알아두면 쓸모 있는 신비한 사이버보안

보충교재: 초급역량

-

목차

정보보안 학습을 위한 기초 용어 정리

정보보안 학습을 위한 기초 용어 정리

- **ARP 스푸핑 (Address Resolution Protocol Spoofing)**

  동일 네트워크에 존재하는 공격 대상 PC의 IP 주소를 공격자 자신의 랜카드 주소와 연결해 다른 PC에 전달 돼야 하는 정보를 가로채는 공격을 말한다. 어떤 PC에 ARP 스푸핑 기능을 가진 악성코드가 설치되면 약간의 조작으로 동일 구역 내의 다른 PC에 쉽게 악성코드를 설치할 수 있다. 즉, 동일 네트워크 하의 PC가 외부 네트워크로 접속을 시도할 경우 악성코드에 감염된 PC를 경유해서 접속 함으로써 해당 악성코드에 자동으로 감염되게 되는 것이다. 또한 동일 네트워크 하의 모든 PC가 감염된 PC를 게이트웨이로 인식해 외부 네트워크와 통신하기 위해 발생하는 모든 패킷을 해당 PC에 전송하므로 네트워크 속도가 크게 느려진다.

- **COM(Component Object Model) 후킹 (Component Object Model Hooking)**

  COM(Component Object Model)은 마이크로소프트사가 책정한 통신 규약으로 거의 모든 마이크로소프트 제품들 간의 근간 기술이다. 인터넷 익스플로러나 탐색기 프로그램 등의 가장 하부에 위치해 있고 응용 프로그램 간 자료 공유 등을 위한 공통 인터페이스를 제공한다. 이러한 COM 인터페이스를 후킹해 사용자가 입력한 계좌 정보 등을 변조할 수 있다.

- **DMZ구간 (DMZ zone)**

  군사용어인 비무장 지대와 비슷한 개념으로, 내부 네트워크에 포함되어 있으나, 외부에서 접근할 수 있는 구간을 지칭하는 네트워크 디자인 개념. 일반적으로 인터넷을 통해 외부에 서비스를 제공해야 하는 웹 및 메일 서버 등이 위치하는 구간을 지칭하며, 정보보안 강화를 위해 방화벽을 이용하여 내부망과 분리되도록 구성

- **IP/Port (IP/Port)**

  TCP/IP 프로토콜상에서 네트워크계층의 IP address(예:100.100.100.100) 및 전송계층의 service port(예: HTTP – 80) 정보

- **RSA 알고리즘 (RSA Algorithm)**

  RSA 알고리즘은 비대칭형 공개키 암호화 체계의 알고리즘을 말하는데 1977년 이를 발명한 MIT대학의 교수 'Rivest', 'Shamir', 'Alderman'의 이름을 따서 만들어진 이름이다.

  RSA 알고리즘은 가장 보편적으로 사용되는 암호화 및 인증 알고리즘으로서 넷스케이프와 마이크로소프트 웹브라우저, 노츠 등의 제품에 채용되어 있다. RSA 알고리즘은 대형 소수의 곱으로 이루어진 숫자의 소인수분해가 매우 어렵다는 전제에 따라 결정되는 공개키 암호 체계를 따른다.

- **SQL 인젝션(Injection) (SQL Injection)**

  웹 페이지의 입력 값을 통해서 SQL명령어를 주입하고 관리자 또는 기타 다른 계정으로 접근하여 DB조작 등을 하는 해킹방법을 말한다.

- **가로채기 (Interception)**

  보안공격의 하나로 인가 받지 않은 자들의 불법적인 접근에 의한 신뢰성에 대한 공격이다.

- **가상 사설망 (VPN [Virtual Private Network])**

  VPN은 Virtual Private Network(가상사설망)란 의미 그대로 공중 데이터 통신망을 사용자가 마치 자신이 구축한 개인 통신망과 같이 직접 운용, 관리할 수 있게 한 네트워크 아키텍처를 말한다. 이 같은 특징으로 사용자들은 공중 통신망을 회사의 전용회선처럼 이용할 수 있게 된다. 이처럼 전용회선 비용보다 훨씬 저렴한 비용으로 원거리 통신망을 가능하게 하기에 점차 이용이 늘고 있다. 그러나 VPN은 개방된 망을 사용하기 때문 보안을 위해 파이어월이나 인증, 암호화 장비 등의 별도의 장치를 설치해야 안전하게 이용할 수 있는 단점이 있다. 그래서 최근 VPN의 보안에 IKE(인터넷 키 교환)과 IPSec(인터넷 프로토콜 보안) 방식이 이용되고 있다. VPN의 보안에 있어 암호화는 VPN의 한 지점에서 인터넷을 거쳐 다른 지점(다른 네트워크 또는 독립형 PC가 될 수 있음)까지의 프라이버

시를 유지하는데 사용된다.

데이터에 허용되는 보호 수준은 다음 사항에 달려 있다.

- 사용되는 암호 알고리즘

- 사용되는 암호 키의 길이

- 암호 키가 변경되는 빈도

단순한 VPN은 두 컴퓨터 사이의 '가상 터널'이다. 이 컴퓨터 사이의 모든 네트워크 트래픽은 이 가상 터널을 통과한다. 네트워크 레이어에서 암호화가 이루어지기 때문에 네트워크 스택에서 VPN을 지원해야 한다. 터널이 처음 만들어지면 두 컴퓨터는 상대 컴퓨터를 상호 인증해야 한다. 인증 후 두 컴퓨터는 어떤 암호화 알고리즘을 사용할 것인지, 암호화 알고리즘과 함께 사용할 기밀 사항이 무엇인지, 어떤 데이터 무결성 알고리즘을 사용할 것인지, 어떤 네트워크 트래픽이 터널을 통과할 것인지 등을 협의한다. 협의가 성공적으로 완료되면 두 컴퓨터 사이의 네트워크 트래픽이 구축된 VPN을 통해 흐른다.

- **가상회선 (Virtual Circuit)**

  네트워크 내의 지점들 간에 불연속적으로 보이는 회선이나 경로를 뜻한다. 그러나 물리적 경로는 실제로 관리되는 회선 자원들을 모아두었다가 특정 회선들의 트래픽 요건에 맞추기 위해 필요만큼 할당된다.

- **감사 (Audit)**

  제어 확립, 정책 및 운영 절차를 준수하고 제어, 정책, 또는 절차에 있어서 실질적 변경 사항을 제안하기 위한 기록 및 활동에 대해 독립적으로 조사하는 행위.

  1. 한 대 이상 컴퓨터에 설치된 모든 소프트웨어 및/또는 하드웨어에 대한 목록 작성 과정을 말한다. 일단 감사가 수행되면 허가 받지 않은 소프트웨어, 하드웨어 구성 요소 누락 등을 확인하기 위해 데이터를 분석할 수 있다.

  2, 모든 보안 관련 사건에 대한 목록 작성 과정을 말한다. 이 과정에는 사건을 일으킨 사용자도 포함된다.

- **감사 추적 (Audit Trail)**

  컴퓨터 보안 시스템에서 시스템 자원 사용에 대해 시간 순서에 따라 기록된 사용 내역을

말한다. 이 기록에는 사용자 로그인, 파일 접근, 기타 다양한 활동 내역, 그리고 실질적 또는 시도된 보안 위반 사항이 합법적으로 그리고 허가를 받지 않고 발생했는지 여부가 포함된다. 감사 추적은 사용자 행위를 추적하여 보안 사건들이 특정 개인의 행위와 관련되었는지는 밝힐 수 있는 자료가 되므로, 안전한 시스템을 위해 필요한 책임추적성의 기초 요구 사항이다.

- **강제적 접근 제어 (MAC [Mandatory Access Control])**

  비밀성을 갖는 객체에 대하여 주체가 갖는 권한에 근거하여 객체에 대한 접근을 제어하는 방법으로 관리자만이 정보자원의 분류를 설정하고 변경 가능하다.

- **개방 보안 (Open Security)**

  시스템이 작동하기 전에 또는 작동하는 중에 악성 논리의 도입에 대해 응용 프로그램 및 장비를 보호하도록 충분히 보장하지 못하는 환경을 말한다.

- **개방 시스템 상호연결 표준 (OSI Standard [Open Systems Interconnection Standard])**

  개방 시스템 상호연결 표준의 약어로 통신 프로토콜의 일반적 참조 모델을 말한다.

- **게이트웨이 (Gateway)**

  서로 다른 프로토콜 사이를 변환하는 하드웨어 또는 소프트웨어, 또는 또 다른 시스템에 대한 액세스를 제공하는 모든 매카니즘을 말한다. 즉, 게이트웨이는 서로 다른 네트워크들을 함께 연결하기 위해 사용된다. 예를 들어 Apple Talk 네트워크와 Microsoft 네트워크는 게이트웨이 컴퓨터에 의해 연결되어야 한다. ISP는 게이트웨이를 통해 사용자를 인터넷에 연결해준다.

- **게이트키퍼 (GateKeeper)**

  윈도의 사용자 계정 컨트롤(UAC)과 유사한 기능으로, 인터넷을 통해 다운로드한 앱이나 써드 파티(Third-party) 앱들로부터 맥(Mac)을 보호하는 기능이다.

- **격리 영역 (Quarantine Area)**

  의심이 가거나 감염된 파일이 이동하여 사용자들이 사용할 수 없지만 영구적으로 손실되지 않는 영역을 설명하기 위해 백신 프로그램에서 사용하는 용어다. 이 영역을 통해 보안을 의식하는 조직에서 감염된 파일을 영구적으로 삭제하지 않고 일반적으로 배포되지 못하도록 파일을 삭제할 수 있다. 관리자는 제어 조건 하에서 감염된 파일을 치료할 수 있고 치료된 파일을 원래 소유자에게 보낼지 여부를 결정할 수 있다.

- **경쟁 상태 (Race Condition)**

  Race Condition(경쟁 상태)는 둘 이상의 사용자가 동시에 접근가능한 채널을 이용하려고 시도할 때, 모든 사용자가 현재 이용중이라는 통보를 받지 못했을 경우 발생하는 현상이다. 공격자들은 네트워크에 불법으로 접속하려고 경쟁 상태에 관한 취약점을 악용하는 경우가 있다.

- **고퍼 (Gopher)**

  정보 메뉴를 인터넷에서 사용할 수 있도록 해주는 클라이언트/서버 프로그램. 고퍼는 월드 와이드 웹 이전까진 어디서든 사용되었지만 이후에는 WWW로 대체되었다.

- **공개키 (Public Key)**

  공개키 암호 시스템에서는 데이터를 잠그기 위한 암호화를 하기 위해서는 공개키를 사용하고 데이터를 잠금 해제하기 위한 복호화를 하기 위해서는 공개키와 쌍이 되는 비밀키를 사용한다. 공개키는 신뢰할 수 있는 디렉토리에 게시를 한다. 공개키를 안전하게 관리하고 신뢰하는 기관을 인증기관(CA, Certificate Authority)이라고 한다.

- **공개키 기반구조 (PKI [Public Key Infrastructure])**

  PKI는 인터넷 트랜잭션과 관련된 각 당사자의 진위를 확인하고 사기나 방해 행위에 대해 보호하고 부인봉쇄를 위한 시스템을 말하며 따라서 트랜잭션 거부에 대해 스스로를 보호할 수 있다. 제3의 신뢰 기관이라고 하는 인증서 발행 기관에서 사용자의 신원의 핵심

구성 요소를 지정하는 전자 메시지의 첨부 형태로 전자 인증서를 발행한다. 인터넷 트랜잭션에 서명이 이루어지는 동안 한 당사자에서 다른 당사자로 암호화된 메시지가 트랜잭션이 처리되기 전에 검증된다.

PKI는 소프트웨어 응용 프로그램에 내장되거나 서비스 또는 제품으로 제공된다. 전자상거래 리더들은 PKI가 트랜잭션 보안 및 무결성에 있어서 매우 중요하고 소프트웨어 업계는 이들의 사용을 위해 개방 표준을 채택하는 쪽으로 선회하고 있다. PKI 데이터를 포함하는 디렉토리 시스템을 간소화 하는 것이 한 가지 도전으로 남아 있다.

