1. 인터넷 프로토콜과 보안

담당교수: 차 영욱

ywcha@andong.ac.kr

안동대학교
ANDONG NATIONAL UNIVERSITY

목 차

- 인터넷 프로토콜의 개요 및 역사
  - 인터넷의 통신 모델
- 네트워크 보안의 정의 및 해킹 동향
- IP 프로토콜의 보안 취약성과 공격
- 보안기법의 계층 구조
- 네트워크 보안의 구성

인터넷 프로토콜의 개요

- 프로토콜(Protocol) : 네트워크에 연결된 시스템(라우터, 스위치, 컴퓨터, …)들의 통신을 위하여 상호 정의한 규칙

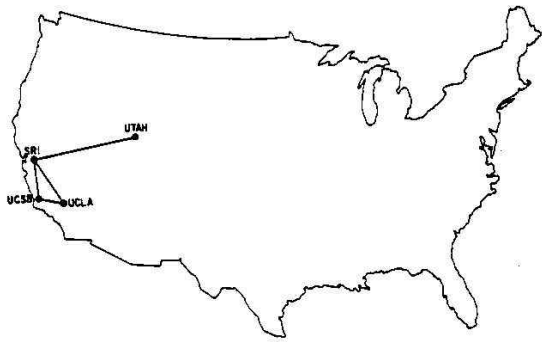
- 인터넷(Internet)은 "정보의 바다"라 불리는 컴퓨터 통신망으로, 전 세계의 컴퓨터가 서로 연결되어 TCP/IP 프로토콜을 이용해 정보를 주고받는 공개 컴퓨터 통신망(참조:http://ko.wikipedia.org)

- 인터넷의 응용 서비스
  - 파일 전송, 전자 메일, 전자 상거래, 인터넷 뱅킹, …

- 초기의 인터넷은 데이터의 전송만을 염두에 두고 개발
  - 메시지의 변조(spoofing) 및 훔쳐보기에 취약
  - 보안의 중요성이 대두되어 보안 프로토콜(IPSec, SSL/TLS, …) 개발

인터넷의 역사

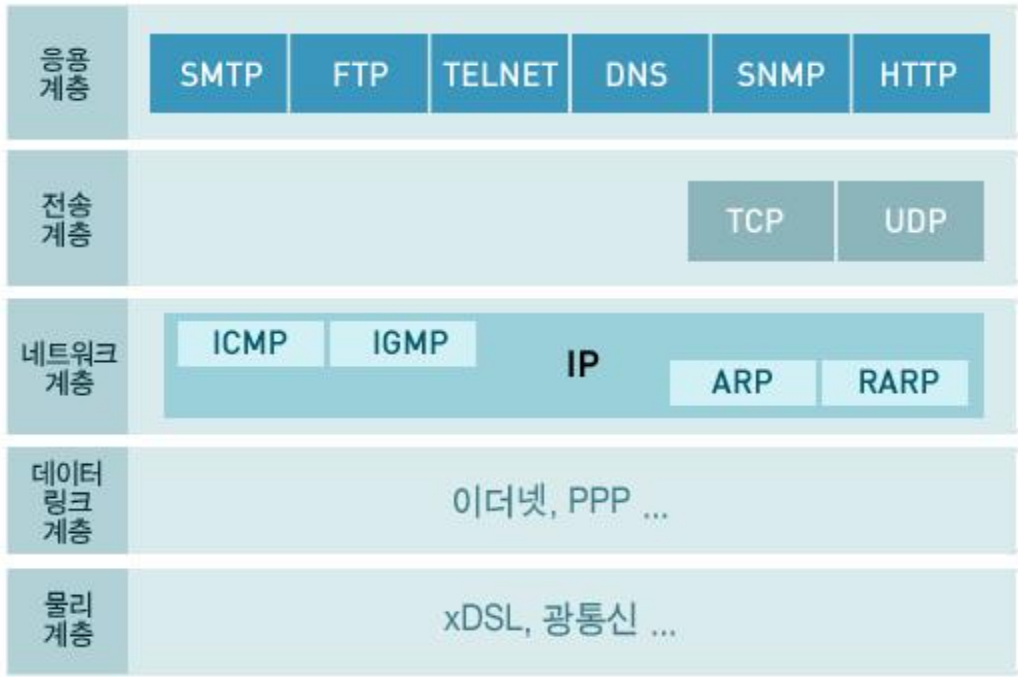
- 1969. 미국 국방성의 ARPA는 4 개의 노드로 구성되는 세계 최초의 패킷 스위칭 네트워크인 ARPANET(Advanced Research Project Agency Network) 설치
  - UCLA, UC Santa Barbara, Stanford Research Institute, University of Utah



- 노드의 수가 증가함에 따라 ARPANET 네트워크 제어 프로토콜의 연동에 문제 발생
- 1974. 미국 국방성에서 인터넷 통신을 위한 TCP/IP 프로토콜 정의
- 1981. UC Berkeley가 TCP/IP를 UNIX에 포함시킴
- 1984. 유연하고 안전하며 상호연동이 가능한 통신 모델을 위하여 ISO(International Standard Organization) 에서 OSI(Open Systems Interconnection) 7계층 모델 정의

인터넷의 통신 모델

- 5 계층 모델
  - 응용계층, 전송계층, 네트워크 계층, 데이터링크 계층, 물리계층



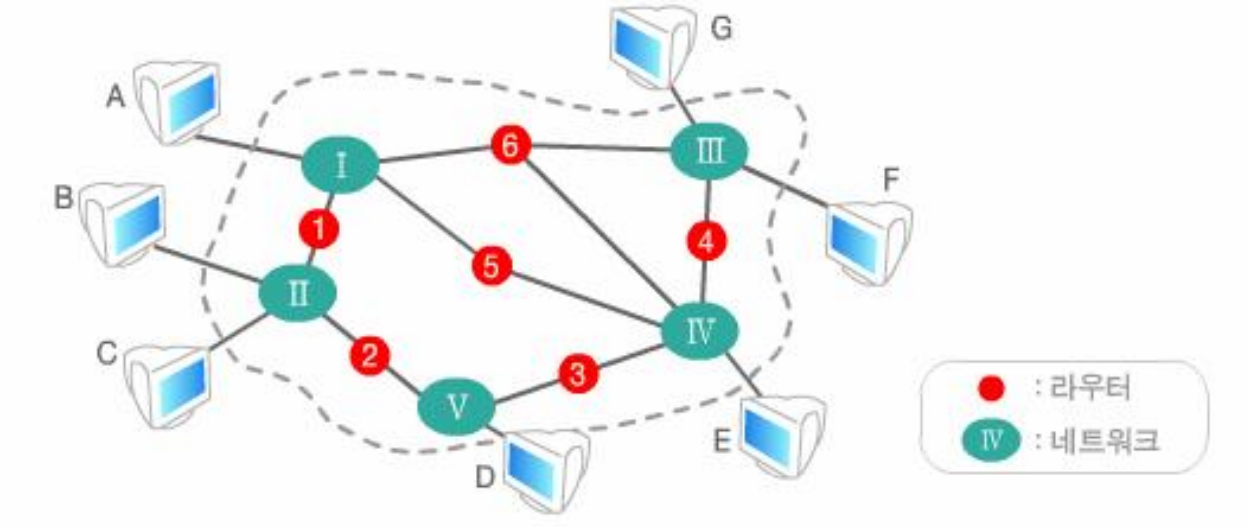
ARP: Address Resolution Protocol
ICMP: Internet Control Message Protocol
IGMP: Internet Group Management Protocol
IP: Internet Protocol

FTP: File Transfer Protocol
HTTP: HyperText Transfer Protocol
TCP: Transmission Control Protocol
UDP: User Datagram Protocol

네트워크 계층

❑ 인터넷 프로토콜(IP: Internet Protocol)

- 발신지에서 인터넷을 통해 목적지로 패킷을 전달하는 프로토콜로 주소지정, 패킷의 분할과 결합 및 라우팅 기능을 수행
- 버전: IPv4와 IPv6



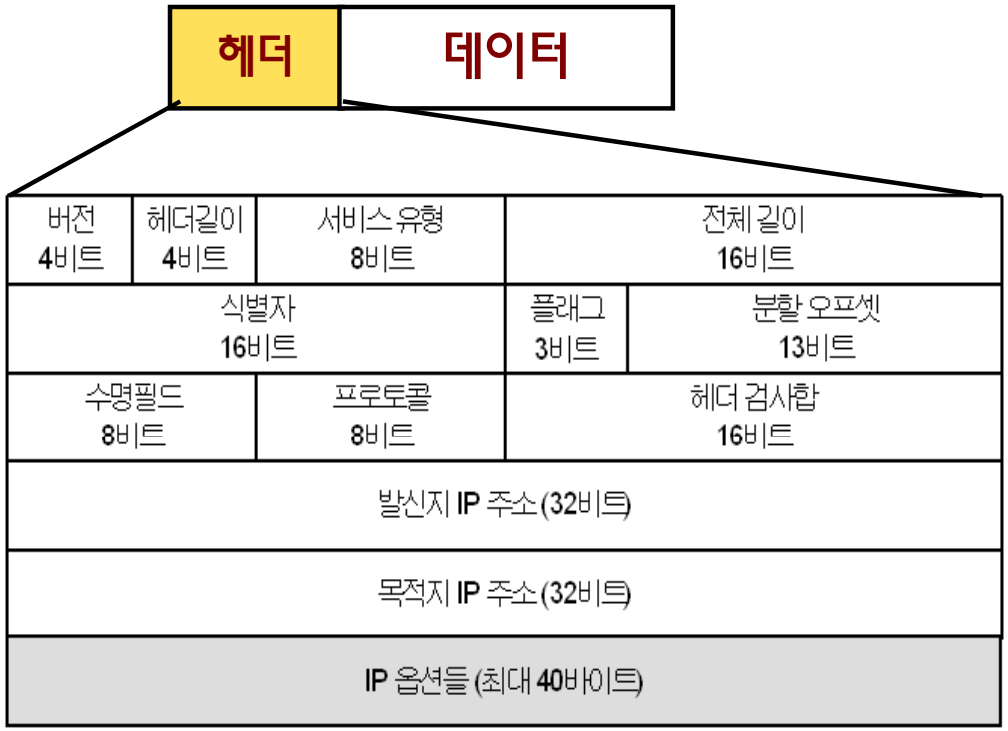
❑ 지원 프로토콜

- 인터넷 제어메시지 프로토콜(ICMP), 인터넷 그룹관리 프로토콜(IGMP), 주소변환 프로토콜(ARP)

IP 버전 4 (1/2)

❑ IP 패킷

- **헤더 부분:** 20바이트 고정 부분과 가변 길이의 선택사항 부분
- **데이터 부분:** 전송계층(TCP 또는 UDP), ICMP, IGMP, OSPF 메시지



