소프트웨어 개발 보안 구축 - 보안용어	
IDS (Intrusion Detection System, 침입 탐지 시스템)	정보시스템의 보안을 위협하는 침입행위가 발생할 경우 이를 탐지, 적극 대응하기 위한 시스템이다.
DMZ (비무장지대)	( ) 솔루션은 내부 네트워크와 외부 사이에 위치하며 외부 인터넷에 서비스를 제공하는 서버를 위치시키기에 가장 적합한 장소다. ( )에 위치하는 시스템으로는 웹서버, FTP 서버 등이 있다.
DLP (Data Loss Prevention, 데이터 유출 방지)	기업 내부자의 고의나 실수로 인한 외부로의 정보 유출을 방지하는 솔루션
웹 방화벽 (Web Firewall)	일반 방화벽이 탐지하지 못하는 SQL 삽입 공격, Cross-Site Scripting(XSS) 등의 웹 기반 공격을 방어
Anti-DDoS	DDos 차단 보안 솔루션
VPN (Virtual Private Network, 가상 사설망)	인터넷망과 같은 공중망을 사설망처럼 이용해 회선 비용을 크게 절감할 수 있는 기업통신 서비스. 인터넷망을 전용선처럼 사용할 수 있도록 특수통신체계와 암호화기법을 제공하는 서비스로 기업 본사와 지사 또는 지사간에 전용망을 설치한 것과 같은 효과를 거둘 수 있으며, 전용선에 비해 20~80% 이상의 비용을 줄일 수 있다.
NAC (Network Access Control, 네트워크 접근 제어)	사전에 인가하지 않은 누리꾼이나 보안 체계를 갖추지 않은 정보기기의 통신망(네트워크) 접속을 적절히 조절하는 일 또는 솔루션.
UTM (Unified Threat Management, 통합 위협 관리)	침입 차단 시스템, 가상 사설망 등 다양한 보안 솔루션 기능을 하나로 통합한 보안 솔루션. 보안 솔루션은 그 목적에 따라 방화벽, 침입 탐지시스템(IDS: Intrusion Detection System), 침입 방지 시스템(IPS: Intrusion Prevention System), 가상 사설망(VPN: Virtual Private Network), 데이터베이스 보안, 웹 보안, 콘텐츠 보안 등 다양한 솔루션 형태로 분화, 발전되어 왔으나 그 결과 각각의 보안 솔루션 운용 방법을 익히기 위한 시간 비용, 그리고 운용을 위한 물리적 공간과 인력 확보가 요구되었다. 통합 위협 관리(UTM)는 다양한 보안 솔루션을 하나로 묶어 비용을 절감하고 관리의 복잡성을 최소화하며, 복합적인 위협 요소를 효율적으로 방어할 수 있다.
ESM (Enterprise Security Management 기업 보안 관리)	방화벽, 침입 탐지 시스템, 가상 사설망 등의 보안 솔루션을 하나로 모은 통합 보안 관리 시스템.
DoS (서비스 거부 공격, Denial Of Service)	정보 시스템의 데이터나 자원을 정당한 사용자가 적절한 대기 시간 내에 사용하는 것을 방해하는 행위. 주로 시스템에 과도한 부하를 일으켜 정보 시스템의 사용을 방해하는 공격 방식이다.
죽음의 핑 (Ping of Death)	인터넷 프로토콜 허용 범위(65,536 바이트) 이상의 큰 패킷을 고의로 전송하여 발생한 서비스 거부(DoS) 공격.