PKI는 공개 키 암호화와 전자 서명 서비스를 제공하기 위해 필요한 전반적인 시스템에 부여되는 용어이다. 따라서 PKI의 목적은 키와 인증서를 관리하고 따라서 진정한 네트워크 환경을 구축하고 유지 관리하는 것이다. (참고: 인증서 발행 기관, 전자 서명, 공개 키 암호)

- **공개키 암호 (Public Key Cryptography)**

  암호화 과정이 공개적으로 사용 가능하고 보호되지 않은 암호의 한 종류를 말한다. 그러나 복호화 키의 한 부분이 보호되고 따라서 복호화 과정의 양 부분을 알고 있는 당사자만 암호문을 복호화 할 수 있다.

  두 가지 키, 즉 공개 키와 비밀 키를 사용하는 암호화 키를 말한다. 누구나 한 개인의 공개 키를 알 수 있지만 한 개인의 비밀 키를 아는 사람은 없다. 암호화된 메시지는 해당 개인의 공개 키를 사용하여 수신자에게 전송될 수 있다. 그러나 이 메시지는 관련 비밀 키로만 복호화할 수 있다. 이러한 방식으로 복호화 키는 결코 공개되지도 전송되지도 않는다. (참고: 비밀 키 암호)

- **공개키 암호작성 시스템 (PKCS [Public-Key Cryptography System])**

  안전한 정보 교환을 위해 미국의 RSA에 의해 만들어졌으며, 산업계 내부에서 사용되는 비공식 표준 프로토콜이다.

- **깃허브 (GitHub)**

  깃(Git)을 사용하는 프로젝트를 지원하는 웹 기반의 호스팅 서비스. 깃(Git)은 리눅스를 개발한 리누스 토발즈가 리눅스 개발 중 코드 관리의 필요성을 느끼고 개발한 버전 관리 툴이다.

- **내부 게이트웨이 프로토콜 (IGP [Interior Gateway Protocol])**

  근거리 통신망과 같은 자율 네트워크 내 게이트웨이들 간에 라우팅 정보를 주고받는데 사용되는 프로토콜을 말한다. 주로 사용되는 IGP로는 RIP와 OSPF가 있다.

- **내성 워터마킹 (Robust Watermarking)**

  Authentication을 제외한 Copy control, copyright protection, play control과 같은 대부분의 응용 분야에 요구되는 watermaring 기술이다.

- **네트워크 기반 침입방지시스템 (NIPS [Network-based IPS])**

  원하지 않는 트래픽을 막기 위해 패킷레벨에서 탐지 및 방지 사용, 공격 세션으로 부터 원하지 않는 패킷들만 탈락기능 단점으로는 효과적인 보안업데이트에 의존해야 한다.

- **네트워크 보안 (Network Security)**

  인증되지 않은 변경, 파괴 또는 노출로부터 네트워크와 서비스를 보호하고, 네트워크가 중요한 기능을 올바로 수행하고, 해로운 부작용이 없다는 보증을 제공하는 것을 의미한다. 네트워크 보안에는 데이터 무결성 제공도 포함된다

- **네트워크 분석용 보안 관리자 도구 (SATAN [Security Analysis Tool for Auditing Networks, Security Administrator's Tool for Analyzing Networks])**

  IP 네트워크에 연결된 시스템의 취약성을 원격으로 조사하여 확인하는 강력한 프리웨어 프로그램이다. SATAN은 네트워크를 통해 원격 시스템의 보안 정도를 조사하고, 그 자료를 데이터베이스에 저장한다. 이 결과를 HTTP 프로토콜을 지원하는 HTML 브라우저를 통해 쉽게 볼 수 있다. 또한 호스트의 타입, 서비스, 결점 등의 보고서를 만들어낼 수도 있다.

- **네트워크 수준 방화벽 (Network Level Firewall)**

트래픽이 네트워크 프로토콜(IP) 패킷 수준에서 검사되는 방화벽이다.

- **네트워크 액세스 지점 (NAP [Network Access Point])**

  인터넷 액세스 제공업자를 함께 묶는 역할을 하는 많은 인터넷 상호연결 지점 중 하나이다.

- **네트워크 접속 저장장치 (NAS [Network Attached Storage])**

  네트워크에 접속되도록 특화된 파일서버이다. 이더넷이나 TCP/IP와 같은 LAN 프로토콜을 사용하며, 유닉스의 NFS와 도스/윈도우의 SMB와 같은 파일 입출력 요청을 처리한다.

- **네트워크 주소 변환 (NAT [Network Address Translation])**

  외부로 보여지는 공인 IP 주소와 내부에서 쓰여지는 사설 IP주소로 변환하는 기능을 말한다. 외내부 네트워크를 통과할 때에 주소 변환 과정을 반드시 거치게 됨으로 보안성을 가지며, 또한 요구를 제한하거나 인증하고, 또 이전의 요구와 일치시키는 기회를 제공한다.

- **네트워크 카드 (NIC [Network Interface Card])**

  네트워크와 컴퓨터 사이의 인터페이스로서 역할을 하는 하드웨어 카드를 말한다.

- **논리 폭탄 (Logic Bomb)**

  포크 폭탄(Fork Bomb)으로도 알려져 있다. 실행시 특정 조건이나 컴퓨터의 특정 상태를 확인하는 상주형 컴퓨터 프로그램으로서 조건이 만족하면 인증되지 않은 활동의 범행을 시작한다

- **능동적 공격 (Active Attack)**

  파일의 조작, 또는 허가 받지 않은 파일의 추가 등 허가를 받지 않은 상태 변경을 초래하는 네트워크 공격으로 수동적 공격과는 반대 개념이다.

수동적 공격은 상태를 변경하지는 않지만 오히려 활동 또는 로그 정보를 감시한다

- **다이어 (Dyre)**

'다이어(Dyre)'는 뱅킹 악성코드이다. 코드나 파일 은닉이 아니라 주요 웹사이트에서 개인정보 보호를 위해 SSL(Secure Socket Layer) 암호화를 하는데, 이를 활용해 암호화된 트래픽에 공격코드를 은폐시킨다. 이 경우 보안 솔루션 등과 같은 장비에서는 트래픽에 대한 가시성을 확보하지 못하면 정상 SSL 트래픽과 악성 트래픽을 구분할 수 없는 취약점을 갖는다. 이에 비해 파일에 대한 기본적인 동작들이 일반적인 악성코드 중 웜(Warm)류와 유사한 점이 많아 백신에서 쉽게 탐지할 수 있다.

- **다중 사용자 제어 (MUC [Multi-User Control])**

지정된 타겟에 대하여 다수의 사용자가 연합하여 요청할 경우의 접근통제정책을 지원하는 수단이 있어야 한다. 즉, 명시된 두 개인이 동의할 것을 요구하는 경우, 두 개의 역할에 대응한 개인들이 동의 할 경우, 그리고 하나의 그룹에서 특별히 명시된 몇 명의 멤버들(다수결)에 의하여 접근통제를 수행할 필요가 있을 수 있다.

- **다중 프로토콜 레이블 스위칭 (MPLS [Multiprotocol Label Switching])**

네트워크 트래픽 속도 향상 및 관리를 위한 기술을 말한다. MPLS는 주어지는 패킷열에 대하여 특정 경로를 설정하는 것에 관여하여 소요되는 시간을 절약할 수 있다. 트래픽을 전반적으로 빠르게 움직이게 하는 것 외에도, QoS를 위한 네트웍 관리를 쉽게 해준다.

- **단순 객체 접근 프로토콜 (SOAP [Simple Object Access Protocol])**

웹 서비스 메시징 표준으로써 HTTP를 사용하여 (80번 port) XML로 정의된 메시지를 전달, 방화벽 통과, SSL을 통한 암호화 및 인증 보안기능 제공한다.

- **단순 네트워크 관리 프로토콜 (SNMP [Simple Network Management Protocol])**

네트워크 관리 및 네트워크 장비의 감시를 다루는 프로토콜을 말한다. 보고 장치 및 데이터 수집 프로그램 간에 정보가 전달되는 방식을 설명하는 프로토콜을 말한다. 전자우편을 분산시키기 위한 표준 인터넷 프로토콜이다.SNMP는 관리자가 네트워크 성능을 관

리하고 문제점을 찾아 수정하는 데 도움을 준다. TCP/IP 네트워크에만 국한되지는 않는다.

- **단순 서비스 검색 프로토콜 (SSDP(Simple Service Discovery Protocol))**

  SSDP는 네트워크 상의 서비스나 정보를 찾는 프로토콜이다. 프린터나 스캐너, IP카메라, 스마트TV 등 IoT 기기가 네트워크를 탐색할 때 SSDP를 쓴다.

- **데이터 암호 표준 (DES [Data Encryption Standard])**

  일종의 개인키(대칭키) 암호화 알고리즘으로, 송신자와 수신자가 동일한 키로 데이터를 암호화/복호화 한다. 이때 길이가 충분히 긴 키를 사용하면 상당히 안전한 것으로 알려져 있다. DES는 원래 IBM에서 개발되었으며, 이후 FIPS 46에서 발행되었고, 정부 및 공공 사용에 대해 NIST에서 승인되었다. 기술적으로 DES는 56비트의 키가 16회의 작업으로서 조직된 64 비트 블록 암호문이다.

- **데이터 위주 공격 (Data Driven Attack)**

  악의적인 의도로 만들어졌지만, 겉으로 보기엔 정상적인 데이터에 의해 수행되는 공격 형태로서 사용자나 프로세스에 의해 수행되며 알 수 없는 손상을 유발한다. 데이터 위주 공격은 데이터 형태로 방화벽을 거친 뒤 시스템에 대한 공격을 시작하기 때문에 방화벽과 관련된 문제이다.

- **도메인 이름 서버 (DNS Server [Domain Name System Server])**

  도메인 이름(mydomain.com)을 IP 주소(123.456.789.012)로 변환하기 위해 DNS를 사용하는 서버이다.

- **도메인 이름 서버 스푸핑 (DNS Spoofing [Domain Name System Spoofing])**

  희생 대상 시스템의 이름 서비스 캐쉬를 손상하거나 유효한 도메인에 대한 도메인 네임 서버를 손상하여 다른 시스템의 DNS 이름을 가장하는 행위이다.

- **래티스 보안 모델 (Lattice Security Model)**

불법 정보 흐름 방지를 한다. 주체 및 객체에게 보안 클래스 부여한다. 정보 흐름을 통제한다.

- **랜드 어택 (LAND Attack)**

  공격자가 임의로 자신의 IP 주소와 Port를 해당 호스트의 IP 주소와 Port와 같게 하여 서버에 접속함으로써 서버의 실행속도가 느려지거나 마비되게 하는 공격을 말한다.

- **랜섬웨어 (Ransomware)**

  ransom(몸값)과 ware(제품)의 합성어로 컴퓨터 사용자의 문서를 '인질'로 잡고 돈을 요구한다고 해서 붙여진 명칭이다. 최근 출현한 랜섬웨어는 적절한 사용자 동의 절차 없이 사용자 PC에 설치되어 PC의 동영상 파일을 한곳의 폴더에 수집한 후 그 폴더를 루트킷(Root Kit) 기능으로 감춰 사용자들이 접근할 수 없도록 한 뒤에 동영상을 보기 위한 결제를 유도한다.

- **레진 (Regin)**

  레진(Regin)은 은닉형 악성코드로, 시만텍에서 2014년 11월 발견하여 공유한 정보 유출형 악성코드이다. 레진은 메모리 패치와 같이 다양한 악성코드와 은닉 기능을 사용했다. 보통의 악성코드에서는 볼 수 없는 복장성을 띄고 있다. 지난 2010년 특정 시스템을 공격하고 코드 전개가 전문화되고 복잡했던 '스턱스넷(Stuxnet)'과 비교되지만 내부 기법이나 목적에는 차이가 있다.

- **로드 밸런싱 (Load Balancing)**

  1개의 서버나 방화벽에 트래픽이 집중되는 것을 분산시키기 위한 스위칭 기술을 말한다. 집중된 데이터들을 서버로 분산시킴으로써 과부하 방지 및 네트워크 속도 향상 등 전체적인 네트워크 균형을 유지한다.