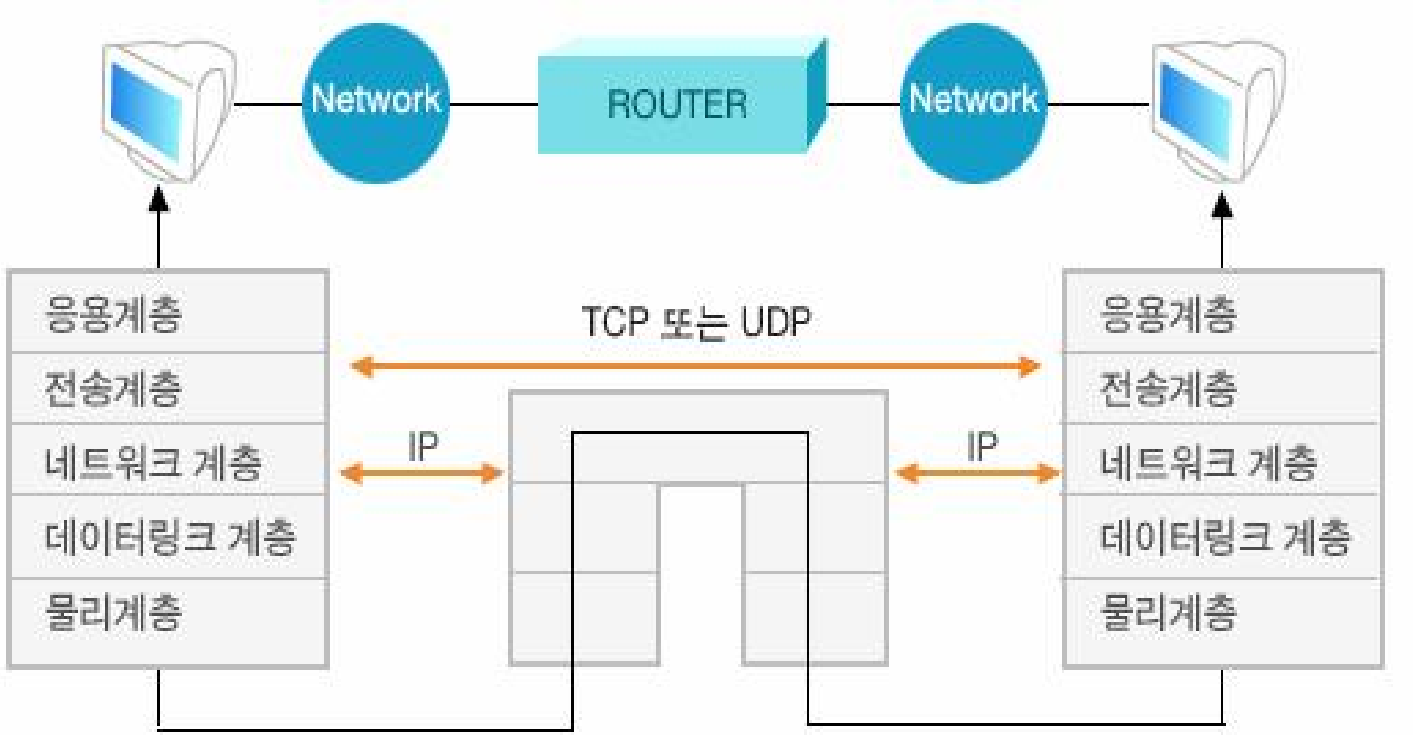
- **IP 프로토콜의 버전**: 4
- **IP 헤더의 길이**
- **서비스 유형**: 네트워크에 요구하는 지연, 처리율, 신뢰성과 같은 서비스 유형 지시
- **IP 패킷의 전체 길이**(최대 2^{16})
- **분할과 관련된 헤더필드: 식별자, 플래그, 분할 오프셋**
  - 데이터링크 계층이 지원하는 최대 길이(예, 이더넷 1560 바이트)보다 긴 패킷은 IP 계층에서 여러 패킷으로 분할
- **프로토콜**: 패킷 데이터 부분의 메시지 종류(TCP, UDP, ICMP, IGMP, …)

IP 버전 4 (2/2)

- 수명(TTL: Time-To-Live)
  - 발신지 호스트는 패킷의 생성 시에 초기값(예, 32) 설정 → 패킷이 라우터를 통과하면 TTL 값이 1씩 감소
  - 목적지에 도착하기 전에 TTL 값이 0이 되면 라우터는 패킷 폐기 → 목적지가 없는 패킷이 네트워크에서 무한정 순환하는 것을 방지
- 헤더 검사합: IP 헤더의 손상 연부를 검사하기 위하여 사용
- 발신지/목적지 IP 주소: 패킷의 발신지 및 목적지를 나타내는 4바이트 IP 주소(예, 220.89.62.37)
- IP 헤더 옵션
  - 경로설정, 타이밍 관리 등과 같은 패킷에 대한 부가적인 정보를 전달
  - 대부분의 라우터들이 IP 헤더 옵션 필드를 사용하지 않음

전송계층

- 파일전송, 메일전송, 웹 서비스 등의 인터넷 서비스를 위하여 호스트와 호스트 사이에 공통적으로 적용되는 프로토콜
  - 전송제어 프로토콜(TCP: Transmission Control Protocol)
  - 사용자 데이터그램 프로토콜(UDP: User Datagram Protocol)



TCP 프로토콜

- ❑ 연결형 전송 서비스 제공
- ❑ 흐름제어 및 오류제어 서비스 제공

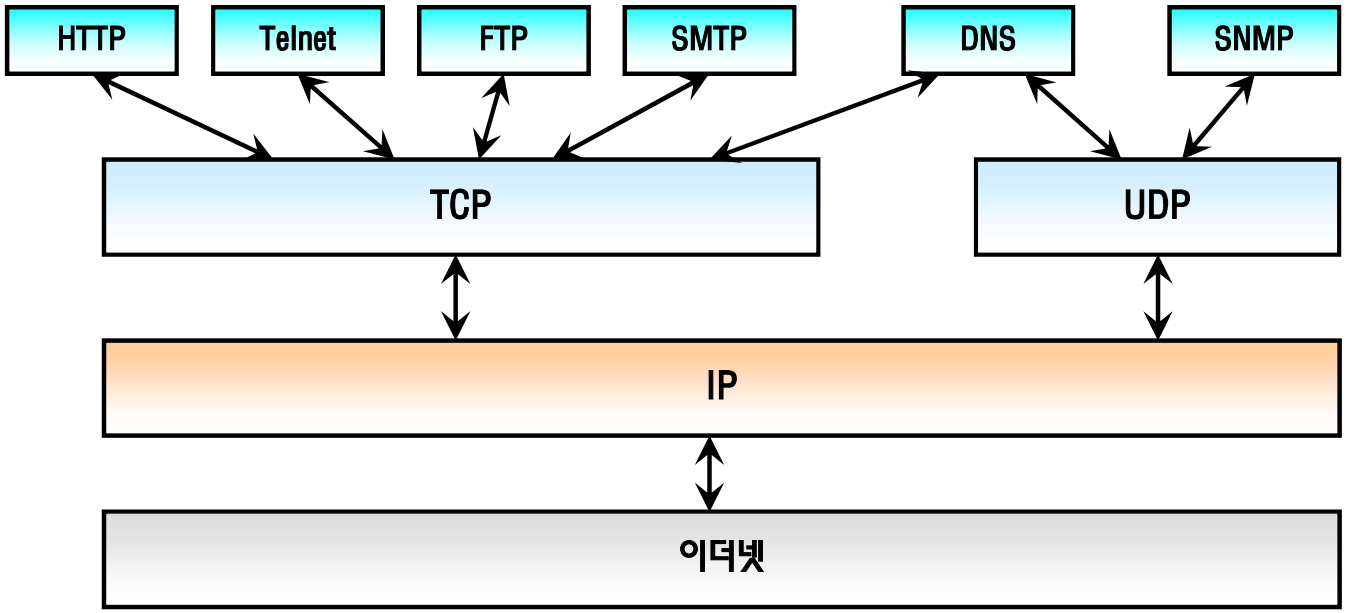
- **포트번호**: 발신지 및 착신지 호스트의 응용계층을 식별
  - FTP: 20, 21
  - HTTP: 80
  - 전자우편 프로토콜(SMTP): 25
- **순서 및 응답번호**: 신뢰성 있는 전달을 위하여 메시지의 손실 및 중복 등의 오류 제어 기능 지원
- **제어 필드**: TCP 연결의 설정 및 해제 등을 위한 제어 플래그
- **윈도우**: 호스트 사이에 주고 받는 메시지의 양을 조정하는 흐름제어 기능 지원
- **검사합**: 메시지의 손상 여부를 검사

UDP 프로토콜

- 흐름제어 및 오류제어 기능이 없는 비연결형 전송 서비스 제공
- UDP 헤더
  - 포트번호
    - 부트스트랩 프로토콜: 67
    - 시간 동기화 프로토콜(NTP): 123
    - 망관리 프로토콜(SNMP): 161
    - 실시간 인터넷 방송
  - 전체 길이: 메시지의 전체 길이
  - 검사합: 메시지의 손상 여부를 검사