SYN Flooding (SYN 플러딩)	대량의 SYN(동기 제어 문자, 접속할 때 사용하는 패킷) packet을 이용해서 타켓 서버의 서비스를 더 이상 사용할 수 없도록 만드는 공격 기법
TCP 3-way handshaking	신뢰성 있는 연결을 위해 송신지 외 수신지 간의 통신에 앞서 3단계에 걸친 확인 작업을 수행한 후 통신
handshaking(악수, 주고받기)	데이터를 전송할 때에, 두 장치 간에 동기를 맞추기 위하여 일련의 신호를 주고받는 것
스머핑 (Smurfing)	고성능 컴퓨터를 이용해 초당 엄청난 양의 접속신호를 한 사이트에 집중적으로 보냄으로써 상대 컴퓨터의 서버를 접속 불능 상태로 만들어 버리는 해킹 수법 (IP, ICMP 특성 악용)
ICMP(Internet Control Message Protocol)	서버와 게이트웨이 사이에서 메시지를 제어하고 알려주는 프로토콜
LAND 공격 (Local Area Network Denial Attack)	공격자가 패킷의 출발지 주소(Address)나 포트(port)를 임의로 변경하여 출발지와 목적지 주소(또는 포트)를 동일하게 함(무한 응답)
TearDrop 공격	패킷 제어 로직을 악용하여 시스템의 자원을 고갈시키는 공격으로 데이터의 송/수신 과정에서 패킷의 크기가 커 여러 개로 분할되어 전송될 때 분할 순서를 알 수 있도록 Fragment Offset 값을 함께 전송하는데, 이 값을 변경시켜 수신 측에서 패킷 재조립시 과부하가 발생하도록 공격.
SNMP(Simple Network Management Protocol, 간이 망 관리 프로토콜)	네트워크 장비를 관리 감시하기 위한 목적으로 UDP 상에 정의된 응용 계층 표준 프로토콜
TCP(Transmission Control Protocol, 전송 제어 프로토콜)	OSI 기본 참조 모델을 기준으로 제4계층(전송 계층)에 해당되는 프로토콜. 패킷의 도착 순서대로 배열이나 오류 수정 등이 행해지므로 ( )보다 상위층에서 보았을 때는 2대의 컴퓨터가 신뢰성이 높은 전용선으로 연결된 것같이 보인다.
UDP(User Datagram Protocol, 사용자 데이터그램 프로토콜)	인터넷의 표준 프로토콜 집합인 TCP/IP의 기반이 되는 프로토콜의 하나. TCP/IP에서는 망 계층(OSI의 제3계층에 해당) 프로토콜인 IP와 전송 계층(OSI의 제4계층에 해당) 프로토콜인 전송 제어 프로토콜(TCP) 또는 사용자 ( )의 어느 하나를 조합하여 데이터를 주고받는다. TCP에서는 세션(접속)을 설정한 후에 통신을 개시하지만, ( )에서는 세션을 설정하지 않고 데이터를 상대의 주소로 송출한다. ( )의 특징은 프로토콜 처리가 고속이라는 점이다. 그러나 TCP와 같이 오류 정정이나 재송신 기능은 없다. 신뢰성보다도 고속성이 요구되는 멀티미디어 응용 등에서 일부 사용된다.

IP(Internet Protocol, 인터넷 프로토콜)	OSI 기본 참조 모델을 기준으로 하면 제3계층(네트워크 계층)에 해당되는 프로토콜. ( ) 주소에 따라 다른 네트워크 간 패킷의 전송, 즉 경로 제어를 위한 규약으로 다른 네트워크 간의 데이터 전송을 가능하게 하는 것이 이 프로토콜의 특징이다. 그러나 패킷이 발신된 순서대로 도착하는 것은 보증하지 않는다. 전송 제어 프로토콜(TCP) 또는 사용자 데이터그램 프로토콜(UDP)과 함께 사용한다.