- **립프로그 공격 (Leapfrog Attack)**

  다른 호스트를 훼손하기 위해 한 호스트에서 불법적으로 얻은 사용자 ID와 암호 정보를 사용하는 것이다. 추적을 불가능하게 하기 위해 하나 이상의 호스트를 통해 TELNET을 수행하는 행위를 말한다.(일반적인 크래커의 작업 절차)

- **마이너 악성코드 (Miner)**

  악성코드의 한 종류로, 사용자 몰래 PC의 시스템 리소스를 이용해 가상화폐(암호화폐)를 채굴(마이닝, Mining)하는 악성코드를 안랩 등 보안 업체에서는 마이너(Miner) 또는 코인 마이너(Coin Miner)로 분류한다. '채굴 악성코드'로 불리기도 한다.

- **매크로 바이러스 (Macro Virus)**

  사용자가 알지 못하는 상태에서 실행할 수 있으며, 그 결과 손상을 야기하거나 자체를 복제하는 매크로이다.

  매크로 바이러스는 전달 과정만 제외하면 모든 면에서 표준 바이러스와 유사하다. 프로그래밍 언어로 코드가 작성되어 실행 파일에 첨부된 형태가 아닌 매크로 언어로 코드가 기록되어 문서에 첨부된다. 그래서 매크로 바이러스는 자체에 매크로 언어를 갖고 있는 모든 응용 프로그램과 연관될 수 있다. 말할 필요도 없지만 매크로 언어의 기능이 강력하면 할수록 매크로 바이러스의 잠재적인 위험은 더 커진다.

  매크로 바이러스의 대부분은 MS Word 바이러스이다. 그 이유는 다음과 같다.

  - Word의 매크로 바이러스는 매우 강력하고 다양하며, 사용하기 쉽다.

  - Word는 멀티 플랫폼에서 작동되며 광범위하게 사용된다. 따라서 바이러스 작성자가 쉽게 악용할 수 있는 대규모의 '대상'을 만들어 준다.

  Word 바이러스는 다음의 두가지 이유 때문에 각별한 주의가 필요하다.

  - 바이러스는 문서 자체가 아니라 문서에 첨부된 템플릿에 있다.

  - 감염된 문서가 첨부된 전자 우편을 받는다고 해서 곧바로 바이러스에 감염되는 것은 아니다. 문서를 Word에서 열어야만 바이러스에 감염된다.

  이러한 정보를 아는 것만으로도 약간의 방어를 취할 수 있으며, 먼저 어떤 전자 우편 첨부물도 허용하지 않는다는 보안 정책을 채택할 수도 있다. 이러한 전자 우편을 받으면 문서를 열지 않고 단지 삭제만 하면 되기 때문이다.

  두 번째 옵션은 Microsoft의 free Word 뷰어로만 첨부된 문서를 여는 방법이다. 이러면 어떠한 관련 매크로도 활성화하지 않고 Word 문서의 내용을 볼 수 있다. 이러한 방식으로 내용을 안전하게 읽을 수 있으면서, 해당 문서를 어떻게 처리해야 할지를 결정할 수 있다. 하지만 어떤 방식을 채택하든 간에 주요 바이러스 방지 제품의 사용과 함께 보안

정책을 강화하는 것이 중요하다.

- **맨트랩 (ManTrap)**

  공격자가 시스템에 침입할 때에 침입 전 가짜 호스트 주소로 유도 및 제어하여 실제 시스템을 보호하는 것을 말한다.

- **멀웨어 (Malware)**

  컴퓨터에 악영향을 끼칠 수 있는 모든 소프트웨어의 총칭이다. 예를 들어 바이러스, 웜, 트로이 목마 등

- **메일 폭탄 (Mail bomb)**

  메일 폭탄은 한 사용자의 이메일 계정에 수많은 이메일을 동시에 전송하거나, 사용자를 수많은 이메일 그룹에 가입시키는 등의 방법으로 한꺼번에 스팸 메일을 받도록 하거나, 혹은 엄청난 양의 메일을 다수의 사용자들에게 보내 불편을 초래하거나 메일 서버를 다운되게 함으로써 업무를 마비시키는 경우를 일컫는 말이다.

  메일 폭탄을 사전 방지하려면, 특정 인터넷 주소나 이메일 주소, 또는 메일 제목이나 내용에 특정한 단어들이 들어가 있는 이메일을 자동으로 필터링 하여 수신을 차단하는 방법이 동원된다. 현재 이메일 폭탄 및 스팸 메일을 방어해주는 제품이나 도구들이 많이 나와 있다.

- **무작위 공격 (Brute Force Attack)**

  정확한 키를 찾을 때까지 각각의 가능한 키를 시도하는 공격 유형을 말한다. 암호문을 알아볼 수 있는 평문을 찾기 전까지는 다른 키로 그 뜻을 파악한다. 평균적으로 이 공격은 키스페이스에 있는 키의 절반만 시도하면 된다.

- **바이러스 (Virus)**

  바이러스는 MS워드나 엑셀과 같이 컴퓨터에서 실행되는 프로그램의 일종이다. 그러나

다른 유용한 프로그램들과 달리 자기 복제를 하며, 컴퓨터 시스템을 파괴하거나 작업을 지연 또는 방해하는 악성 프로그램이다. 악성 프로그램에는 컴퓨터 바이러스 외에도 웜, 트로이목마 등이 있다.

컴퓨터 바이러스에 '바이러스'란 이름이 붙은 것은 컴퓨터 바이러스에 생물학적인 바이러스와 같은 자기 복제 능력이 있기 때문이다.

예전에는 바이러스 프로그램이라는 말을 사용했으나 매크로와 스크립트를 이용한 바이러스들이 많이 나타남에 따라 바이러스 코드로 그 의미를 확장시키기도 한다.

컴퓨터 바이러스가 모두 직접적인 피해를 가져오는 것은 아니지만, 대부분 부작용을 동반한다. 특히 파일에 손상을 주거나 하드디스크의 정보를 파괴하는 등의 치명적인 부작용을 일으키기도 한다.

최근에는 네트워크 환경의 발달로 이메일을 통해 전세계적으로 퍼지는 바이러스 형태가 증가하면서 그 피해는 광범위하고도 급속하게 번지고 있다. 따라서 백신 등을 이용한 철저한 방역대책을 세우는 것이 필요하다.

- **방사 보안 (Emission Security)**

  시스템에서 나오는 유해한 방사물의 분석 및 가로채기로부터 유도되어질 수 있는 가치 있는 정보를 보호하기 위한 모든 수단을 말한다.

- **방해 (Interruption)**

  보안공격의 하나로 시스템의 일부를 파괴하거나 사용할 수 없게 하는 경우로 가용성에 대한 공격이다.

- **방화벽 (Firewall)**

  방화벽은 인터넷과 특정 조직의 개별 네트워크 사이의 정보 흐름을 관리하는 하드웨어/소프트웨어 체제이다.

  방화벽은 인증되지 않은 인터넷 사용자가 인터넷, 특히 인트라넷에 연결된 사설 네트워크에 접근하는 것을 방지할 수 있으며, 인터넷으로부터 유입되는 바이러스의 공격도 차단할 수 있다. 방화벽은 또한 부서 간의 데이터 교환을 제어하기 위해 지역 네트워크의 두 개 이상의 부분을 분리하기 위해 사용될 수도 있다. 방화벽의 구성 요소는 필터와 스크린이 있는데 이들은 각기 특정 범위의 트래픽 전송을 제어한다.

방화벽은 사설 정보 보호를 위한 첫 방어선을 제공하지만, 포괄적인 보안 시스템은 암호화와 내용 필터링, 침입 탐지 등과 같은 다른 보완 서비스와 방화벽을 조합한다.방화벽은 인터넷과 같은 외부 통신 체제로부터 기업의 네트워크를 보호해주는 매카니즘이다.

방화벽은 대개 PC와 두 개의 네트워크 인터페이스 카드(NIC)가 있으며, 특수한 방화벽 프로그램을 수행하는 Unix 컴퓨터로 구성된다. 한 개의 네트워크 카드는 회사의 사설 LAN에 연결되며, 다른 하나는 인터넷에 연결된다. 이 컴퓨터는 두 네트워크 사이를 통과하는 모든 정보가 거쳐야만 하는 방어벽과 같은 역할을 한다.

방화벽 소프트웨어는 두 네트워크 사이를 통과하는 각각의 정보 패킷을 분석하여 미리 구성된 규칙에 맞지 않는 패킷이 있으면 이를 거부한다.

- **백 도어 (Back Door)**

트랩도어(Trap Door)라고도 불리는 백도어는 원래 시스템 관리자나 개발자가 유사시 트러블슈팅이나 유지보수 등을 할 관리적 목적으로 필요에 의해 시스템에 고의로 남겨 둔 보안 헛점의 일종이다. 그러나 이것이 순수한 목적으로 이용되지 않고 악의적으로 이용되는 경우 보안상 치명적인 문제를 일으킬 수 있다. 특히 정상적인 로그인 절차를 거치지 않고 트로이목마를 침투시켜 백도어로 이용하는 경우, 시스템 침입 사실 은폐는 물론이고 재침입을 위한 백도어 설치 등이 가능하기 때문에 매우 위험하다.

백도어의 주요 특징은 다음과 같다.

1. 시스템 관리자의 보안 관리를 우회하여 동작한다. 따라서 관리자가 수시 패스워드 갱신 등 아무리 안전한 관리를 하더라도 언제든지 시스템에 침입할 수 있다.

2. 대부분의 백도어 프로그램은 로그(흔적)를 남기지 않고 침입한다(wtmp, utmp, lastlog 등).

3. 시스템 침입시간이 짧다.

대표적인 백도어의 종류는 다음과 같다.

패스워드 크랙킹 백도어 / Rhosts++ 백도어/ 체크섬(Checksum) 백도어 / 타임스탬프(Timestamp) 백도어 / 로긴(Login) 백도어 / Telnetd 백도어 / Services 백도어 / Cronjob 백도어 / Library 백도어 / Kernel 백도어 / 파일 시스템(File system) 백도어 / 부트 블럭(Bootblock) 백도어 / 프로세스 은닉 백도어 / 루트킷(Rootkit) / 네트워크 트래픽(Network traffic) 백도어 / TCP 쉘(TCP Shell) 백도어 / UDP 쉘(UDP Shell) 백도어 / ICMP 쉘(ICMP Shell) 백도어 / 암호화 링크(Encrypted Link)

- **백 오리피스 (Back Orifice)**

  백오리피스는 대표적인 트로이목마 프로그램으로, 'Cult of Dead Cow(죽은 소에 대한 숭배)'라는 해커 그룹의 일원인 Sir Dystic이 제작 발표한 MS 윈도우 95/98 및 윈도우 NT 해킹 툴이다. 백오리피스라는 명칭은 마이크로소프트(MS)의 네트워크 관리 프로그램인 '백오피스'를 패러디해 붙여진 이름이다.

  백오리피스는 MS Back Office와 마찬가지로 원격지에서 윈도우용 PC의 모든 프로그램 파일을 관리할 수 있는 도구이기 때문에, 원격지에 있는 타인의 PC에 저장된 파일에 대한 접근은 물론이고 파일 삭제, 생성, 실행 등 PC 이용자 모르게 프로그램 및 파일에 대한 조작을 할 수 있다. 또한 실행 중인 프로그램의 제거 및 정지, 사용자 키보드 입력 자료의 모니터링, 현재 실행중인 화면 캡쳐, 비밀번호 빼내기, 레지스트리 편집 등이 가능하기 때문에, 이로 인한 해킹 피해가 확산되었다.

  백오리피스는 첫 발표 이래로 기능의 확장 및 업그레이드가 이루어지고, 특히 초보자도 금방 숙지할 수 있을 만큼 편리한 사용법으로 인해 인터넷과 PC통신을 통해 급속히 보급되고 있어 사용자들의 많은 경각심이 요구된다.

- **백신 (Vaccine)**

  컴퓨터의 하드디스크와 메모리로 등에 바이러스에 의해 감염되었는지 여부를 진단하고, 감염시 바이러스를 삭제하고 파일이나 시스템을 치료하는 소프트웨어를 말한다.