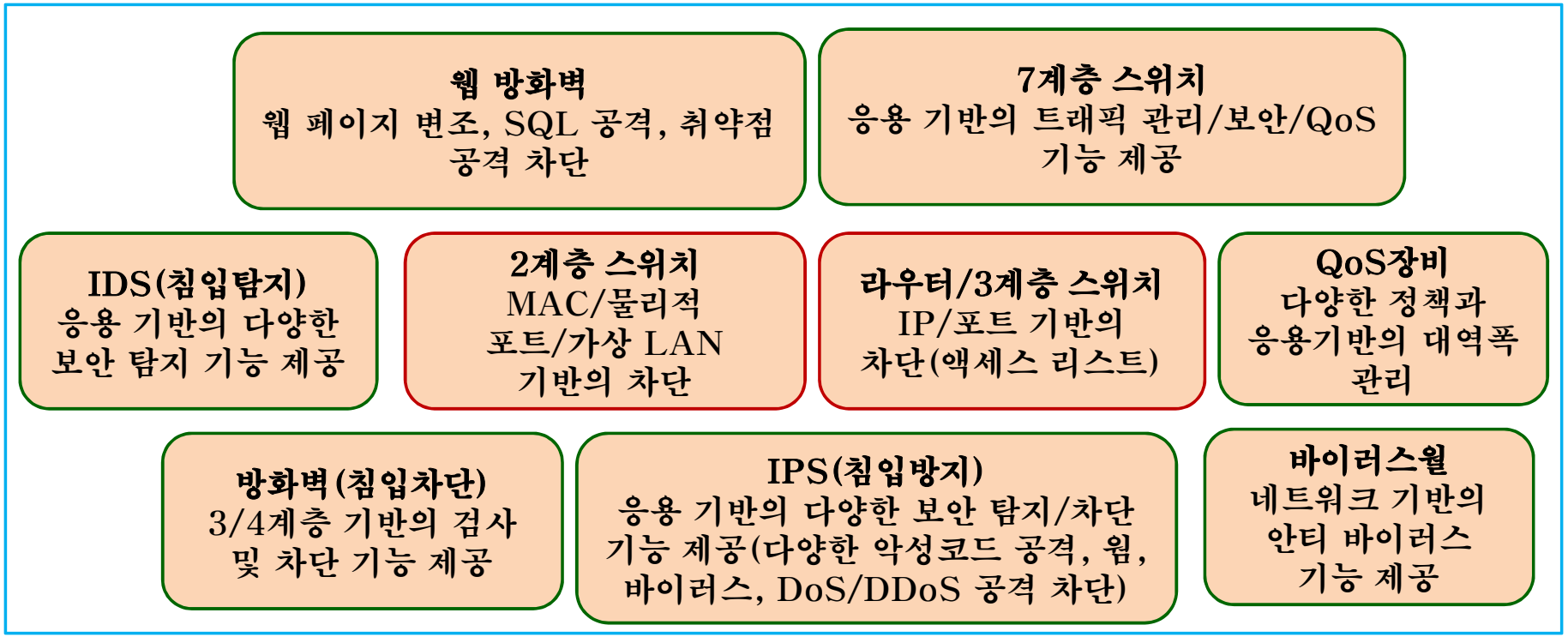
응용 계층

- FTP (File Transfer Protocol): 파일 전송 프로토콜
- SMTP (Simple Mail Transfer Protocol): 메일 전송 프로토콜
- DNS (Domain Name System): 도메인 이름 시스템 프로토콜
  - www.fifa.com ➔ 125.56.214.97
- HTTP (Hypertext Transfer Protocol): 하이퍼텍스트 전달 프로토콜
- Telnet: 원격 로그인 프로토콜
- SNMP(Simple Network Management Protocol): 망 관리 프로토콜



네트워크 보안

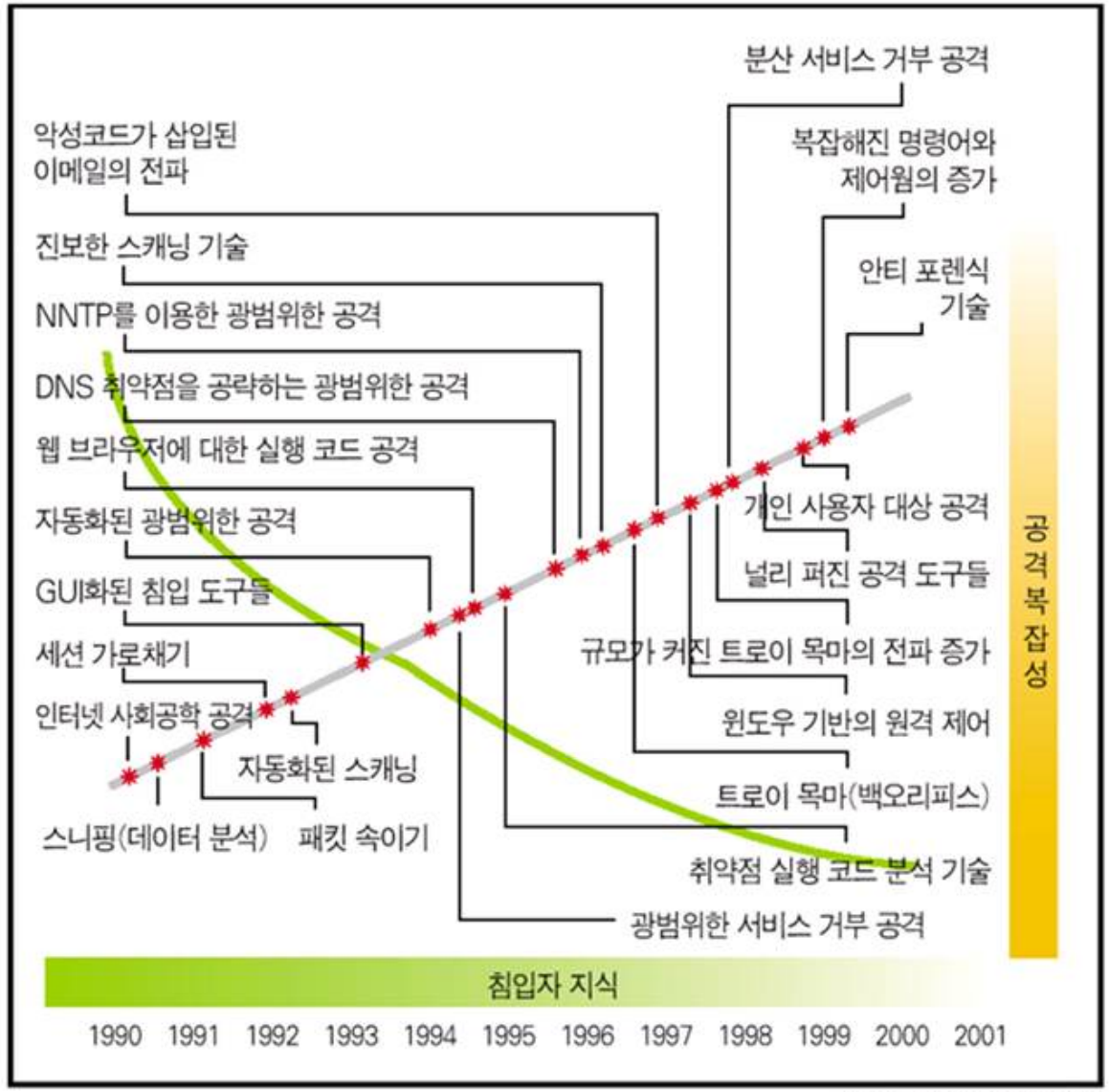
- 네트워크의 위협적인 공격 요소로부터 네트워크 장비, 서버, 운영 체제, 응용 프로그램, 사용자 정보 등을 안전하게 보호
- 근래에는 해킹뿐만 아닌 각종 웜, 바이러스 등이 공격 요소로 등장하면서 네트워크 보안의 범주가 더욱 넓어짐
- 다양한 보안장비



해킹 기술과 공격도구의 발전사

- 해커의 자기과시에서 정치적, 경제적인 이익 추구

- 해킹 기술과 공격도구 경향
  - 공격 도구의 사용 편의성 및 공격 능력 증대
  - 침입자에게 요구되는 지식 감소

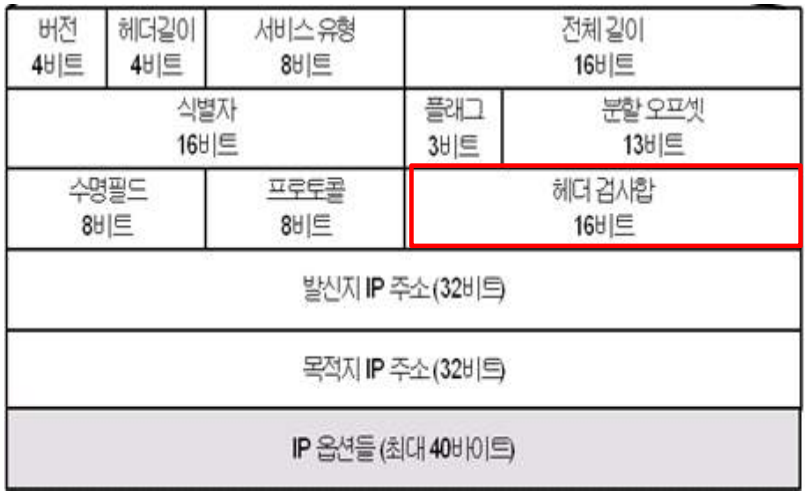


출처 | 카네기 멜론 대학

인터넷 프로토콜의 보안 취약성

- 인터넷 프로토콜은 데이터의 신뢰성 있는 전달을 염두에 두고 설계 → 1970년 대에는 보안이 중요한 고려 대상이 아니었음

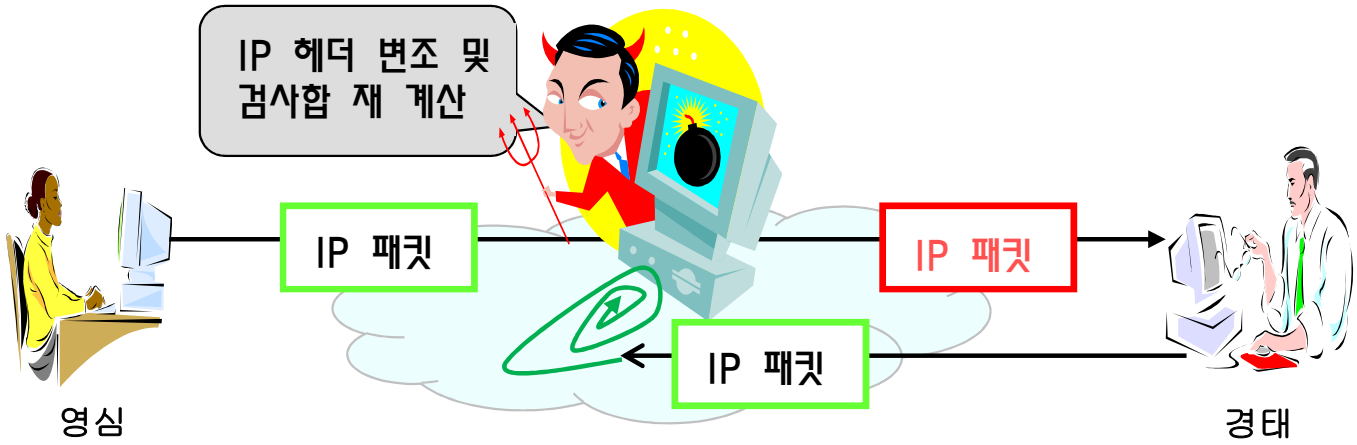
- IP 프로토콜의 보안 취약성
  - IP 주소 및 패킷 내용의 변조 → 헤더 검사합 재계산,
  - 패킷의 재 전송, 패킷 내용의 훔쳐보기, …



- 헤더 검사합 필드
  - IP 헤더의 손상 여부를 검사
  - 계산의 용이성: 16비트의 덧셈 및 보수 계산(각 비트의 1은 0, 0은 1로 변환)