ICMP(Internet Control Message Protocol, 인터넷 제어 메시지 프로토콜)	TCP/IP에서 신뢰성 없는 IP를 대신하여 송신측으로 네트워크의 IP 상태 및 에러 메시지를 전달해주는 프로토콜
IGMP(Internet Group Management Protocol, 멀티 캐스트 라우팅)	로컬 네트워크 상에서 라우터와 호스트 간의 멀티캐스트(1:다) 환경을 제공
HDLC	비트 위주 데이터 링크 제어 프로토콜
X.25	패킷 전송을 위한 DTE/DCE 접속 규격
RS-232C	DTE와 DCE를 상호 접속하는 물리적 인터페이스
ARQ(Automatic Repeat reQuest, 자동 반복 요청)	통신 경로에서 오류 발생 시 수신측은 오류의 발생을 송신측에 통보하고 송신측은 오류가 발생한 프레임을 재전송하는 오류 제어 방식
정지-대기(Stop-and-Wait) ARQ	송신측은 하나의 블록을 전송한 후 수신측에서 에러의 발생을 점검한 다음, 에러 발생 유무 신호 (긍정 : ACK, 부정 : NAK)를 보내올 때까지 기다리는 방식
Go-Back-N ARQ	여러 블록을 연속적(continuous)으로 전송하고 부정 응답(NAK) 이후 모든 블록을 재전송
Selective-Repeat ARQ (선택적 재전송)	여러 블록을 연속적으로 전송하고 부정 응답(NAK)이 있던 블록만 재전송
ITU	국제전기통신연합의 약칭으로 국제 간 통신규격을 제정
X.20	비동기식 전송을 위한 DTE(단말장치:데이터 입/출력)/DCE(신호변환장치, 전송장치, 회선 종단장치, ex. MODEM) 접속 규격
Multicast	인터넷상에서 같은 내용의 전자메일, 화상회의를 위한 화상, 음성 데이터 등을 둘 이상의 다른 수신자들에게 동시에 전송하는 방식이다. 특정한 한 사람의 수신자에게만 데이터 패킷을 전송하는 방식인 유니캐스트와 대응하는 개념이다.
IPv6 (Internet protocol version 6)	IPv4의 주소공간을 4배 확장한 128 비트 인터넷 주소 체계
Unicast	한 호스트에서 다른 호스트로 또는 단일 메시지가 단일 네트워크 목적지로 보내지는 1:1 전송 방식

Broadcast	다수의 국으로 동시에 정보를 보내는 것을 말한다. 동보 메시지는 다중점 회선상의 모든 국에 자발적으로 송신하는 메시지이다.
Anycast	IPv6에서 Broadcast 가 없어지고, 생김. 수신자들을 묶어 하나의 그룹으로 나타낸 주소를 사용하여 그룹 내에서 가장 가까운 호스트에게만 전송하는 것 (1:1)
DDos (Distributed Denial of Service attack, 분산 서비스 거부 공격)	감염된 대량의 숙주 컴퓨터를 이용해 특정 시스템을 마비시키는 사이버 공격. 공격자는 다양한 방법으로 일반 컴퓨터를 감염시켜 공격 대상의 시스템에 다량의 패킷이 무차별로 보내지도록 조정한다. 이로 인해 공격 대상 시스템은 성능이 저하되거나 마비된다.
피싱 (Phishing)	개인 정보(private data)와 낚시(fishing)의 합성어로 낚시하듯이 개인 정보를 몰래 빼내는 것
큐싱 (Qshing)	QR코드와 피싱(Phishing)의 합성어로 QR코드를 이용한 해킹
스미싱 (SMishing)	SMS와 Phishing의 결합어로 문자메시지를 이용 피싱하는 방법
스피어 피싱 (spear phishing)	조직 내에 신뢰할 만한 발신인으로 위장해 ID 및 패스워드 정보를 요구하는 일종의 피싱 공격
APT (Advanced Persistent Threat, 지능형 지속 공격)	다양한 IT 기술과 방식들을 이용해 조직적으로 특정 기업이나 조직 네트워크에 침투해 활동 거점을 마련한 뒤 때를 기다리면서 보안을 무력화시키고 정보를 수집한 다음 외부로 빼돌리는 형태의 공격을 말한다.