- **뱅쿤 (Bankun)**

  스마트폰에 설치된 정상 은행 앱을 삭제한 뒤 악성 은행 앱 설치를 유도하는 모바일 악성코드다.

- **버퍼 초과 (Buffer Overflow)**

  버퍼 또는 저장 영역에 더 많은 데이터가 입력된 후 버퍼에서 처리할 때 발생한다. 버퍼 초과는 생산과 소비 과정 사이의 비율을 처리하는데 있어서 발생하는 불일치에서 비롯된다. 버퍼 초과는 시스템 충돌이나 시스템 접근을 유도하는 백 도어의 생성을 초래할 수 있다.

- **보안 감사 (Security Audit)**

  보안 문제 및 취약성에 대한 컴퓨터 시스템을 통한 검색을 말한다.

- **보안 감사 추적 (Security Audit Trail)**

  원본 트랜잭션에서 관련 기록 및 보고서 방향으로 그리고/또는 기록과 보고서에서 이들의 구성 요소 소스 트랜잭션 방향으로 추적하는데 도움을 주기 위해 사용되는 문서적 처리 증거를 수집하여 제공하는 기록 세트를 말한다. (참고: 감사 추적, 위험 관리)

- **보안 도메인 (Security Domains)**

  주체가 접근할 수 있는 개체 세트를 말한다.

- **보안 등급 (Security Classification)**

  보안 등급은 어느 사용자가 어떤 데이터(일반적으로 사용자 자신의 계층적 기밀 사항 취급 허가 수준에 기초한다)에 접근할 수 있는지 파악하기 위해 사용된다. 보안 등급의 예로는 등급 보류, 등급 완료, 민감한 등급, 비밀 등급 등이 있다.

- **보안 보장 생성 언어 (SAML [Security Assertion Markup Language])**

  이질적인 웹 접근관리와 보안 제품간에 인증과 인가정보의 교환기능을 제공하는 XML기반언어로써, 웹기반의 시스템에 접근제어, 인증, SSO구현을 목적으로 한다.

- **보안 사고 (Security Incident)**

  사용중인 보안 정책을 통제하는 요구 사항에서 파생하는 분류 정보와 관련된 행위 또는 상황을 말한다.

- **보안 셸 (SSH [Secure Shell])**

상당히 긴 통과 어구에 의해 보호되는 두 컴퓨터 간에 완벽하게 암호화된 셸 연결을 뜻한다. 원격 컴퓨터에 안전하게 접근하기 위한 Unix 기반의 명령 인터페이스 및 프로토콜을 말한다. 관리자들이 웹서버 및 여러 종류의 서버들을 원격 제어하기 위해 사용되며 RSA 공개키 암호화 기법을 사용한다.

- **보안 수준 (Security Level)**

  정보의 민감성을 나타내는 계층적 등급 및 비계층적 범주의 조합을 말한다.

- **보안 아키텍처 (Security Architecture)**

  설계를 감독할 일련의 원칙과 함께 보안과 관련된 시스템의 모든 양상에 대한 세부 설명을 말한다.

  보안 아키텍처는 보안 요구 사항을 충족시키도록 시스템을 조립하는 방법을 설명한다.

  (1) 기밀성, 무결성 및 가용성의 조합.

  (2) 제어를 받지 않은 손실 또는 효과의 품질 또는 보호되는 상태

  절대적 보안을 성취하기란 실질적으로 불가능하다. 따라서 보안 "품질"은 상대적일 수 있다. 보안 시스템의 상태 모델 내에서 보안은 다양한 작동 중에 보호되어야 할 특정 "상태"이다.

- **보안 정보 이벤트 관리 (SIEM)**

  SIEM(Security Information & Event Management)은 기업이나 개관 내부의 다양한 보안 로그와 이벤트, 각종 자산 정보를 통합하여 상관 분석한다.

- **보안 커널 (Security Kernel)**

  참조 감시 개념을 구현하는 신뢰를 받는 전산 기지의 하드웨어, 펌웨어 및 소프트웨어 요소를 말한다.

  보안 커널은 모든 접근을 중재해야 하고 수정되지 않도록 보호해야 하고 정확하게 검증할 수 있어야 한다.

- **보안 페이로드 캡슐화 (ESP Protocol [Encapsulating Security Payload Protocol])**

  트랜스포드(Transport Mode)와 터널 모드(Tunnel Mode) 두 가지의 운용 모드를 가지고 있다. 트랜스포드 모드는 일반적으로 보안 호스트 구현시 사용되며 상위 계층 프로토콜에 대한 보호 서비스를 제공한다. 터널 모드의 경우는 보안 호스트 및 게이트웨이 구현시 모두 적용되며 outer IP 헤더를 새로이 생성하여 inner IP 헤더를 포함한 inner IP 패킷 전체에 대한 보호 서비스를 제공한다.

- **보안 평가 (Security Evaluation)**

  기밀 정보를 안전하게 처리하기 위해 시스템에 부여하는 신뢰도를 평가하기 위한 일련의 수행 과정. 두가지 유형으로 구분되는데 먼저 제품 평가는 응용 환경을 배제한 과정에서 하드웨어와 소프트웨어의 기능 및 확인 사항에 대해 수행하는 평가이다. 다른 유형인 시스템 평가는 특정 운영 임무와 관련하여 시스템의 안전 대책을 평가하기 위해 수행되며 인증 및 인가 과정의 핵심 단계다.

- **봇넷 (Botnet)**

  많은 Bot 감염시스템들이 명령을 수신할 목적으로 IRC에 연결되어 있는 네트워크이다.

- **부인봉쇄 (Non-Repudiation)**

  부인봉쇄는 문서나 송,수신자가 유효한 상태일 때 발생하는 기능으로 암호화에 있어서 부인봉쇄는 액세스를 보호하기 위해 개인 키를 사용하는 사람에게 적용되는 것이다. 이로써 해당 개인의 전자 서명을 사용하여 서명된 모든 메시지는 이들로부터 비롯될 수 있음을 보증한다. 전자 상거래에서 키 주인이 재정적 거래에 전자 서명을 사용하면, 이 거래의 대상인이 누구인지를 보증하게 된다.

  데이터 전송자는 배달에 대한 증명을 제공받으며, 수신자는 전송자의 신분을 확인할 수 있는 과정. 이것이 부인봉쇄이며, 따라서 어느 쪽이라도 데이터의 전송이나 수신을 문제 삼아 거부할 수 없다. 부인봉쇄는 미래의 전자 상거래를 위한 기초를 제공하며 필수적인 요소이다.

  키 소유자의 개인 키를 도난으로부터 보호하고 해당 개인 키를 사용하는 컴퓨터를 침입

이나 파괴로부터 완벽히 보호함으로써만 부인봉쇄 기능을 제공할 수 있다.

- **부트 섹터 감염 바이러스 (Boot Sector Infector)**

  컴퓨터가 시동될 때부터 디스크의 부트섹터를 감염시키는 바이러스이다.

- **분산 서비스 거부 공격 (DDoS [Distributed Denial-of-Service attack])**

  인터넷 또는 네크워크 연결 상에서 다수의 시스템이 하나의 대상 표적을 대상으로 다량을 패킷을 전송, 다량의 트래픽을 발생시켜 네트워크 대역폭을 점유하는 방식으로 대상을 시스템을 마비시키는 공격을 말한다.

- **분산 컴퓨팅 환경 (DCE [Distributed Computing Environment])**

  분산 컴퓨터들의 시스템 내에서 컴퓨팅 및 데이터 교환을 설정하고 관리하는데 필요한 산업표준 소프트웨어 기술이다. DCE는 클라이언트/서버 모델을 사용하며 사용자는 원격지의 서버에 있는 응용프로그램과 데이터를 쓸 수 있다.

- **불법자원사용**

  정당한 권한 없이 특정 시스템을 스팸릴레이, 피싱사이트 개설 등에 이용하는 행위이다.

- **비(非) 비밀번호 인증 표준 (UAF)**

  (Univeral Authentication Framework). 비(非) 비밀번호 인증 표준으로 비밀번호 입력 없이 지문이나 홍체 등 생체 인식이나 핀(PIN)으로 인증하는 방법이다.

- **비대칭 알고리즘 (Asymetric Algorithm)**

  비대칭 알고리즘은 공개키 알고리즘이라고도 불리며, 이는 암호화 및 복호화 시 각기 다른 두 가지 키를 필요로 하는 암호 알고리즘을 말한다. 이 키를 일반적으로 공개 키와 비밀 키라고 하며, 비대칭 알고리즘은 대칭 알고리즘에 비해 속도가 느리다. 더욱이 암호화 속도와 복호화 속도가 서로 차이가 날 수 있다. 일반적으로 비대칭 알고리즘은 대칭 세션 키를 교환하거나 메시지를 전자적으로 서명하는데 사용된다. 비대칭 알고리즘의 예로는 RSA, RPK, ECC가 있다.

- **비용-위험 분석 (Cost-Risk Analysis)**

  한 시스템의 데이터를 보호하는 비용 대 데이터의 손실 또는 위험 노출에 따른 비용에 대한 평가를 말한다. 보안에 소요되는 비용이 데이터의 가치를 초과해서는 안된다는 원칙이 널리 통용되고 있다.

- **비임의 보안 (Non-discretionary Security)**

  보안 수준에 기초하여 액세스를 제한하는 DOD 보안 정책의 양상이다. 보안 수준은 읽기 수준과 범주 설정 제한으로 구성된다. 한 정보 아이템에 대한 읽기 액세스를 위해 사용자는 정보 등급화보다 크거나 동일한 허가 수준을 가져야 하며, 또한 정보에 지정된 액세스 범주 모두를 포함하는 범주 허가를 가져야 한다.

- **비콘 (Beacon)**

  비콘(Beacon) : 근거리 위치인식기술. ISM 밴드인 2.4GHz 대역의 라디오 주파수(RF)를 이용했다. BLE(Bluetooth Low Energy) 규격을 이용하여 주기적 신호 발생 장치로 통용되고 있다. 스마트 기기 분야에서 비콘은 BLE를 이용하는 신호발생기를 지칭하는 용어로 통용된다.

- **사물인터넷 (IoT(Internet of Things))**

  수많은 사물이 인터넷에 연결되어 서로 데이터를 주고받고 사물 스스로 의사 결정을 하는 것까지 가능하다는 개념이다.

  제조·스마트홈·지급결제·물류 서비스·웨어러블·스포츠·헬스케어 등 다양한 분야에 적용되고 있다. 미국 시장조사 업체인 가트너는 IoT에서 2020년에 1조 9천억 달러의 시장이 창출될 것으로 전망하고 있다.

- **사용자 데이터그램 프로토콜 (UDP [User Datagram Protocol])**

  UDP는 TCP/IP 네트워크에서 사용하는 상위 프로토콜의 하나로 IP를 사용하는 네트워크 내에서 컴퓨터들 간에 메시지 전송시 제한된 서비스만을 제공하는 통신 프로토콜이다.

  TCP와 마찬가지로 UDP도 한 컴퓨터에서 다른 컴퓨터의 실제 데이터 단위(데이터그램)를

받기 위해 IP를 사용한다. 그러나 UDP는 TCP와는 달리, 메시지를 패킷으로 나누고, 반대편에서 재조립하는 등의 서비스는 제공하지 않으며, 특히 도착하는 데이터 패킷들의 순서를 제공하지 않는다. 즉, UDP를 사용하는 응용프로그램은, 전체 메시지가 올바른 순서로 도착했는지에 대해 확인할 수 있어야 한다는 것을 의미한다. 그러므로 교환해야 할 데이터가 매우 적은 네트워크 응용 프로그램들은 처리시간 단축을 위해 TCP 보다 UDP가 더 효과적일 수 있다. 일례로 TFTP는 TCP 대신에 UDP를 사용한다.