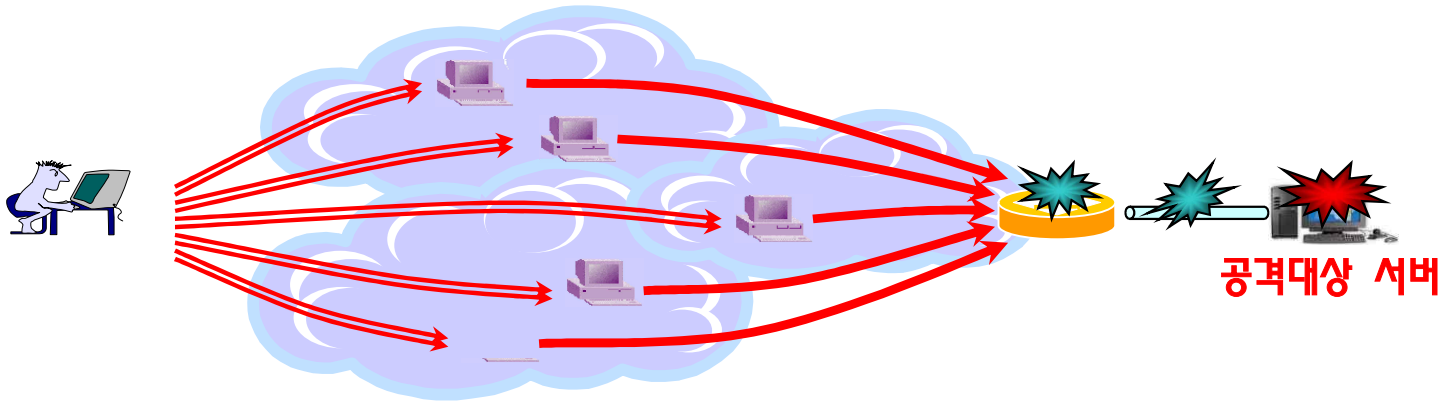
헤더 검사합의 취약성

- 공격자는 영심이가 생성한 IP 패킷(목적지: 경태)을 중간에서 캡쳐
- IP 헤더의 필드(예, 발신지 IP 주소)를 변조 후 헤더 검사합을 다시 계산하여 경태에게 전송
- 경태는 변조된 IP 패킷을 정상적인 것으로 잘못 검증 후 응답 IP 패킷을 전송 함. 응답 패킷은 변조된 IP 패킷의 발신지 주소를 목적지 주소로 사용
- 공격자가 발신지 IP 주소를 변조한 경우 경태가 생성한 IP 패킷은 목적지가 없으므로 네트워크에서 순환하다가 없어 짐



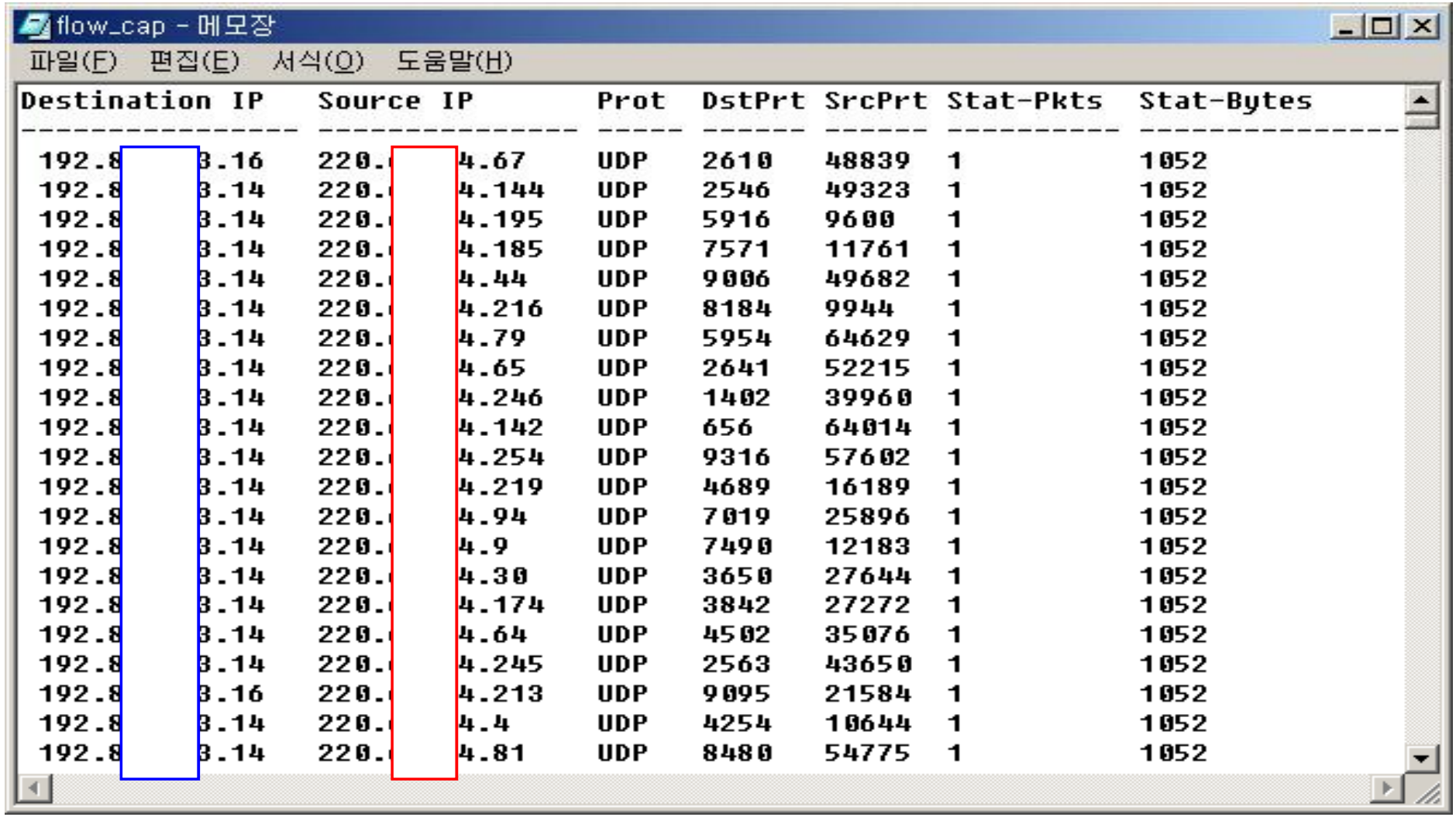
서비스 거부 공격

- 서비스 거부(DOS: Denial of Service) 공격
  - 공격자가 시스템의 자원(예, 메모리, 테이블, 지원하는 연결의 수,…)을 모두 사용하거나 파괴함으로 다른 사용자들이 시스템의 서비스를 더 이상 사용할 수 없도록 만드는 공격
  - 7.7 DDoS(분산 서비스 공격) 대란: 2009년 7월 7일을 기점으로 한국과 미국 등의 주요 정부기관, 포털사이트, 은행 사이트 등의 DDoS 공격으로 서비스의 일시적인 마비 발생



- 헤더 검사합의 취약성을 이용한 서비스 거부 공격
  - 스머프(Smurf) 공격, LAND 공격, UDP 홍수(flood),
  - 동일 착.발신 주소/포트를 갖는 패킷 공격, 과도한 TCP 연결설정(TCP Syn) 공격, …

사례 – IP 주소의 변조에 의한 DoS


flow_cap - 메모장

파일(F) 편집(E) 서식(O) 도움말(H)

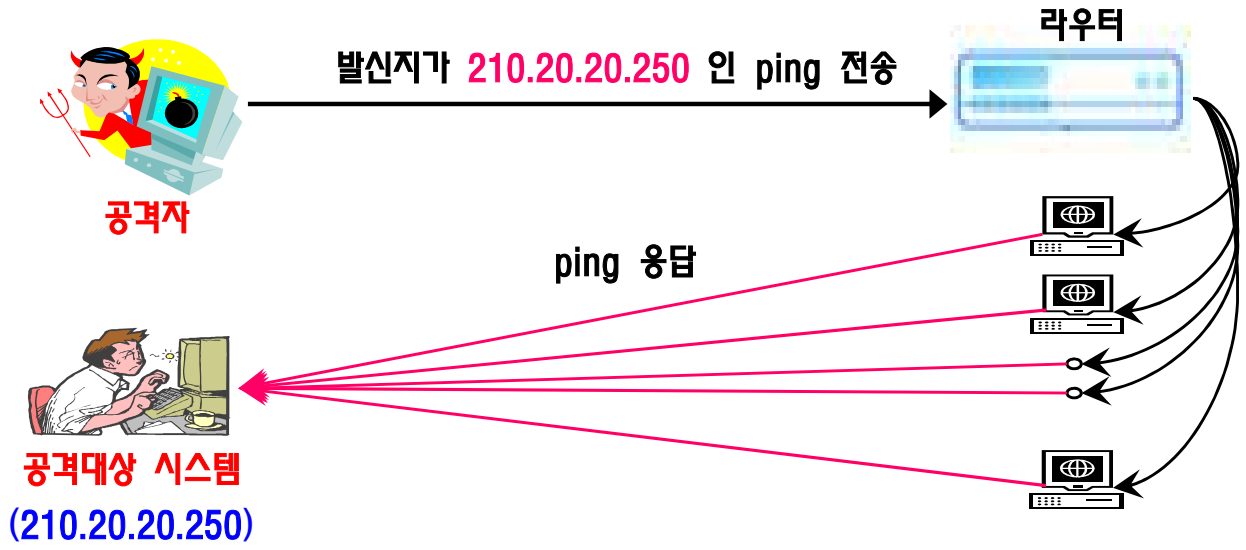
Destination IP	Source IP	Prot	DstPrt	SrcPrt	Stat-Pkts	Stat-Bytes
192.8 3.16	220. 4.67	UDP	2610	48839	1	1052
192.8 3.14	220. 4.144	UDP	2546	49323	1	1052
192.8 3.14	220. 4.195	UDP	5916	9600	1	1052
192.8 3.14	220. 4.185	UDP	7571	11761	1	1052
192.8 3.14	220. 4.44	UDP	9006	49682	1	1052
192.8 3.14	220. 4.216	UDP	8184	9944	1	1052
192.8 3.14	220. 4.79	UDP	5954	64629	1	1052
192.8 3.14	220. 4.65	UDP	2641	52215	1	1052
192.8 3.14	220. 4.246	UDP	1402	39960	1	1052
192.8 3.14	220. 4.142	UDP	656	64014	1	1052
192.8 3.14	220. 4.254	UDP	9316	57602	1	1052
192.8 3.14	220. 4.219	UDP	4689	16189	1	1052
192.8 3.14	220. 4.94	UDP	7019	25896	1	1052
192.8 3.14	220. 4.9	UDP	7490	12183	1	1052
192.8 3.14	220. 4.30	UDP	3650	27644	1	1052
192.8 3.14	220. 4.174	UDP	3842	27272	1	1052
192.8 3.14	220. 4.64	UDP	4502	35076	1	1052
192.8 3.14	220. 4.245	UDP	2563	43650	1	1052
192.8 3.16	220. 4.213	UDP	9095	21584	1	1052
192.8 3.14	220. 4.4	UDP	4254	10644	1	1052
192.8 3.14	220. 4.81	UDP	8480	54775	1	1052

스머프 공격

① 공격자의 ping 전송
- 발신지 IP 주소: 공격대상 시스템의 주소인 210.20.20.250 으로 위장
- 목적지 IP 주소: 공격대상 시스템이 있는 네트워크의 방송 주소