스턱스넷 (stuxnet)	독일 지멘스사의 원격 감시 제어 시스템(SCADA)의 제어 소프트웨어에 침투하여 시스템을 마비하게 하는 바이러스. 원자력 발전소와 송·배전망, 화학 공장, 송유·가스관과 같은 산업 기반 시설에 사용되는 제어 시스템에 침투하여 오동작을 유도하는 명령 코드를 입력해서 시스템을 마비하게 하는 악성 코드이다.
SQL 주입 공격 (SQL injection)	웹 클라이언트의 반환 메시지를 이용하여 불법 인증 및 정보를 유출하는 공격. 웹 응용 프로그램에 강제로 SQL 구문을 삽입하여 내부 데이터베이스(DB) 서버의 데이터를 유출 및 변조하고 관리자 인증을 우회할 수도 있다.
무작위 대입 공격 (brute force attack, 브루트 포스 공격)	조합 가능한 모든 경우의 수를 다 대입해보는 공격
제로 데이 공격 (Zero day attack)	시스템의 보안 취약점이 발견된 상태에서 이를 보완할 수 있는 보안패치가 발표되기 전에 해당 취약점을 이용해 이뤄지는 해킹이나 악성코드 공격. 공격의 신속성을 나타내는 의미로 제로 데이(Zero-day)라는 말이 붙었다.
랜섬웨어 (Ransomware)	인터넷 사용자의 컴퓨터에 잠입해 내부 문서나 스프레트시트, 그림 파일 등을 암호화해 열지 못하도록 만든 후 돈을 보내주면 해독용 열쇠 프로그램을 전송해 준다며 금품을 요구하는 악성 프로그램. ransom(몸값)과 ware(제품)의 합성어로 컴퓨터 사용자의 문서를 '인질'로 잡고 돈을 요구한다고 해서 붙여진 명칭이다.

트랩도어 (Trap Door) 또는 백 도어 (back door)	시스템 보안이 제거된 비밀 통로로, 서비스 기술자나 유지 보수 프로그램 작성자의 액세스 편의를 위해 시스템 설계자가 고의로 만들어 놓은 시스템의 보안 구멍
웜 바이러스 (Worm virus)	'컴퓨터에 근거지를 둔 지렁이와 같은 기생충'이란 의미. 보통 'worm'이라고 한다. 컴퓨터 바이러스와 달리 다른 프로그램을 감염시키지 않고 자기 자신을 복제하면서 통신망 등을 통해서 널리 퍼진다.
키로거 공격 (Key Logger Attack)	컴퓨터 사용자의 키보드 움직임을 탐지해 ID나 패스워드, 계좌 번호, 카드 번호 등과 같은 개인의 중요한 정보를 몰래 빼 가는 해킹 공격
스니핑 (Sniffing)	네트워크의 중간에서 남의 패킷 정보를 도청하는 해킹 유형의 하나
스누핑 (Snooping)	네트워크상에서 남의 정보를 염탐하여 불법으로 가로채는 행위
스푸핑 (Spoofing)	승인받은 사용자인 것처럼 속이는 것
스위치 재밍 (Switch Jamming)	위조된 매체 접근 제어(MAC) 주소를 지속적으로 네트워크로 흘려 보내 스위치 저장 기능을 혼란시켜 더미 허브(dummy hub)처럼 작동토록하는 공격. 스위치를 직접 공격하며, MAC 테이블을 위한 캐시 공간에 버퍼 오버플로 공격을 실시하는 것과 같다.
더미 허브 (Dummy Hub)	단순히 네트워크나 네트워크 장비들과의 연결과 신호 증폭 기능만을 가진 허브. 포트 수만큼 연결을 하며 노드가 증가될수록 네트워크의 속도가 저하되는 단점이 있다. 예를 들어 10Mbps의 대역폭을 가지는 더미 허브에 5대의 컴퓨터를 전체의 대역폭을 나누어 사용하는 방식