- **사이버 킬 체인 (Cyber Kill Chain)**

킬 체인(Kill Chain)은 세계적인 군수업체 록히드마틴의 등록상표로, 적의 미사일을 실시간으로 탐지하고 공격으로 잇는 일련의 공격형 방위시스템을 일컫는 시사 용어이다. 이 용어가 IT 보안 업계에서는 공격자가 조직을 공격할 때 쓰는 방법을 7개의 단계로 정의한 모델로서 사이버 킬 체인으로 표현되고 있는 것이다. 사이버 킬 체인의 7단계는 ▲정찰(Reconnaissance) ▲공격코드 제작(Weaponization) ▲전달(Delivery) ▲취약점 공격(Exploitation) ▲설치(Installation) ▲명령 및 제어(Command and Control) ▲목표시스템 장악(Actions on objectives) 등이다. 사이버 킬 체인은 APT(Advanced Persistent Threat)라고 불리는 지능형 위협 공격을 설명하는데 주로 사용되는 용어 중 하나다.

- **사전 공격 (Dictionary Attack)**

공격자가 암호 등을 알아 맞추기 위해 대규모의 가능한 조합을 사용하는 공격 형태로서, 공격자는 일반적으로 사용되는 백만 개 이상의 암호를 선택하여 이들 중 암호가 결정될 때까지 이를 시험해볼 수 있다.

- **서비스 거부 (DoS [Denial of Service])**

(1) 시스템의 정상적인 기능을 방해하여 인증된 사용자에 의한 해당 시스템 및 데이터에 대한 합법적인 접근을 방해하기 위해 특별히 의도된 공격을 말한다.

(2) 시스템의 일부에서 의도된 목적과 일치하여 기능하지 못하도록 방해하는 일련의 조치를 말한다. 여기에는 인증되지 않은 파괴, 수정, 또는 서비스 지연을 유발하는 모든 행위도 포함된다.

DoS는 공격자가 이익을 얻는 것은 아니지만, 정당한 사용자에 대한 서비스가 거부된다. 또한 데이터 파괴 또는 수정이나 시스템 손상, 인증된 사용자에 대한 서비스 지연/방해되는 등, 시스템의 서비스를 과부하 시킴으로써 일어날 수 있다.

DoS는 대개 원격 통신(인터넷을 통한)을 사용하는 외부 소스나 회사에 대해 자신의 손상을 회복 또는 복수하려는 의도로 이루어지는 경우가 많으며, 다루기 가장 어려운 공격 중 하나이다.

- **서비스 포트 (Service Port)**

  특정 응용프로그램이 인터넷상에서 클라이언트와 통신하는 통로, 일종의 서비스 창구와 같은 개념으로 이해할 수 있다(예 : 웹(web)은 TCP 80 서비스 포트 사용).

  설명자료 요청 (RFC [Request for Comments])

  관련 당사자들이 초안을 작성한 다음 검토하여 만들어지는 공식적인 인터넷 문서 또는 표준을 말한다. 네트워크 프로토콜 또는 서비스를 구현할 때 필요한 절차, 형식 등을 자세히 설명해 놓은 문서 자료다.

- **세드닛 (sednit(or sednit))**

  러시아 해커집단이 만든 최초의 악성코드다. 백도어 프로그램으로 소파시(sednit)라고도 불린다. 스피어 피싱 이메일 또는 감염된 웹사이트에서 구동하는 드라이브 바이 다운로드(Drive-by Download) 형식으로 피해자를 양산한다.

- **세션 키 (Session Key)**

  서버와 클라이언트간 통신Session동안에만 사용하는 한번 쓰고 버리는 암호화 키이다. 하나의 키를 사용한 암호문이 많을 경우 이를 분석 가능하므로 이를 막기 위한 방법으로 쓰인다. (한 Session Key만 가로채어도 그 Session에서만 보안문제가 생김)

- **세션 하이재킹 공격 (Session Hijacking Attack)**

  타인의 세션을 스니핑 및 추측을 통해서 도용하거나 가로채어 원하는 데이터를 보낼 수 있는 방법을 말한다.

- **수동적 IDS (Passive IDS [Passive Intruision Detection System])**

  침입자가 있다는 것을 메신저나 메일을 통해 알려주는 방식이다.

- **수동적 공격 (Passive Attack)**

  능동적 공격과는 반대로 시스템의 상태를 변경하지 않고 허가 받지 않은 정보 노출에 대한 위협을 말한다. 즉 정보의 변경이 아닌 차단을 수반하는 위협의 한 종류로, 데이터를 수동적으로만 감시하고 기록함으로써 공격을 시도한다.

- **스니퍼 (Sniffer)**

  스니퍼는 네트웍 트래픽을 감시하고 분석하는 관리용 프로그램으로서 일반적으로 트래픽에 따른 병목현상을 해결하는 데 이용된다. 그러나 악의적인 용도로 LAN 등 네트워크 환경의 트래픽을 분석하여 사용자 ID나 패스워드, 이메일 정보를 수집하는 공격에 이용된다. 스니퍼 공격에 대비하기 위한 대책으로는, ifconfig 명령이나 cpm을 사용하여 탐지하거나 promiscous 모드를 지원하지 않는 네트워크 카드 및 인텔리전트(Intelligent)한 허브(Hub)를 이용하여 공격에 대비한다. 이외 인증 기능을 강화하거나 암호화로 대처하는 방법이 있다.

- **스머핑 (Smurfing)**

  공격자가 에코 요청 ICMP (VLD) 패킷의 소스 주소를 한 네트워크의 브로드캐스트 주소로 속여 네트워크에 연결된 컴퓨터들이 네트워크를 방해하는 희생자에게 집단으로 대응하도록 하는 서비스 거부 공격을 말한다.

- **스미싱 (Smishing)**

  스미싱은 문자메시지(SMS)와 피싱(Phishing)의 합성어로, 문자메시지를 이용해 개인 및 금융정보를 탈취하는 휴대폰 해킹 기법이다. 특정 링크가 적힌 낚시성 문자를 보내 사용자가 해당 링크를 클릭하게 한 뒤 악성코드를 설치해 소액결제 및 개인정보 탈취 등의 피해를 유발한다.

- **스위치 재밍 (Switch Jamming Attack)**

  위조된 MAC주소를 지속적으로 네트워크로 흘려 보내 스위치의 주소 테이블을 가득차게

하면 스위치는 모든 네트워크 세그먼트로 트래픽을 브로드캐스트하게 되고, 이때 sniffing이 가능해진다.

- **스카다 (SCADA)**

  산업 공정, 기반시설, 설비를 바탕으로 한 작업 공정을 감시하고 제어하는 컴퓨터 시스템(Supervisory Control and Data Acquisition)이다.

- **스파이아이 (SpyEye)**

  '제우스' 악성코드와 함께 전 세계적으로 가장 많은 피해가 보고된 인터넷 뱅킹 정보를 탈취하는 목적의 악성코드다. 지난 2009년 12월경 처음 발견된 이후 지속적으로 변종이 유포되고 있다.

- **스파이웨어 (Spyware)**

  스마트폰을 대상으로 통화 내역, 문자메시지, 이메일 내용 등의 개인 정보를 외부로 유출하는 소프트웨어를 말한다. 스파이웨어는 스마트폰 앱으로 제작돼 상대방에게 문자메시지로도 설치할 수 있다.

  최근 위키리스크는 영국의 감마인터내셔널이 개발한 핀피셔(FinFisher)를 내려받을 수 있도록 공개했다. 핀피셔는 40개 이상 안티바이러스 소프트웨어의 탐지 우회는 물론 PC 웹캠에 비친 영상을 모두 녹화하고 마이크 음성을 녹음할 수 있다.

- **스팸봇 (Spambot)**

  중앙의 원격 제어 서버로부터 명령을 전달받아 무차별로 대량의 스팸메일을 발송하는 자동화된 악성코드의 유형이다.

- **스푸핑 (Spoofing)**

  스푸핑(spoofing)이라 함은, 타인의 시스템 자원에 접근할 목적으로 IP를 날조하여 정당한 사용자인 것처럼 보이게 하거나 승인 받은 사용자인 체 하여 시스템에 접근함으로써 추적을 피하는 고급 해킹 수법이다.

  스푸핑의 대표적인 예로는 IP 스푸핑을 들 수 있다. 1995년 미국의 케빈 미트닉이 이 기법을 사용하여 해킹 범죄를 저질렀다가 체포된 사건으로 더욱 유명해졌는데, 보안에 원

천적으로 취약한 TCP/IP 프로토콜의 취약점을 이용하여 여러 가지 공격 방법들이 존재한다. IP 스푸핑은 공격 대상인 호스트의 IP 주소를 교묘히 바꾸어서 이를 이용해 해킹을 하는 것이다. 만일 특정 호스트에 있는 정보를 훔쳐내고 싶다면, 자신이 현재 머물러 있는 IP 주소를 그 특정 호스트와 함께 하드 디스크를 공유하고 있는 다른 호스트의 주소로 위장하고, 마치 자신이 진짜 호스트인 것처럼 정보를 보내어 공격대상 호스트의 하드 디스크를 공유하도록 만든다. 이 기법은 IP를 속여서 공격하기 때문에 추적이 쉽지 않고, 아무런 흔적도 남기지 않고 원하는 정보를 몰래 훔쳐내올 수 있게 되는 것이다.

- **스피드핵 (Speed Hack)**

  PC의 시스템 타임을 조작해서 게임의 진행 속도를 마음대로 조정하는 해킹을 뜻한다. 속도를 빠르게 혹은 느리게 한다.

- **스피어 피싱 (Spear phishing)**

  특정인 또는 조직을 표적으로 신뢰할 만한 발신인이 보낸 것처럼 위장한 메일을 통해 악성 웹 사이트로 유도하거나 악성 첨부 파일로 악성코드에 감염시키는 피싱 공격을 말한다. 작살(spear)과 피싱(phishing)이 합쳐진 말로, 작살로 물고기를 잡는 '작살 낚시(Spear Fishing)'에서 유래했다.

- **시그니처 (Signature)**

  악성코드를 진단/치료하기 위해 사용되는 진단값. 패턴이라고도 한다.

- **시큐어 소켓 레이어 (SSL [Secure Sockets Layer])**

  SSL은 인터넷 상에서 비밀 문서를 전송하기 위해 넷스케이프에서 최초로 개발한 프로토콜이다. SSL은 비밀 키를 사용하여 SSL 연결을 통해 전송되는 데이터를 암호화한다. SSL은 신용 카드 번호 등 또한 기밀 사용자 정보를 입수하기 위해 사용할 수도 있다.

  SSL 연결을 필요로 하는 웹 페이지는 https:로 시작한다. 더욱 새로운 보안 프로토콜은 TLS (트랜잭션 레이어 보안)은 때때로 SSL 응용 프로그램과 통합되어 결과적으로 인터넷 보안의 표준으로 자리잡을 것이다. TLS는 복잡한 삼중 DES 암호화를 사용하여 클라이언트와 호스간의 터널을 생성함으로써 전자상거래를 위한 메일 암호화 및 인증을 제공한다.

- **시큐어 소켓 레이어 가상 사설망 (SSL VPN [Secure Sockets Layer Virtual Private Network])**

  보안 통신 프로토콜인 SSL을 통해 VPN을 구현하는 것으로 다수의 원격 사용자를 가진 환경 혹은 웹기반 어플리케이션 운영환경에 유용하다.

- **시큐어 코딩 (Secure Coding)**

  소프트웨어 개발 보안이라고도 부른다. 안전한 소프트웨어 개발을 위해 소스 코드 등에 있을 수 있는 잠재적인 보안 취약점을 제고하고 보안을 고려하여 기능을 설계 및 구현하는 등 소프트웨어 개발 과정에서 지켜야 할 일련의 보안 활동을 의미한다.

- **시타델 (Citadel)**

  금융 정보 탈취형 악성코드로, 온라인 뱅킹에 사용되는 개인 금융 정보를 탈취하기 위한 목적으로 제작 및 유포된다. 허위백신 등을 다운로드 및 실행해 사용자에게 금전을 요구하기도 한다. 주로 수집하는 정보들은 사용자의 로컬 네트워크 도메인 정보, 데이터베이스 서버 리스트, 사용자 네트워크 환경, 윈도우 사용자 및 그룹 계정 정보, 나아가 웹 브라우저에 홈페이지로 설정된 정보까지 다양하다. 악성코드 생성기 '시타델 빌더'로 만들어지며 '시타델 스토어'를 통해 판매된다.