② 공격대상 시스템이 있는 네트워크의 모든 시스템들은 ping 응답을 공격대상 시스템으로 전송

③ 공격대상 시스템은 과도한 ping 응답으로 시스템의 부하 증가 또는 다운



과도한 TCP 연결설정 공격 (1/2)

❑ 연결설정을 위한 TCP의 제어 필드
- 연결설정 요청: SYN 비트
- 연결설정 확인: ACK 비트

❑ TCP의 3단계 핸드세이크 연결 설정

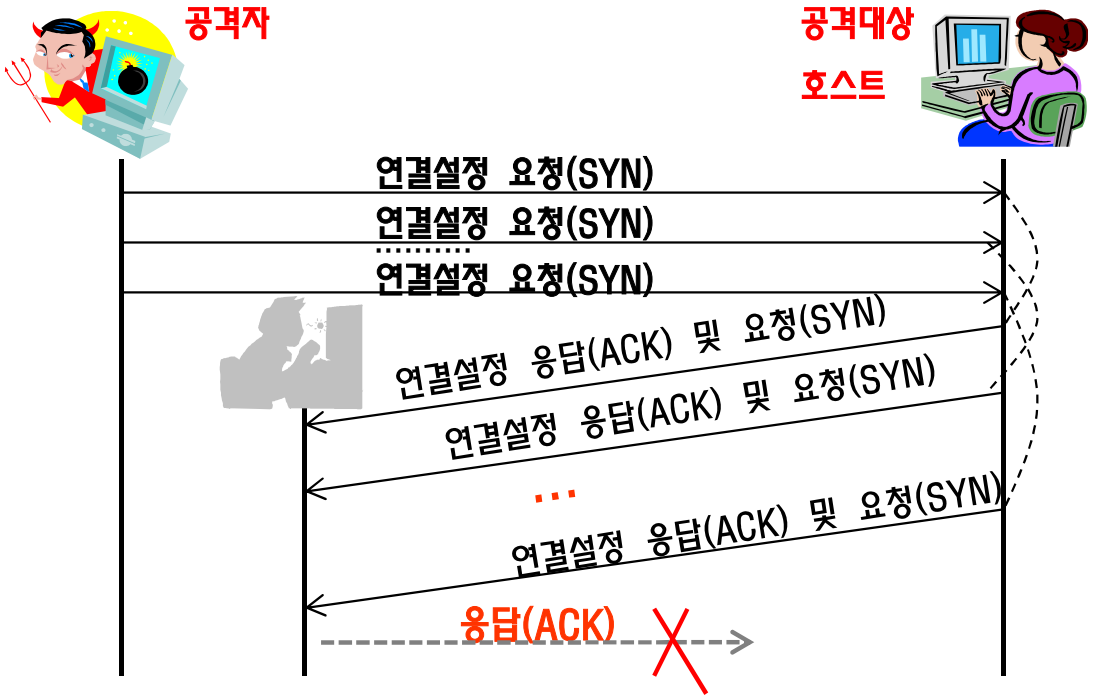
① 호스트-A는 호스트-B로의 데이터 송신을 위하여 TCP 연결설정 요청(SYN) 송신

② 호스트-B는 응답(ACK)을 보내고 호스트-A로의 데이터 송신을 위하여 위하여 연결설정 요청(SYN) 송신

③ 호스트-A는 호스트-B의 연결요청을 응답(ACK) 함으로 양 방향 통신을 위한 연결설정 완료

과도한 TCP 연결설정 공격 (2/2)

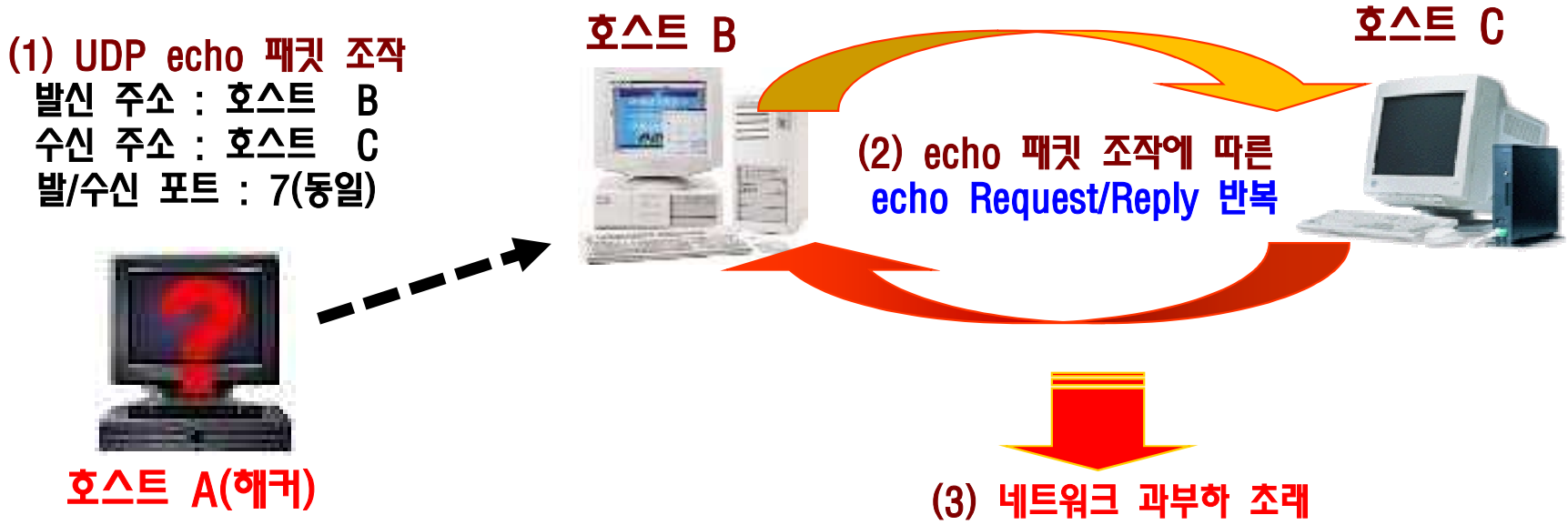
- 공격자는 발신지 IP 주소 위조 → 공격대상 호스트에게 대량의 연결설정(SYN) 요청
- 공격대상 호스트는 존재하지 않는 위조된 IP 주소로 응답(ACK)을 보내고 양방향 통신을 위하여 연결설정(SYN) 요청 → 위조된 IP 주소로 부터 응답(ACK)을 받을 때까지 대기
- 위조된 대량의 연결설정(SYN) 요청 패킷이 수신되면 서버의 대기 큐(Backlog Queue)에 오버플로우 → 서비스거부 상태




```
[root@net /root]# netstat -na|grep SYN
                                                    Local                 Remote
tcp        0      0 127.0.0.1:80                83.232.136.253:1911     SYN_RECV
tcp        0      0 127.0.0.1:80                199.106.229.9:1308      SYN_RECV
tcp        0      0 127.0.0.1:80                1.81.31.169:2051        SYN_RECV
tcp        0      0 127.0.0.1:80                47.95.74.60:1107        SYN_RECV
tcp        0      0 127.0.0.1:80                57.138.85.69:1697       SYN_RECV
tcp        0      0 127.0.0.1:80                54.125.11.117:2433      SYN_RECV
tcp        0      0 127.0.0.1:80                160.187.111.239:2064    SYN_RECV
tcp        0      0 127.0.0.1:80                167.129.136.239:2043    SYN_RECV
tcp        0      0 127.0.0.1:80                47.183.44.170:1256      SYN_RECV
tcp        0      0 127.0.0.1:80                124.215.160.217:1636    SYN_RECV
tcp        0      0 127.0.0.1:80                76.151.250.211:1673     SYN_RECV
tcp        0      0 127.0.0.1:80                95.168.224.46:1986      SYN_RECV
tcp        0      0 127.0.0.1:80                22.249.49.106:1362      SYN_RECV
tcp        0      0 127.0.0.1:80                21.255.176.15:1610      SYN_RECV
tcp        0      0 127.0.0.1:80                50.110.236.208:2272     SYN_RECV
tcp        0      0 127.0.0.1:80                114.218.24.238:1351     SYN_RECV
tcp        0      0 127.0.0.1:80                88.78.25.148:1215       SYN_RECV
```

동일 포트를 갖는 패킷 공격

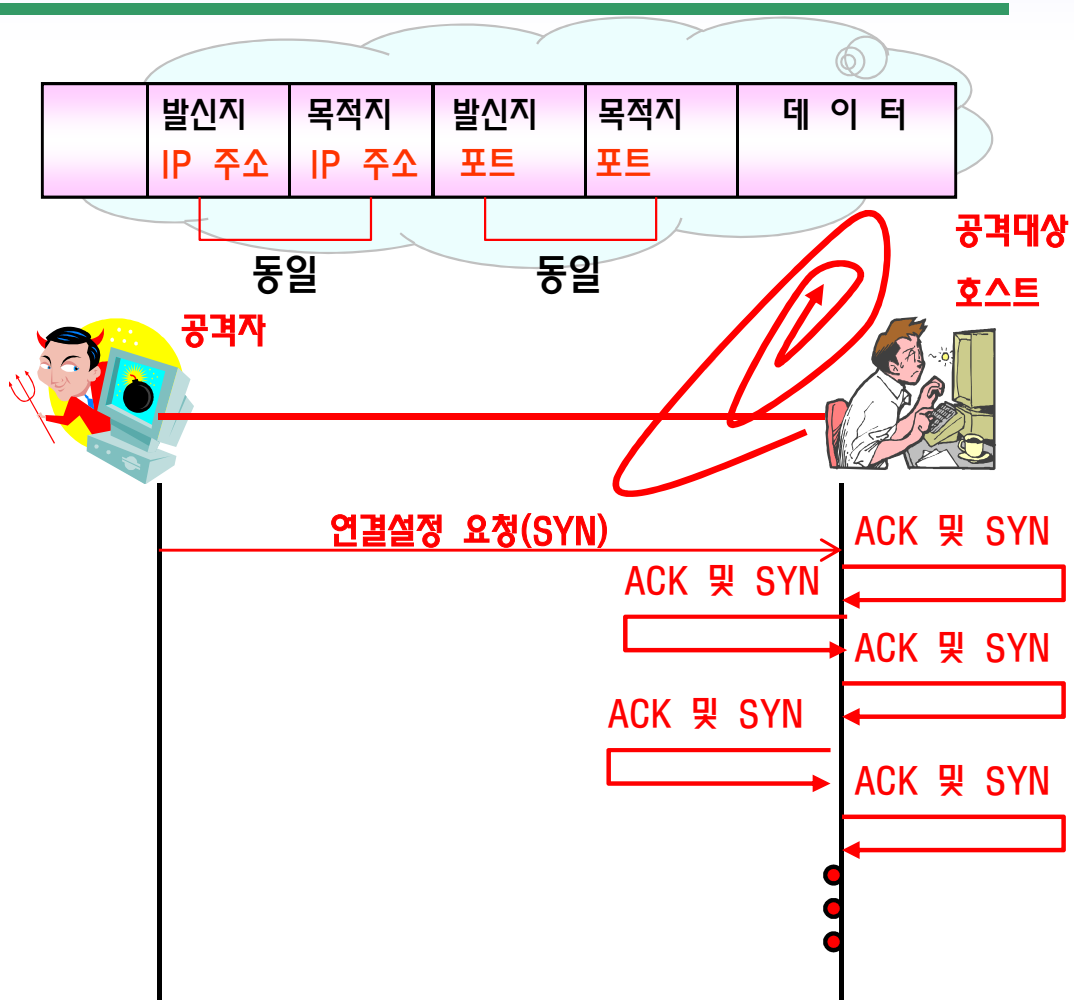
- 공격자-A는 패킷을 위조하여 공격대상 호스트-B로 전송
  - IP 패킷 헤더의 발신지 주소를 호스트-B, 목적지 주소를 호스트-C로 지정
  - UDP 헤더의 발신 및 목적 포트를 동일하게 지정
- 위조된 패킷에 대한 응답 패킷을 생성하여 전송하는 경우 루프 상태에 빠지므로 심각한 네트워크 과부하 유발
  - 응답 패킷은 수신한 패킷의 발신지 주소를 목적지 주소로 사용 함
- 이 공격은 주로 echo와 chargen 서비스를 이용한다.



