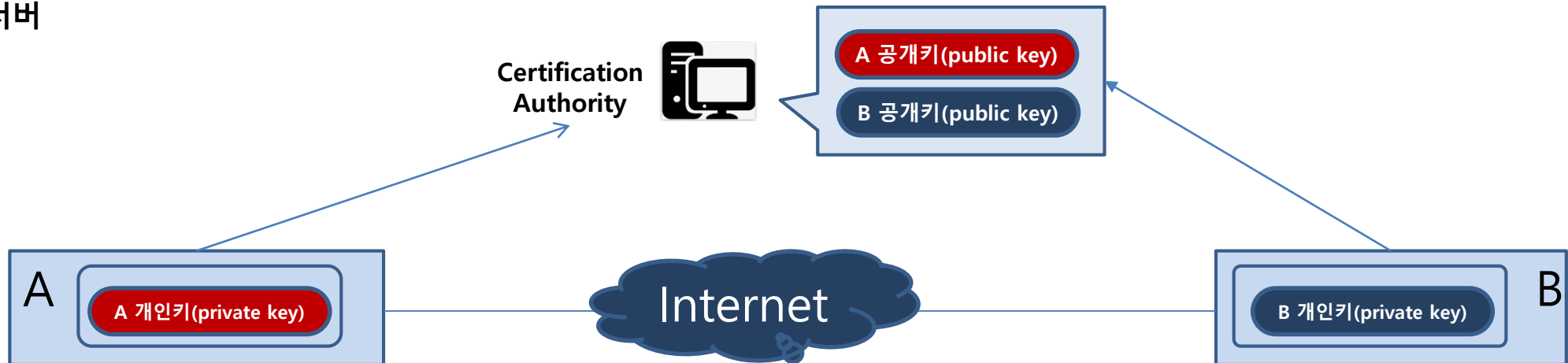


- 키 교환을 하려는 호스트 사이에 공격자가 끼어든다.
- 교환되는 공개키를 가로채어 자신의 공개키(C)를 상대방인 것처럼 속여 양쪽에 전달
- A나 B에서 C 공개키로 암호화된 데이터는 C 개인키로 해독 가능

암호화 방식 - 대칭 암호화 방식 / 비대칭 암호화 방식

비 대칭 암호화 방식 : 암호화 키 \neq 복호화 키

CA 서버



- 키를 발생하는 것은 많은 CPU time 소용
- 키 교환 과정의 구조적 보안 문제를 해결하기 위해 키 자체를 인증기관에 등록 후 사용
- 공인 인증기관을 활용하면 굳이 키를 교환할 필요는 없다.