- **알고리즘 (Algorithm)**

  특정 문제를 해결하기 위한 공식 또는 일련의 단계. 알고리즘의 각 단계는 명확하게 정의되어야 한다. 알고리즘은 프로그램 작성 언어를 포함하여 모든 언어에 대해 보편적이다. 바꾸어 말하면, 데이터를 조작하는 일련의 컴퓨터 언어 지침으로 일반적으로 명쾌하게 인코드될 수 있는 수학적 절차이다. 암호 알고리즘은 메시지를 암호화 및 복호화하고 문서를 전자적으로 서명하기 위한 목적으로 사용되는 수학적 절차이다.

- **암호 분석 (Cryptanalysis)**

  1) 기밀 변수 및/또는 평문을 포함한 기밀 데이터를 추론하기 위한 암호 시스템 또는 임호 시스템의 입출력 분석을 말한다.

2) 암호 알고리즘 및/또는 암호화 시 사용된 키를 처음부터 모르더라도 암호화된 메시지를 일반 텍스트 변환할 때 수행되는 여러 가지 조작 행위를 말한다.난해한 문제로 인해 감추어진 정보를 알아내는 학문, 즉 암호 분석을 통해 암호문의 의해 감추어진 비밀을 밝혀낸다.

- **암호 해시 함수 (Cryptographic Hash Function)**

  해시어(hashword)가 보호될 때 데이터의 조작을 간파할 수 있는 방식으로 특정 데이터 단위에서 값(해시어라고 함)을 계산하는 과정을 말한다.

- **암호문 (Cryptography)**

  암호문은 공공망을 통한 전송을 위해 데이터를 비밀 코드로 변환하는 과정을 말한다.

  원문이 암호 알고리즘에 따라 코드문 또는 암호문으로 변환된다. 데이터를 안전하게 보호하는 학문으로 알려져 있는 암호문은 정보를 보관하거나, 관련이 없는 당사지들이 보관된 정보를 알거나 접근하지 못하도록 그리고 통신 방법을 알지 못하도록 차단하는 방식으로 당사자끼리만 통신할 수 있도록 해준다.

  암호화 과정은 알기 쉬운 텍스트를 가져와서 이를 알기 힘든 데이터 조각(암호문이라고 함) 변형한다. 복호화 과정은 알기 힘든 데이터를 알기 쉬운 데이터로 복구한다. 두 가지 모두 수학 공식 또는 알고리즘과 키라는 비밀 데이터 시퀀스가 필요하다.

  암호 서비스는 기밀성 (데이터를 비밀로 유지), 무결성 (데이터의 수정 방지), 진위성(자원 또는 사용자의 신원)과 부인 방지(메시지 또는 트랜잭션이 발신 및/또는 수신되었음을 증명함)를 제공한다. 암호문에는 두 가지 종류가 있다. 공유/비밀 키(대칭) 암호문에서는 양 교신 당사자들이 비밀로서 공유하는 키가 하나만 있다.

  암호화 및 복호화 시 동일한 키가 사용된다.공개 키 (비대칭) 암호문에서는 암호화 및 복호화 시 각기 다른 키가 사용된다. 한 당사자에게는 두 가지 키,즉 공개 키와 비밀 키가 있다.

  이 두 가지 키는 수학적으로 관련이 있지만 공개 키에서 비밀 키를 알아내기란 실질적으로 불가능하다. 어떤 사람의 공개 키(공개 디렉토리에서 입수)를 사용하여 암호화 된 메시지는 과련된 비밀 키를 사용해야만 복호화 할 수 있다. 바꾸어 말해서, 비밀 키는 문서를 "서명"하는데 사용하고 공개 키는 문서의 출처를 입증하는데 사용할 수 있다.

- **암호키 (Cryptographic Key)**

  평문 데이터를 암호문 데이터로 변형, 암호문 데이터를 평문 데이터로 변형, 데이터에서 계산된 전자 서명, 데이터에서 계산된 전자 서명의 입증, 또는 데이터에서 계산된 데이터 인증 코드 (DAC)를 결정하는 암호 알고리즘과 연동하여 사용하기 위한 매개 변수 즉, 키를 말한다.

- **암호화 (Encryption)**

  암호화는 데이터를 인가되지 않은 사람이 알아 볼 수 없는 암호문(ciphertext)의 형태로 변환하는 것을 말하며, 이와 반대로 복호화(해독, Decrpytion)는 암호회된 데이터를 원래의 형태로 다시 변환하는 과정이다.

  암호화와 복호화는 처음에 전쟁시 적에게 정보가 유출되는 것을 방지하기 위해 사용되었으나, 오늘날에는 주로 인터넷 전송과 시스템 데이터의 보안을 유지하기 위해 사용되고 있다.

  암호화와 복호화는 암호 알고리즘과 키를 이용함으로써 수행되는데, 이때 사용하는 키의 종류에 따라 암호화 키와 복호화 키가 동일한 대칭키 암호 알고리즘과 암호화 키와 복호화 키가 서로 다른 공개키 암호 알고리즘으로 구분된다.

  그러나 암호 알고리즘과 키를 이용하여 암호화된 데이터도 완벽히 안전할 수는 없다. 암호화는 인가되지 않은 사람이 복호화를 시도할 경우, 이를 어렵게 만들 수 있기는 하지만 무제한적인 처리 능력과 시간만 보장된다면, 어떠한 암호 시스템도 무너질 수 밖에 없다.

  따라서, 암호화의 목적은 데이터의 비밀이 유지되어야 하는 기간 내에 암호문을 보호하는 것이라고 할 수 있으며, 강력한 암호화라는 것은 효과적인 암호의 유효 기간 내에 실제로 키를 발견하는 것이 불가능 할 것이라는 의미를 내포한다. 이때 강력한 암호화와 약한 암호화의 차이는 단지 처리 능력의 문제일 뿐이기 때문에, 컴퓨터의 기능이 급속히 향상되고 비용까지 내려감에 따라 현재의 "강력한 암호화"는 결국 "약한 암호화"가 될 수 밖에 없을 것이다.

- **암호화 파일 시스템 (EFS [Encrypting File System])**

  Windows 2000 운영 체제의 기능으로서, 어떤 파일이나 폴더도 암호화된 형식으로 저장될 수 있으며, 개별 사용자나 인증된 복구 에이전트가 해독할 수 있다.

- **액티베이션 락 (Activation lock)**

  애플이 2013년 6월 iOS7에 넣은 분실 및 도난 방지 기능. 스마트폰 분실 및 도난 사건이 증가하면서 스마트폰 제조사에서 이를 예방하기 위해 착안해낸 기술이다. 스마트폰 분실 시 사용자의 비밀번호를 입력해야 쓸 수 있다. 사용자가 분실 또는 도난 당한 아이폰과 아이패드를 못쓰게 한다. 기기 정보를 초기화하거나 기본 작동 상태로 되살리려면 기기 주인의 아이튠즈 계정으로 접속해야 한다. 삼성전자는 2013년 갤럭시S4에 '로잭(Lojack)'이라는 도난방지 소프트웨어를 펌웨어 업데이트 방식으로 탑재했다.

- **웹서비스 메시지 보안 기술 (WS-Security)**

  SOAP기반의 안전한 웹서비스 메시지 교환 위한 기술. SOAP을 기반으로 하며 인증, 무결성, 부인봉쇄, 기밀성 등의 보안기능을 확장 제공한다.. XML전자서명 및 XML Encryption 확장하여 적용한다.

- **웹서비스 보안 상호연동 프로파일 기술 (WS-Fedration)**

  핵심 웹서비스 보안표준들의 상호운용을 위한 프로파일 기술이다.

  웹서비스 보안정책기술 (WS-Policy)

  웹서비스 응용에 대한 보안정책의 생성과 교환을 위한 기술이다. 웹서비스의 정책 설명 및 전달을 위한 범용모델과 해당 구문을 제공하는 명세이다.

- **웹서비스 신뢰관리 기술 (WS-Trust)**

  상이한 보안 체계에 속한 웹서비스 응용들 간의 인증 및 인가를 지원한다. 다양한 신뢰 도메인 내에서 보안 토큰의 발행 및 교환 방법과 신뢰관계의 존재 설정 및 접근 방법에 대한 확장 정의한다.

- **웹서비스 응용간통신키 관리기술 (WS-Secure Conversation)**

  웹서비스 응용 간 보안 컨텍스트의 생성과 공유를 위한 기술이다. 보안 컨텍스트의 생성과 공유 등을 위한 프로토콜과 기능을 명세 한다.

- **웹서비스 프라이버시 보호기술 (WS-Privacy)**

  개인의 프라이버시 선호도와 응용 정책 교환기술이다. 웹서비스와 요청자가 주체의 프라이버시 선호화 기업의 프라이버시 실행 구문 서술방법에 대한 모델 기술이다.

- **위조 (Fabrication)**

  보안공격의 하나로 비인가자들이 시스템에 대한 위조물을 삽입하는 것을 말하며, 이는 인증에 대한 공격이다.

  위험 관리 (Risk Management)

  위험을 확인하고 컴퓨터 시스템에 대한 공격에 대해 방어함으로써 보안을 제공하는 활동을 말한다.

  위험 관리 프로그램은 일반적으로 세 가지 기본적인 요소, '안전 수단 선택', '인증 및 인가', 그리고 '비상 계획'에 초점이 맞추어진다. 안전 수단 선택은 한 조직에서 시스템 위협을 완화하기 위한 최상의 방법이라고 판단하는 비용, 효율적 보안 도구의 선택을 지칭한다. 인증은 보안 활동의 운영 및 중단의 공식적 허가인 반면 시스템 안전 수단이 적합하고 제대로 기능하는지를 기술적으로 검증하는 것이다. 비상 계획은 네트워크 종단 사태가 발생할 시 중요한 시스템에 대해 지속적으로 처리하는 능력을 보증한다.

- **위험 노출 (Compromise)**

  기밀 정보에 대해 인가를 받지 않은 노출, 수정 또는 파괴가 발생할 수 있는 컴퓨터 시스템에 대한 침입을 말한다.기밀 정보에 대해 인가받지 않은 접근 또는 노출이 발생할 경우 데이터가 위험에 노출되었다고 말한다.

- **위험 분석 (Risk Analysis)**

  한 조직의 정보 자원, 기존 제어 및 컴퓨터 시스템 취약성에 대한 분석을 말한다. 위험 분석은 잠재적인 피해 수준을 현금 및 기타 자산으로 파악한다.

  보호할 필요가 있는 내용, 다른 대상으로부터 보호해야 할 내용, 그리고 보호하는 방법을 파악하는 것은 사용자의 모든 위험을 조사하고 심각성 수준별로 이러한 위험들에 대해 등급을 매기는 과정을 말한다.

- **위험 평가 (Risk Assessment)**

  컴퓨터 시스템의 취약성, 위험, 가능성, 손실 또는 영향, 그리고 보안 조치의 이론적 효과 등에 관한 연구를 말한다. 예상 손실을 파악하고 시스템 운영에 대한 수용성 정도를 확립하기 위해 위험 및 취약성을 평가하는 과정으로 알려져 있다.

- **위협 평가 (Threat Assessment)**

  정보 시스템에 대한 위협의 정도를 공식적으로 평가하고 위협의 성격을 설명하는 과정을 말한다.

- **유선급 프라이버시 (WEP [Wire Equivalent Provacy])**

  전송데이터 암호화 표준이다.

- **은닉 바이러스 (Stealth Virus)**

  바이러스가 다양한 수단으로 탐지를 피하는 능력을 말한다. 예를 들어 dir 명령을 변경하여 마지막에 숨어 있는 바이러스 코드의 결과로서 생성된 긴 버전보다는 감염된 파일의 원래 길이를 보여준다.

- **은닉형 악성코드**

  은닉형 악성코드란 보안을 위해 암호화하는 데이터에 숨어드는 악성코드를 말한다. 악성코드는 기본적으로 시스템을 감염시킨 후 지속적으로 남아서 악의적인 기능을 하고자 한다. 그러다 보니 악성코드 제작자는 사용자나 백신 프로그램 및 기타 보안 시스템에 발견되지 않도록 그 기술을 점점 정교하게 악용하고, 이에 따라 현재의 다양하고 교묘한 은닉 기능들이 발견되고 있다.은닉형 악성코드에는 레진(Regin), 뱅킹 악성코드인 '다이어(Dyre)' 등이 있다.