LAND 공격

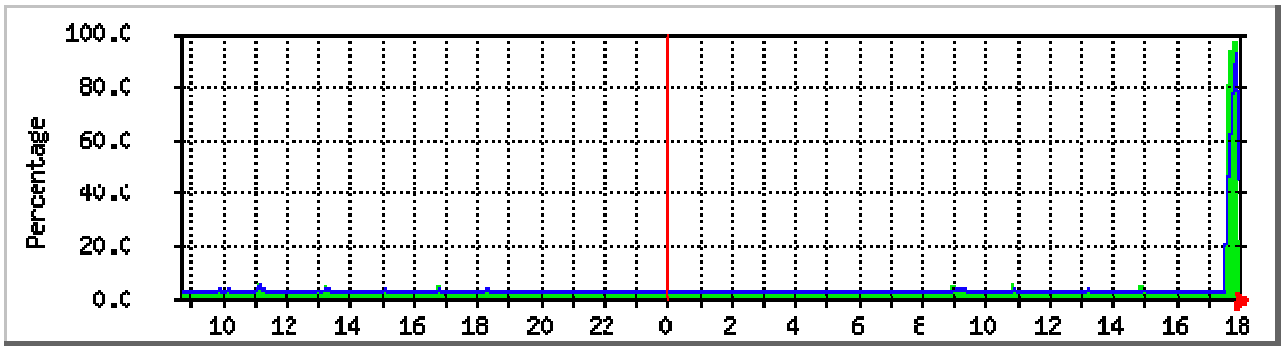
- 공격자가 발신지와 목적지 주소 및 포트 번호를 모두 피해 호스트의 주소로 변조한 TCP SYN 패킷을 전송
  → SYN 패킷의 루프 발생

- 1997년에 나온 고전적인 공격 기법
  - 운영체제의 TCP 스택 결함 패치
  - 라우터나 방화벽 등에서 출발지와 목적지가 동일한 패킷 차단

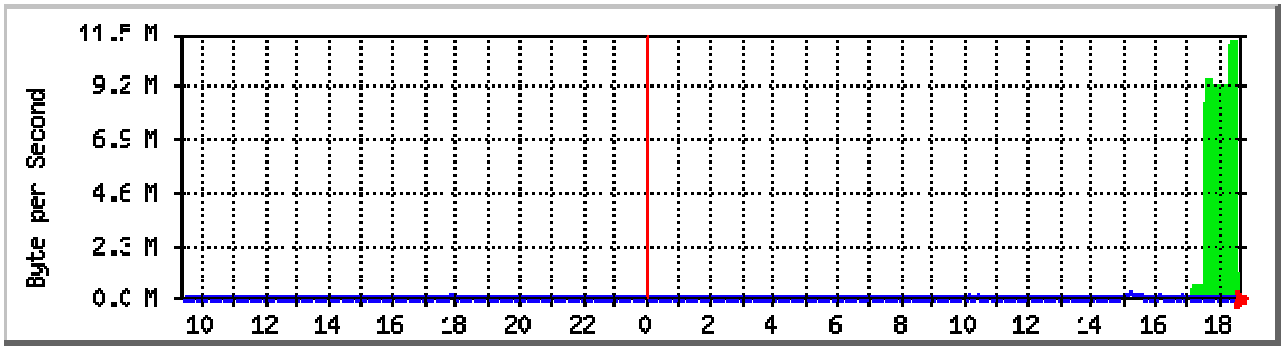


사례 – DoS 공격시의 네트워크과 장비 상태

- 장비의 CPU 사용량 급격히 증가



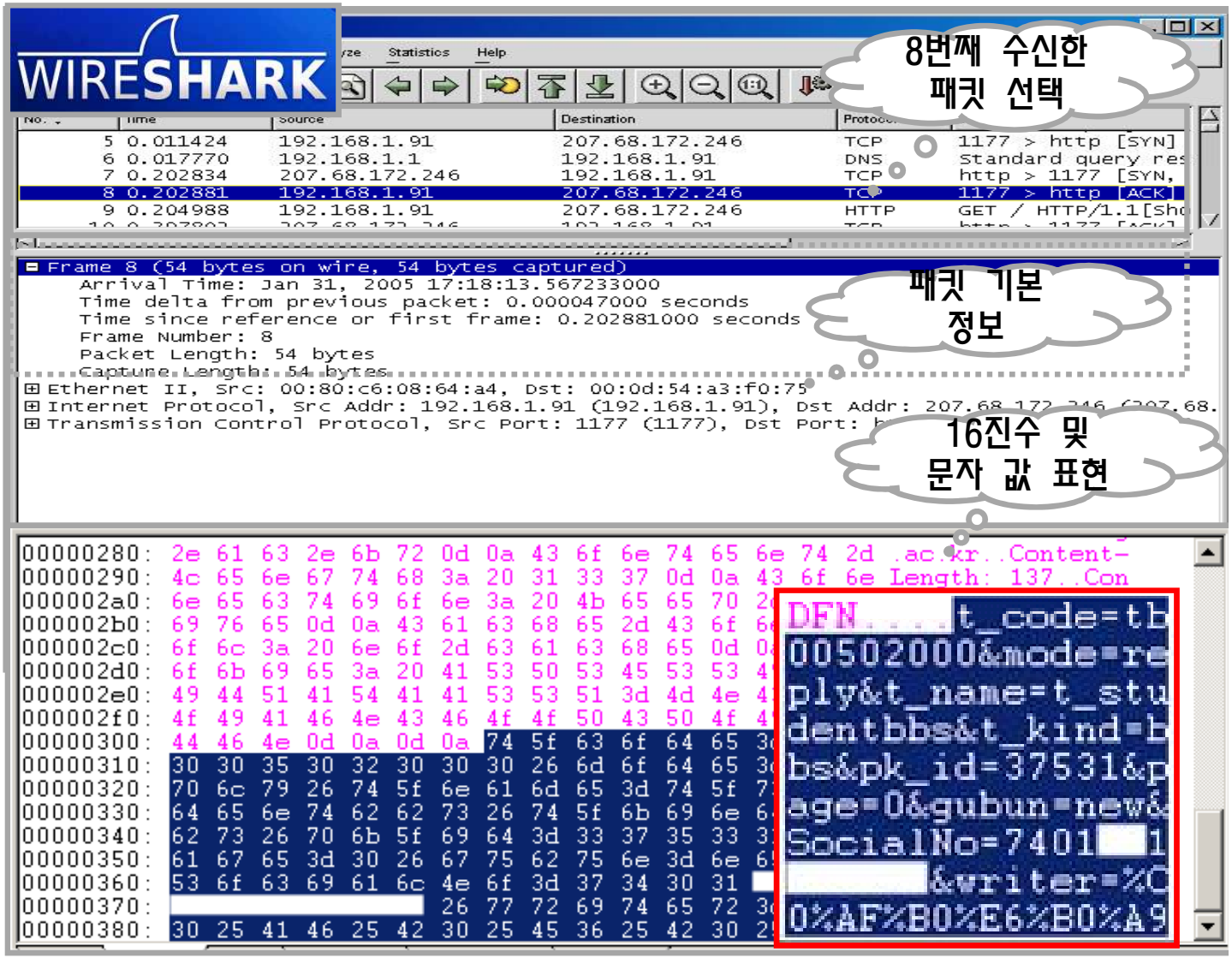
- 네트워크에서 폭주 현상 발생



스니퍼(Sniffer)

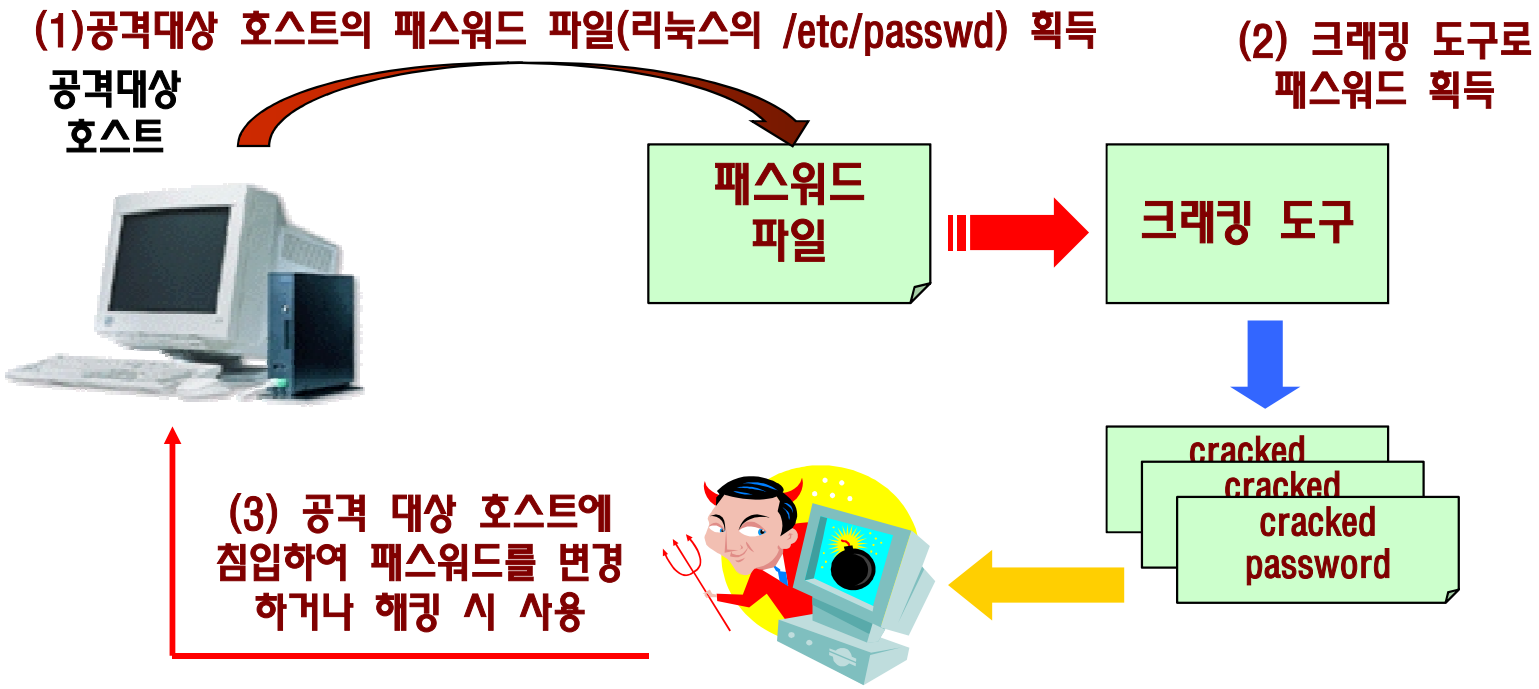
- 네트워크 상의 패킷을 분석하여 다른 사용자들의 중요한 정보를 수집하는 행위

- Wireshark
  - 윈도우 및 리눅스
  - http://www.wireshark.org/
- tcpdump
  - 리눅스
  - http://www.tcpdump.org/



패스워드 크래킹

- 대상 프로그램이나 OS 자체를 크래킹하여 패스워드의 확인 단계를 거치지 않는 방법
- 예상되는 ID와 패스워드 목록을 가지고 패스워드를 크래킹
  - 목록을 가지고 있는 파일을 이용하는 방법(wwwhack)
  - 해킹 공격 프로그램의 소스에 목록이 포함되는 방법
- 패스워드가 저장된 파일을 획득하여 패스워드를 알아내는 방법(Crack)



SSH 서비스에 대한 패스워드 스캔

❑ 취약한 암호를 사용하는 SSH(22/tcp) 서비스에 대한 패스워드 스캔 공격의 사례 보고 (2004년 12월)

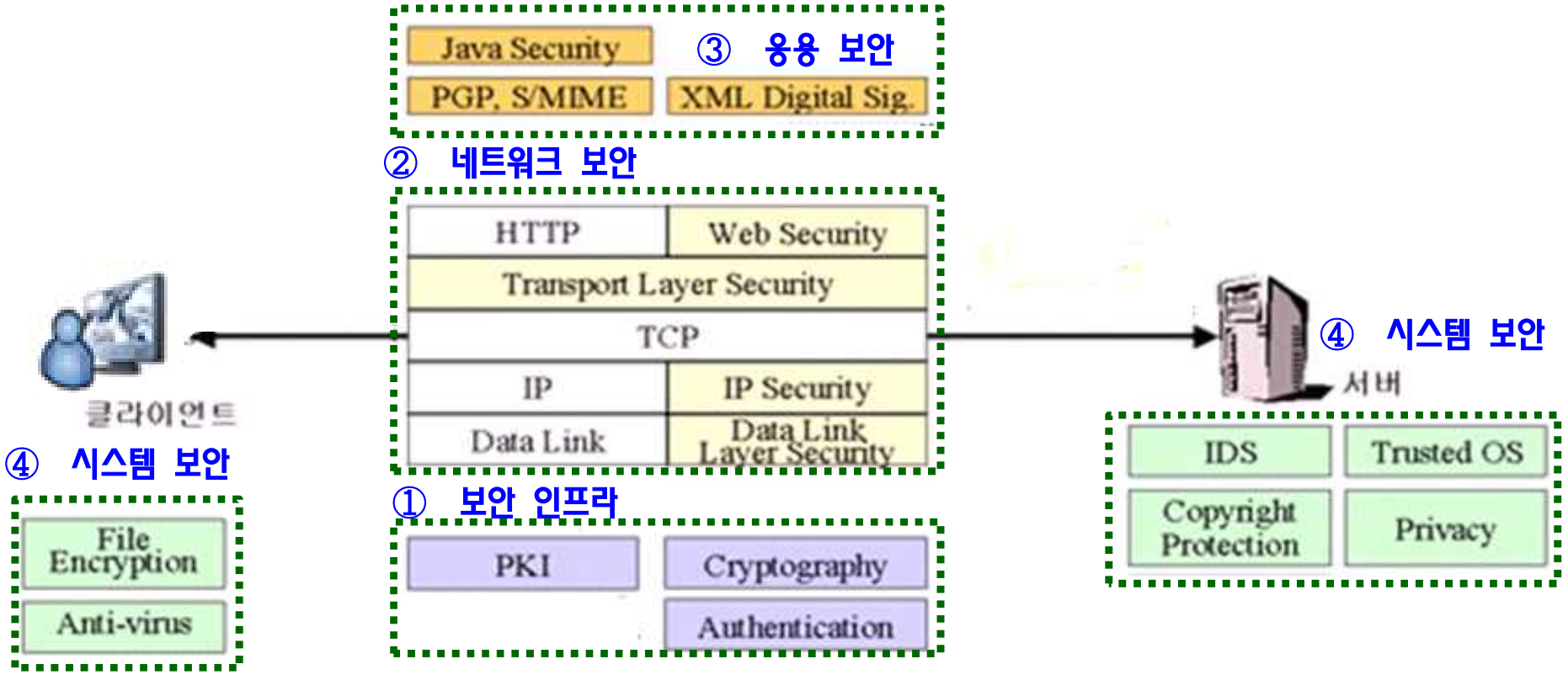
- test, guest, admin, root 사용자에 대해 암호가 없거나 암호가 단순한 계정의 전사적인 접속시도
  21:51:43 services sshd[695]: Illegal user test from xxx.228.156.19
  21:51:44 services sshd[697]: Illegal user guest from xxx.228.156.19
  21:51:46 services sshd[699]: Illegal user admin from xxx.228.156.19
  .....

- 위의 스캔과 관련된 공격코드 중 일부 ☞ 별도의 사전파일을 사용하지 않고 소스에 직접 2,000여개의 암호가 포함되어 있음

```
checkauth("test","test",buff);
checkauth("guest","guest",buff);
checkauth("admin","admins",buff);
checkauth("user","user",buff);
checkauth("root","root",buff);
checkauth("root","123456",buff);
checkauth("test","123456",buff);
checkauth("test","12345",buff);
checkauth("test","1234",buff);
checkauth("test","123",buff);
.....
```

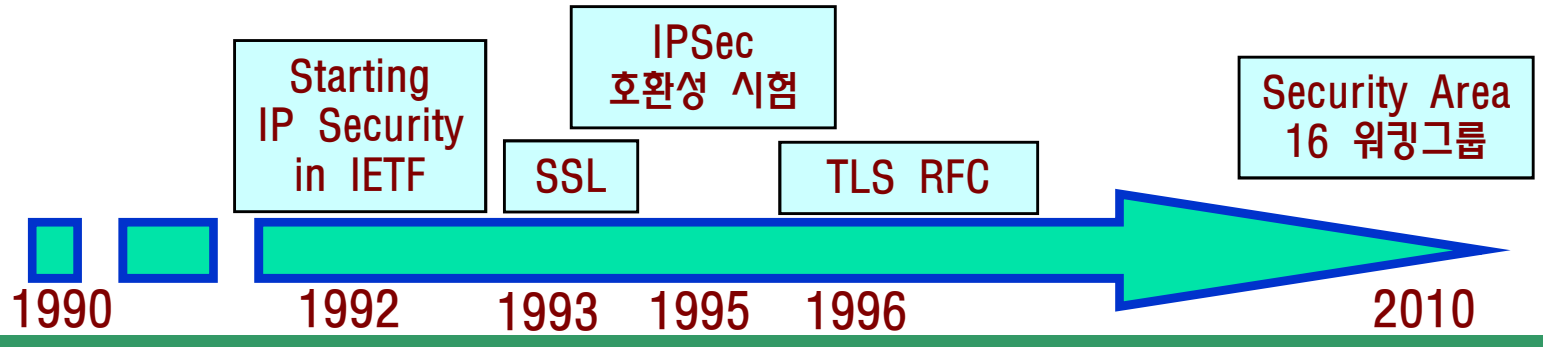
보안기법 계층 구조

- 보안 인프라: PKI(Public Key Infrastructure), 암호학, 전자서명, …
- 네트워크 보안: 웹 보안, SSL/TLS, IP 보안, 데이터링크 보안, …
- 시스템 보안: 파일 암호화, 앤티 바이러스, IDS(침입탐지시스템), 신뢰성 있는 OS…
- 응용 보안: S/MIME(Secure/Multipurpose Internet Mail Extensions), PGP, XML 보안, …