  응용 계층 게이트웨이 [방화벽] (Application Level Gateway [Firewall])

  TCP 연결 상태와 순서화를 통제하는 과정에 따라 네트워크 활동을 관리하는 방화벽 시스템을 말한다.

응용 프로그램 수준 방화벽은 종종 트래픽의 주소를 다시 지정하여 외부로 나가는 트래픽이 내부 호스트보다는 오히려 방화벽에서 시발하는 것처럼 보이게 한다.

- **응용 계층 보안 (ALS [Application Layer Security])**

  HTTP 기반에서 S-HTTP의 장점을 수용한 응용 계층 보안 프로토콜이다.

- **이더넷 (Ethernet)**

  LAN(근거리 통신망)에서 컴퓨터를 네트워크로 묶는 가장 일반적인 방법으로, 이더넷은 10Mbit/sec으로 처리가 가능하며 거의 모든 종류의 컴퓨터에서 사용될 수 있다.

- **이더넷 스니핑 (Ethernet Sniffing)**

  사용자에게 관심이 되는 패킷을 찾아내고 이더넷 인터페이스 소프트웨어를 사용하여 도청하는 행위를 말한다. 소프트웨어가 특정 기준을 만족하는 패킷을 찾으면, 이를 파일로 기록한다. 이러한 패킷 중 일부에는 로그인이나 암호와 같은 단어가 포함될 수 있다.

- **인적 보안 (Personnel Security)**

  분류된 정보에 접근하는 모든 사람들이 적합한 통과 절차뿐만 아니라 요청한 허가를 받을 수 있도록 보장하기 위해 확립된 절차를 말한다.

- **인증 (Authentication)**

  인증은 한 개인을 식별하는 보안 절차를 의미한다. 이 과정에서 개인은 자신이 누구라고 주장하도록 보장하지만 개인의 접근 권한에는 영향을 미치지 않는다. 사용자 이름, 패스워드 및 생체측정 스캐닝 등은 모두 인증 기술들이다.

  인증에는 크게 두가지가 있다.

  1. 사용자/과정/장치 인증보안 시스템에서는 모든 사용자들이 다른 시스템 작동을 수행하기 전에 스스로를 식별하도록 요구한다. 인증은 접근을 시도하는 사용자를 검증하는 과정이다. 사용자 인증의 일차적 방법은 다음과 같다.

  1) 접근 패스워드(사용자가 알고 있는 것)

  2) 접근 토큰(사용자가 소유하고 있는 것)

3) 생체측정(지문, 손금 또는 음문 등 사용자에게 존재하는 것)

4) 지리(위치) (특정 워크스테이션 등)

2. 데이터 인증데이터의 무결성이 위험에 노출되지 않았음을 검증하는 과정이다.

- **인증 (Certification)**

  지정한 일련의 보안 요구 사항 및 표준과 일치하는지 시스템에서 결정하기 위한 보안 시스템의 공식 평가를 말한다.

  주요 인가 표준에는 미국의 TCSEC와 유럽의 ITSEC 스키마가 있다. 이 표준과 다른 표준은 공통 기준(CC)로 대체될 것으로 예상된다. 공통 기준은 새로운 인가 표준으로 기존 표준의 최고 기능들이 통합되어 있다.

- **인증 헤더 (Authentication Header [AH])**

  IP 데이터그램에서 IP 헤더 바로 다음에 오며, 데이터그램에 대한 인증 및 무결성 확인을 제공하는 필드를 말한다.

- **인터넷 프로토콜 보안 워킹 그룹 (IPsec WG [Internet Protocol Security Working Group])**

  IPsec WG에서는 IP의 client 프로토콜에 대한 보호를 제공하기 위한 방법을 개발하고 있으며 데이터에 대한 기밀성, 무결성, 접근 제어 및 인증 등의 보안 서비스를 복합적이고 유연하게 제공하기 위한 네트워크 계층에서의 보안 프로토콜에 대한 연구 및 표준화를 진행하고 있다. 현재까지 IPsec WG에서는 AH, ESP, IKE, 데이터 암호 알고리즘 및 데이터 인증 알고리즘 등의 기본적인 보안 프로토콜이 RFC(Request For Comments)로 완성되어 있는 상태이다.

- **인터넷 프로토콜 보안 원격 접속 워킹 그룹 (IPsra WG [Internet Protocol Security Remote Access Working Group])**

  IPsra WG에서는 일명 "Road-Warriors"라 불리는 휴대용 이동 단말기를 사용하여 지역 ISP(Internet Service Provider)를 통한 유선 접속 및 원격지에서 유무선 LAN을 통한 접속

시 보안 서비스를 제공하기 위한 절차 및 프로토콜에 대한 표준화를 진행하고 있다.

- **인터넷 프로토콜 보안 정책 워킹 그룹 (IPsp WG [Internet Protocol Security Policy Working Group])**

  IPsp WG에서는 보안 정책 서비스를 제공하기 위한 두 가지 모델로 정책 저장소와 독립적인 모델(Repository-Independent Information Model)과 정책 저장소와 관련된 모델(Repository-Specific Data Model) 등을 고려하고 있으며, 정책 규격 언어인 SPSL(Security Policy Specification Language)에 대한 개발과 확장, 정책 교환 및 협상을 위한 SPP OPS (Security Policy Protocol)에 대한 개발이 이루어지고 있다.

- **접근 중재 (Access Mediation)**

  접근 중재는 정보 시스템의 자원에 대한 접근을 감시하고 통제하는 처리, 승인하지 않은 접근이나 적당하지 않은 접근 등의 방어뿐만 아니라, 접근하는 동안 정책 특성에 대한 감시나 갱신에도 제한을 두지 않는 것을 말한다.

- **접근 토큰 (Access Token)**

  해당 소프트웨어 또는 하드웨어와 연결하여 사용할 경우 해당 시스템에 대한 허가된 접근을 허용하는 보안 장치로 정상적으로는 시스템의 COM 포트에 부착된다. 이러한 보안 장치의 예로는 스마트카드와 스마트카드 판독기, 터치 메모리 장치가 있다.

- **정보보안 관리시스템 (ISMS [Information Security Management System])**

  정보보호의 목적인 정보자산의 비밀성, 무결성, 가용성을 실현하기 위한 절차와 과정을 체계적으로 수립·문서화 하고 지속적으로 관리·운영하는 시스템이다. 즉, 조직에 적합한 정보보호를 위해 정책 및 조직 수립, 위험관리, 대책구현, 사후관리 등의 정보보호관리 과정을 통해 구현된 여러 정보보호대책들이 유기적으로 통합된 체계이다.

- **정보보안 관제서비스**

  고객사의 정보보안과 관련된 상황을 24시간 모니터링 하여 이상징후를 조기에 탐지/분석하며, 침해사고가 발생하게 되면 침해사고에 대한 복구/분석을 제공하는 서비스

- **정책 (Policy)**

  정책은 정보의 계산 및 관리에 관한 한 조직 내의 규칙 또는 규정으로 정보는 조직에서 보유한 파일의 전체적 보안에 기여한다. 훌륭한 보안 시스템은 잘 구조화된 보안 정책에서 시작되지만, 조직에서 이를 인식하지 못할 경우 많은 침해 사고가 발생한다.

  보안 정책은 조직의 보안 목적과 이러한 목적을 성취하는 방법을 정하는 규칙의 집합을 말하며, 명백하고 완벽하게 문서화 하여 시행해야 한다. 보안 정책은 두가지 부분, 즉 이슈 정책과 기능 정책으로 분류된다.

  (1) 이슈 정책 : 조직의 관심 분야와 이에 대한 조직의 태도를 지정하기 위해 필요하다.

  (2) 기능 정책 : 이슈정책을 충족시킬 수 있는 방법에 대한 역할을 정의한다. 이 방법은 하드웨어 및 소프트웨어 사양과 활용 정책을 필요로 하고 스탭의 행동 정책도 필요로 한다.

- **제3의 신뢰 기관 (Trusted Third Party)**

  암호화 등 트랜잭션을 가능하게 하는 보안 관련 서비스 및 안전하게 수행해야 할 인증을 제공하는 은행 또는 전문 상담소 등의 신뢰를 받을 만한 조직을 말한다.

  유럽 및 전세계를 통해 수많은 정부에서 구현하거나 제안한 다양한 스키마 하에서 강력한 암호화를 사용하는 회사들은 조직 범죄, 마약 또는 테러리즘 등을 수사하는 집단 등 법집행 집단에게 키를 공개하기 위해 제3의 신뢰 기관과 함께 회사의 암호화 키 사본을 보유해야 한다.

- **제로데이공격 (Zero-Day Attack)**

  해킹에 악용될 수 있는 시스템 취약점에 대한 보안패치가 발표되기 전에, 이 취약점을 악용해 악성코드를 유포하거나 해킹을 시도하는 것을 말한다. 보안패치가 나오기 전까지는 이를 근본적으로 막을 수 없다는 점에서 가장 우려하는 공격 형태이다.

- **제우스 (ZeuS)**

  가장 대표적인 인터넷 뱅킹 악성코드 및 봇넷(BotNet) 생성 킷(kit)으로 금융 거래 증명서

를 훔치거나 자동결제시스템, 급여 시스템의 비인증 온라인 거래를 하는 등의 범죄의 주범으로 지목되고 있다.

- **제한 수신 시스템 (CAS [Conditional Access System])**

  방송 사업자의 비즈니스와 수익을 보호하는 목적으로 유료 방송 서비스에 대한 고개의 접근 여부를 제어하는 시스템이다.

- **조건 규칙-중심 보안 정책 (Term Rule-Based Security Policy)**

  모든 사용자들에게 부과된 전체 규칙에 기초한 보안 정책을 말한다. 이 규칙들은 일반적으로 접근하는 자원들의 기밀성과 해당 속성을 가진 사용자들의 소유, 즉 사용자 그룹, 또는 사용자들을 대신하여 활동하는 기관의 소유를 비교하는 것에 의존한다.

- **조크 (Joke)**

  악의적인 목적이 없이 사용자의 심리적인 동요나 불안을 조장하는 가짜 컴퓨터 바이러스 또는 프로그램으로써, 물질적인 피해는 없으나 백신에서 진단/삭제한다. 대표적으로 하드디스크를 포맷하는 화면을 보여주는 Win-joke/Format Game이나 공포스런 얼굴을 작업중에 갑자기 나타나게 하여 놀라게 하는 고스트(Win-Joke/Ghost) 등이 있다.

- **좀비피씨 (Zombie PC)**

  악성코드에 감염된 컴퓨터를 말하며 주로 공격자의 명령을 받아 특정 서비스를 방해할 목적으로 DDoS 공격 등을 수행한다.

- **종합위험관리시스템 (RMS [Risk Management System])**

  기업 내 IT자원의 취약점 및 위험요소들을 분석, 평가 해 사전에 보안사고를 예방하는 능동형 솔루션으로 IT자산의 가치, 취약점의 위험도, 위협의 심각성 등의 상관 관계를 정확하게 산출, 최적의 보안위험 관리를 지원, 위험 방어 위한 정책 설정이다.

- **청색 폭탄 (blue bomb [WinNuke or nuking])**

  Winnuke라고도 불리우는 청색폭탄은 처리 불가능한 과도한 양의 네트워크 대역을 넘어

서는 패킷을 말하며 이를 다른 시스템 사용자에게 전송함으로써 시스템 운영체제를 다운시키는 원인을 제공한다. 운영체제는 저장하지 못한 데이터 이 외에 피해 없이 다시 구동이 가능하며 청색 폭탄이란 용어는 상황이 발생했을 시에 윈도우 운영체제가 파란 에러 화면을 나타난 것에서 기인한다. 현재는 대부분의 ISP가 청색폭탄이 도달하기 전에 패킷을 필터링 한다.

- **체스트 (Chest)**

  스마트폰 사용자의 소액결제 및 개인정보 탈취 등을 유발하는 모바일 악성코드를 말한다.

- **추적 라우터 (Tracerouter)**

  정보를 파악하기 위해 추적 패킷을 보내는 작용을 말하며 지역 호스트의 UDP 패킷을 원격 호스트로 하여 라우트하는 것을 추적한다. 정상적으로 추적 라우트는 대상 컴퓨터에 도달하는데 걸린 라우트의 시간 및 위치를 표시한다.

- **추적 패킷 (Trace Packet)**

  패킷 교환망에서 각각의 방문 시스템 요소로부터 네트워크 제어 센터로 전송될 과정의 각 단계를 보고하는 고유한 패킷을 말한다.

- **취약성 (Vulnerability)**

  컴퓨터 시스템 즉, 하드웨어, 소프트웨어, 펌웨어 등의 시스템에서 제기되는 보안상의 결점을 말한다. 자동화 시스템 보안 절차, 관리상 제어, 물리적 배치, 내부 제어 등이 취약하면 인가를 받지 않은 접근에 의해 중요한 정보가 침해 당할 수 있다. 이를 방지하기 위해 암호화, 침입탐지, 침입차단 등의 다양한 보안 기법이 이용되고 있다.

- **취약성 분석 (Vulnerability Analysis)**

  정보 시스템 또는 제품에 대해 보안 결함 여부를 확인하고, 이미 제안되어 있는 보안 대책의 적합성과 효과성을 분석해 본다. 이에 따라 보안 대책을 구현하고, 또한 그 대책이 적합한지 확인하는 일련의 검사 과정을 말한다.

- **침입 방지 시스템 (IPS [Intrusion Prevention System])**

  능동형 보안솔루션이라고도 불리는 IPS는 인터넷 웜, 악성코드 및 해킹등에 기인한 유해 트래픽을 차단하는 네트워크 보안 기술 중 예방적 차원의 시스템에 해당한다. 악의적인 공격에 대한 공격탐지를 하고 설정해 놓은 규칙에 기반한 즉각적인 대응이 가능한 시스템이라고 할 수 있다. 전송된 특정 패킷을 점검하여 부적절한 패킷이라 판단되면 해당 포트 및 IP에 대한 연결을 봉쇄하고 적절한 패킷에 대해서는 지연 없이 바로 전달한다. 탐지 기법으로는 주소 대조, HTTP 스트링과 서브스트링 대조, 일반 패턴 대조, TCP 접속 분석, 변칙적인 패킷 탐지, 비정상적인 트래픽 탐지 및 TCP/UDP 포트 대조 등이 있다.

- **침입 탐지 시스템 (IDS [Intruision Detection System])**

  침입 탐지 시스템(IDS)은 네트워크 시스템 파일과 로그인을 감시하여 컴퓨터 시스템에 침입하거나 이를 악용하려는 침입자를 찾아낸다.

  침입 탐지 시스템의 두 가지 주요 유형은 익명적 탐지(anomaly detection)와 악용 탐지(misuse detection)이다. 익명적 탐지기는 정상적인 시스템 사용에서 발생하는 행동을 탐지하며, 악용 탐지기는 알려진 공격 시나리오와 일치하는 행동을 탐지한다.

- **침입감내시스템 (ITS [Intrusion Tolerant System])**

  침입과 결함이 일부 발생하여도 데이터와 프로그램의 일관성을 유지하고 DoS 공격에 대항하는 차세대 정보보증 기술을 말한다.

- **침입방지시스템 (IPS (Intrusion Prevention System))**

  자체적으로 내장된 각종 해킹수법을 기반으로 비정상적인 트래픽에 대해 능동적으로 해당 트래픽을 차단, 격리 등 방어조치를 취하는 보안 솔루션.

- **침입탐지시스템 (IDS (Intrusion Detection System))**

  자체적으로 내장된 각종 해킹수법을 기반으로 컴퓨터 시스템의 비정상적인 사용, 오용, 남용 등을 실시간으로 탐지하는 보안솔루션. 네트워크 기반(NIDS)과 호스트기반(HIDS)으로 구분되나, 국내에서는 일반적으로 NIDS를 IDS라 칭함.

- **침투 테스트 (Penetration Testing)**

  시스템 소유자의 허가를 받아 시스템의 보안에 대해 합법적으로 침투를 시도하는 보안 보안 테스트의 일종이다. 침투자들은 모든 시스템 설계 및 구현 문서를 사용할 수 있는 것으로 가정할 수 있으며, 여기에는 시스템 소스 코드 목록, 설명서 및 회로 다이어그램 등이 포함될 수 있다. 침투자들은 일반 사용자들에게 적용되는 제약과 달리 아무런 제약도 받지 않고 작업을 한다.

  침투 테스트의 목적은 해커들이 이용할 수 있는 취약점들을 찾아내어 제거하는 것으로, 테스트를 위한 침투자들은 타이거 팀이라고도 불리며, SATAN과 같이 자동화 소프트웨어 피캐지를 사용하기도 한다.

- **카이텐 (Kaiten)**

  카이텐(Kaiten)은 쓰나미(Tsunami, Sunami), Sunam 등으로도 불리는 DDoS 공격 악성코드이다. 2002년 처음 발견된 이후 2014년에 변종이 등장했다.

- **컨텐트 보안 (Content Security)**

  컨텐트 보안은 조직이 데이터 흐름을 통해 전자우편 또는 웹 바이러스 등의 위협으로부터 컨텐트의 손실, 전자우편을 통한 기밀 정보 유출, 또는 전자우편을 통한 명예훼손이 확산되지 않도록 보장해준다. 참고적으로 방화벽은 한 네트워크에서 다른 네트워크로 연결할 때 사용자들 또는 서비스를 허용하거나 거부하는 역할을 수행한다.

- **크래커 (Cracker)**

  크래커는 인가를 받지 않고 컴퓨터 시스템에 접근하려고 시도하는 사람이다. 해커와는 구별되는 의미로, 이 사람들은 다양한 수단을 이용하여 악의적으로 시스템에 침입한다. 해커가 선의와 악의를 동시에 나타낸다면, 크래커는 악의적으로 피해를 주는 부정적인 해커로 간주되기도 한다. 이런 의미에서 본다면 크래커는 피해를 입히거나 데이터를 훔치려는 특수한 목적을 가지고 다른 시스템에 침입하는 해커라고 할 수 있다.

- **트래픽 패팅 (Traffic Padding)**

네트워크 트래픽 분석을 방지하기 위해 본래의 데이터 흐름에 임의의 암호문 등의 방해 데이터를 흘려서 정보유출을 막는 방법을 말한다.

- **트랩 도어 (Trap Door)**

  컴퓨터 범죄 수법의 하나로 시스템 설계자나 유지보수자가 고의적으로 컴퓨터 보안에 구멍을 남겨놓은 것을 말한다. 백 도어와 유사한 개념으로 이 숨겨진 구멍(소프트웨어 또는 하드웨어 메커니즘)은 보안 제어를 파괴하기 위해 사용된다.

- **트랩와이어 (Trapwire)**

  보안용 소프트웨어 도구를 말한다. 기본적으로 트랩와이어는 파일의 바이트 카운트에 관한 정보를 유지 관리하는 데이터베이스와 함께 작동한다.

  바이트 카운트가 변경되면 트랩와이어는 시스템 보안 관리자에게 변경 사항을 알려준다.

- **트로이 목마 (Trojan Horse)**

  옛 오딧세우스 소설에서 이름을 가져다 붙인 트로이 목마는 컴퓨터 시스템에서 정상적인 기능을 하는 프로그램으로 가장해 다른 프로그램 안에 숨어 있다가 그 프로그램이 실행될 때 자신이 활성화하는 악성 프로그램을 말한다.

  컴퓨터 바이러스와 달리 자기 복사 능력은 없지만, 자기자신이 실행되는 순간 시스템에 직접적인 피해를 가하는 특징을 가지고 있다.

  트로이 목마 프로그램은 고의적으로 포함되었다는 점에서 프로그래머의 실수인 일명 버그(Bug)와는 다르며, 자기 자신을 다른 파일에 복사하지 않는다는 점에서 컴퓨터 바이러스와 다르다. 따라서 어떤 프로그램을 실행시켰을 때 하드 디스크의 파일을 지우되 다른 프로그램에 복사되지 않으면, 이것은 컴퓨터 바이러스가 아니라 트로이 목마 프로그램이라 할 수 있다.

  현재까지 수많은 트로이 목마들이 발견되었으며, 가장 대표적인 것이 백오리피스(Back Orifice)이다. 종래의 트로이 목마 프로그램은 실행시 하드 디스크를 포맷해 버리는 등 그 자체로 피해를 주는 형태가 주종을 이루었지만, 최근의 백오리피스와 같은 프로그램은 여기서 나아가 백도어(Back door) 방식으로 시스템이나 사용자 정보를 몰래 빼오는 형태가 많아지는 추세이다.

  트로이 목마 프로그램은 일반적인 백신 프로그램에 그에 해당하는 진단/삭제 기능을 추

가함으로써 퇴치가 가능하지만, 그 대처 방법은 컴퓨터 바이러스와는 차이가 있다.

컴퓨터 바이러스는 다른 프로그램에도 감염될 수 있기 때문에 한 프로그램에서 컴퓨터 바이러스가 발견되면 다른 프로그램도 모두 검사해 봐야 한다. 이에 반해 트로이 목마 프로그램은 자기 복사 능력이 없어 한 프로그램 내에서만 존재하기 때문에 백신으로 검사해도 치료가 불가능하다. 그러나 그 프로그램만 지워버리면 문제가 간단히 해결된다.

- **파밍 (Pharming)**

  합법적인 사용자의 도메인을 탈취하거나 도메인 네임 시스템(DNS) 또는 프록시 서버의 주소를 변조함으로써 사용자들로 하여금 진짜 사이트로 오인하여 접속하도록 유도한 뒤 개인정보를 탈취하는 공격 기법이다.

- **파싱 (Parsing)**

  언어 해석기인 컴파일러 또는 인터프리터가 프로그램을 이해하고 해석한 후 기계어로 번역하는 작업이다. 다시 말해 프로그램의 구성 요소(연산자, 피연산자, 키워드 등), 구문(프로그램 문법)을 해석해 기계어로 번역하는 과정을 말한다. 또한 인터프리터의 개념으로 임의의 데이터를 사람이 식별가능한 데이터로 변환하는 작업도 파싱이라고 부른다.

- **파일 감염자 (File Infector)**

  자신이나 자신의 일부 또는 자신의 복사본을 다른 파일에 부착하는 바이러스를 말한다.

- **파일 배치표 (FAT [File Allocation Table])**

  하드 디스크는 디스크에 파일 위치를 기록한 표를 포함하는 이 파일 시스템을 사용하여 파일을 저장하고 복구한다. MS-DOS, Windows 3.x 및 Windows 95(그리고 일부 경우의 Windows NT)에서 하드 또는 플로피 디스크의 데이터 영역으로서 파일이 디스크에 저장된 장소를 운영 체제가 찾을 수 있게 한다.

  디스크의 물리적 손상, 불완전한 소프트웨어나 바이러스 등으로 인한 FAT 손상은 전문가와 소프트웨어 도구 등을 사용하여 수정될 수 있다.

- **혼잡 모드 (Promiscuous Mode)**

원래 NIC은 기본적으로 자기의 MAC주소와 일치하거나, Broadcast 패킷만 받도록 설정되어 있다. 그런데, 스니퍼를 실행하게 되면 자신의 NIC는 아무거나 받아들이게 된다. 이러한 모드를 Promiscuous mode라고 한다. 만약 자신의 시스템의 NIC가 Promiscuous mode로 동작한다면 스니퍼가 실행된다고 생각하면 된다.

- **확장형 인증 프로토콜 (EAP [Extensible Authentication Protocol])**

  다양한 인증 메카니즘을 수용하는 확장 가능한 인증 프로토콜이다.

- **힙 스프레이 기법 (Heap Spraying)**

  자바스크립트를 이용하여 Heap 메모리 영역에 뿌리듯이(Spraying) 쉘코드를 채우는 방식으로, 주로 엑티브엑스(ActiveX) 또는 인터넷익스플로러 취약점을 통해 공격자가 원하는 명령(쉘코드)을 수행하기 위해 사용되는 기법이다.