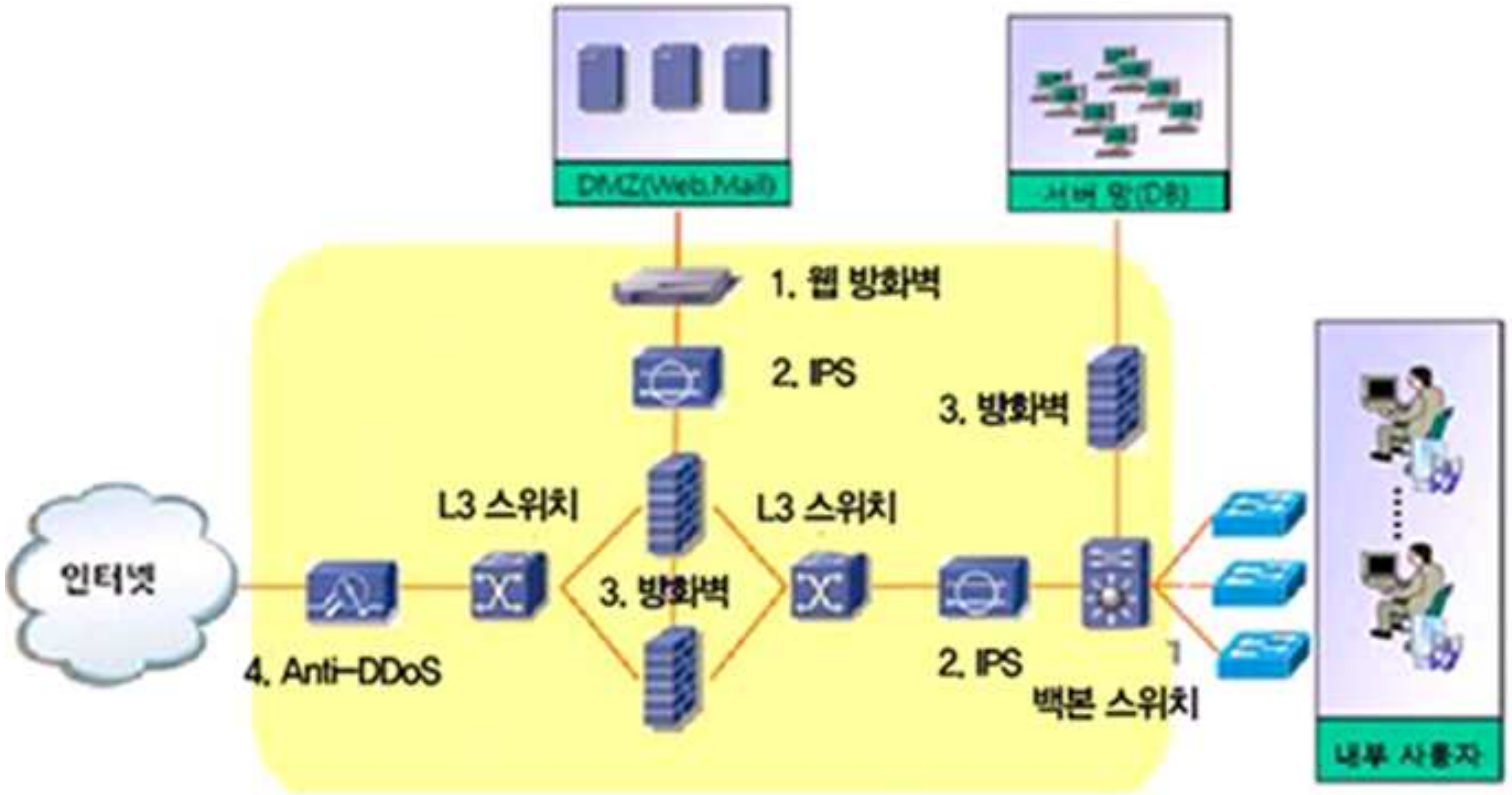
인터넷 보안 프로토콜

- 인터넷 프로토콜의 취약성을 해결하기 위하여 보안 프로토콜 개발
- IP 보안(IPSec)
  - 키관리 프로토콜(ISAKMP)
  - 인증헤더(AH) 프로토콜, 캡슐화 보안 페이로드(ESP) 프로토콜
- SSL(Secure Socket Layer)
  - 1993년 웹 서버와 브라우저 사이의 안전한 통신을 위하여 Netscape 사에서 개발
  - 주요기능: 서버/클라이언트 인증, 기밀성 보장
  - 지원 프로토콜: HTTPS(443), TELNETS(992), POPS(995) 등
- TLS(Transport Layer Security)
  - SSL을 기반으로 1999년 IETF가 TLS 표준화(SSL3.1)



네트워크의 보안 구성 [1/3]

- 내부사용자, DMZ 그리고 서버 망을 같이 보유하고 있는 대다수 사이트의 네트워크 보안 구성(참고: 안철수연구소의 네트워크 보안 Good case Study)
  - ① 웹 방화벽(Web Application Firewall)
  - ② IPS(침입방지시스템)
  - ③ 인터넷 및 서버 망의 방화벽
  - ④ Anti-DDoS(DDoS 대응장비)



네트워크의 보안 구성 [2/3]

❑ 인터넷 및 서버 망의 방화벽

- 계층 3 및 4 레벨에서 동작하며 송수신 되는 패킷의 정상 여부 판단 ➔ 비 정상적인 접근 차단
- 인터넷에 대한 방화벽을 구축하여 외부/DMZ/내부 망의 보안 도메인으로 분리 및 접근제어
- 중요한 정보를 보유하고 있는 서버 망에 별도의 방화벽을 구축하여 외부는 물론 내부 사용자로부터의 불법적 접근 차단 및 네트워크 공격(DDoS)에 대한 방어

❑ 웹 방화벽

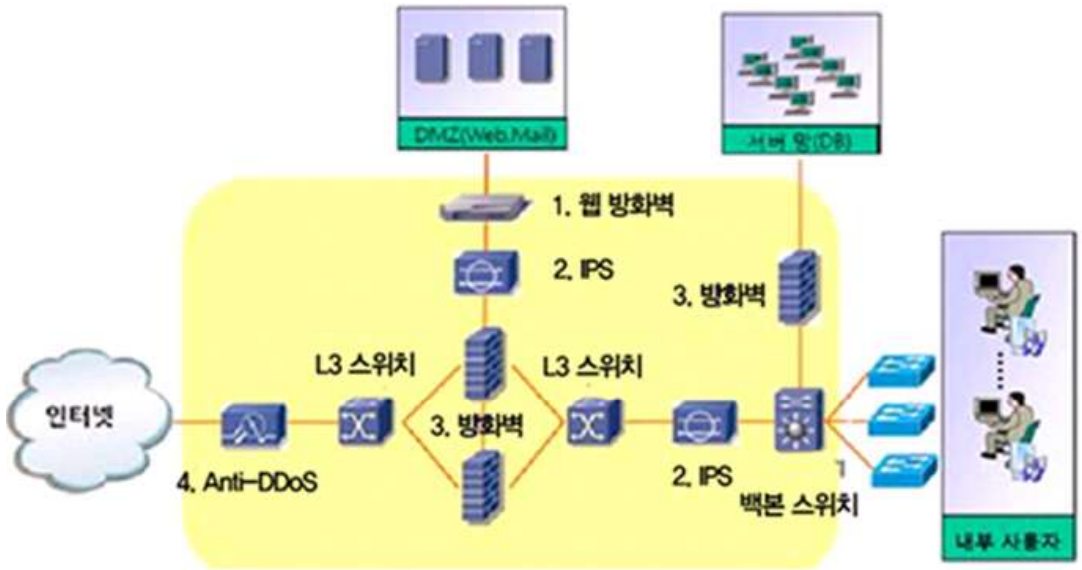
- HTTP와 HTTPS 요청이 있는 응용 계층에서 동작 ➔ 패킷이 아닌 비정상적인 URL과 사용자의 요청(GET, Post...) 차단
- 웹 서버의 주요 정보에 대한 무결성을 검증하므로 공격에 의한 내부 정보의 변조를 방어
- 웹 서비스가 중요한 사이트의 경우 웹 서비스에 특화된 웹 방화벽 구축
  - 공개 웹 방화벽: ModeSecurity(Apache 웹 서버용), WebKnight(IIS 웹 서버용)

```
1  20:08:34 W3S[      ]01 GET /common/Main_LoginChk.asp - 23.[      ].12 HTTP/1.
2  20:08:34 W3S[      ]01 GET /common/Main_LoginChk.asp - 23.[      ].12 HTTP/1.
3  20:08:34 W3S[      ]01 GET /common/Main_LoginChk.asp - 23.[      ].12 HTTP/1.
4  20:08:34 W3S[      ]01 GET /common/Main_LoginChk.asp - 23.[      ].12 HTTP/1.
5  20:08:34 W3S[      ]01 GET /common/Main_LoginChk.asp - 23.[      ].12 HTTP/1.
6  20:08:35 W3S[      ]01 GET /common/Main_LoginChk.asp - 23.[      ].12 HTTP/1.
7  20:08:35 W3S[      ]01 GET /common/Main_LoginChk.asp - 23.[      ].12 HTTP/1.
8  20:08:35 W3S[      ]01 GET /common/Main_LoginChk.asp - 23.[      ].12 HTTP/1.
9  20:08:35 W3S[      ]01 GET /common/Main_LoginChk.asp - 23.[      ].12 HTTP/1.
10 20:08:35 W3S[      ]01 GET /common/Main_LoginChk.asp - 23.[      ].12 HTTP/1.
11 20:08:35 W3S[      ]01 GET /common/Main_LoginChk.asp - 23.[      ].12 HTTP/1.
12 20:08:35 W3S[      ]01 GET /common/Main_LoginChk.asp - 23.[      ].12 HTTP/1.
13 20:08:35 W3S[      ]01 GET /common/Main_LoginChk.asp - 23.[      ].12 HTTP/1.
```

네트워크의 보안 구성 [3/3]

❑ IPS(침입방지시스템)

- DMZ 망의 IPS: 네트워크 방화벽에서 허용되는 웹 및 메일 등의 트래픽을 심층적으로 분석하여 악성코드/해킹 차단
- 내부 망에 설치된 IPS: 내부 사용자가 외부의 악성코드 유포 사이트를 통해 다운받은 악성코드 차단 및 내부 사용자 PC에서 외부로 정보를 유출시키는 스파이웨어 트래픽 차단



❑ DDoS 대응장비

- 근래에 무분별하게 발생하고 있는 DDoS 공격의 효과적인 방어를 위하여 외부에서 사이트로 접근하는 최전방에 설치

요점 정리(1/2)

- 인터넷은 "정보의 바다"라 불리는 컴퓨터 통신망으로, TCP/IP 프로토콜을 이용해 정보를 주고받는 공개 컴퓨터 통신망
  - 5 계층 모델:응용계층, 전송계층, 네트워크 계층, 데이터링크 계층, 물리계층
- 네트워크 보안: 각종 위협적인 공격 요소로부터 네트워크 장비, 서버, 운영 체제, 응용 프로그램, 사용자 정보 등을 안전하게 보호하는 것
- 인터넷 프로토콜은 데이터의 신뢰성 있는 전달을 염두에 두고 설계 → 1970년 대에는 보안이 중요한 고려 대상이 아니었음
  - IP 프로토콜의 보안 취약성: IP 주소 및 패킷 내용의 변조, 패킷의 재 전송, 패킷 내용의 훔쳐보기, 인터넷 전화의 도청
- 헤더 검사합의 취약성을 이용한 서비스 거부 공격
  - 스머프(Smurf) 공격, 동일 착.발신 주소/포트를 갖는 패킷 공격(LAND 공격, UDP 홍수), 과도한 TCP 연결설정(TCP Syn) 공격, …

요점 정리(2/2)

- 스니퍼: 네트워크 상의 패킷을 분석하여 다른 사용자들의 중요 정보를 수집하는 행위
  - Wireshark, tcpdump, …
- 패스워드 크래킹
  - 예상되는 ID와 패스워드 목록을 가지고 패스워드를 크래킹
  - 패스워드가 저장된 파일을 획득하여 패스워드를 크래킹
- 보안기법의 계층 구조
  - 응용 보안: S/MIME(Secure/Multipurpose Internet Mail Extensions), PGP, XML 보안, …
  - 네트워크 보안: 웹 보안, SSL/TLS, IP 보안, 데이터링크 보안, …
  - 시스템 보안: 파일 암호화, 앤티 바이러스, IDS(침입탐지시스템), …
  - 보안 인프라: PKI(Public Key Infrastructure), 암호학, 전자서명, 스마트 카드, …
- 내부사용자, DMZ 그리고 서버 망을 보유하고 있는 사이트의 네트워크 보안 구성
  - 네트워크 방화벽, IPS(침입방지시스템)
  - 웹 방화벽(Web Application Firewall), DDoS 대응장비