

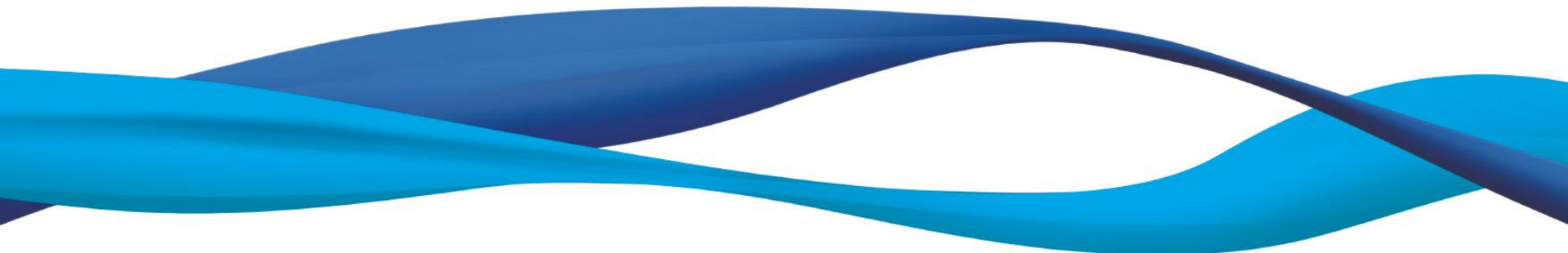
1장. 컴퓨터 보안 개요

개요, 보안위협, ICT 보안위협

박중혁

서울과학기술대학교 컴퓨터공학과

jhpark1@seoultech.ac.kr



- 1-1. 컴퓨터보안 개요
- 1-2. 보안위협
- 1-3. 최근 ICT 서비스보안 위협

1-1. 컴퓨터 보안 개요

컴퓨터 보안 (정보 보호) 개념

컴퓨터보안?

“자동화된 정보 시스템내의 자원(하드웨어, 소프트웨어, 펌웨어, 정보/데이터, 통신)들의 무결성, 가용성, 기밀성을 보존하기 위해 제공되는 보호”

- NIST 컴퓨터 보안 핸드북[NIST95]



정보보호 ?

- 정보보호(Information Security)의 법률적 의미

"정보보호'란 정보의 수집, 가공, 저장, 검색, 송신, 수신 중 발생할 수 있는 정보의 훼손, 변조, 유출 등을 방지하기 위한 관리적·기술적 수단을 마련하는 것"¹⁾

- 정보보호의 사전적 의미

"정보의 수집, 가공, 저장, 검색, 송신, 수신 중에 정보의 훼손, 변조, 유출 등을 방지하기 위한 관리적·기술적 수단 또는 그러한 수단으로 이루어지는 행위"²⁾

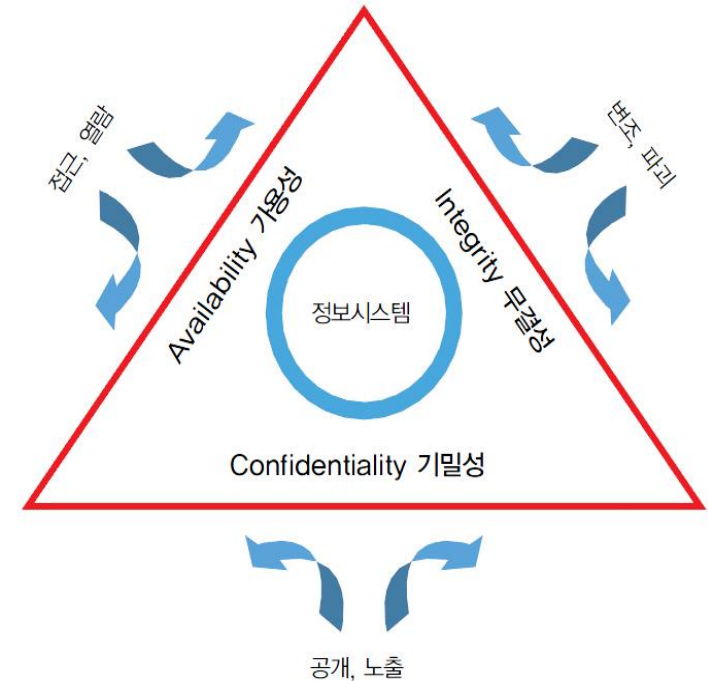
일반적으로 정보는 **기밀성(Confidentiality)**, **무결성(Integrity)**, **가용성(Availability)**을 유지해야 함

1) 「국가정보화 기본법」 제3조제6항

2) 한국정보통신기술협회의(TTA, Telecommunications Technology Association) 용어의 정의

정보보호의 기본 목표(3대 목표)

- 기밀성(Confidentiality)
 - 허락되지 않은 사용자 또는 객체가 정보의 내용을 알 수 없도록 하는 것
- 무결성(Integrity)
 - 허락되지 않은 사용자 또는 객체가 정보를 함부로 수정할 수 없도록 하는 것
- 가용성(Availability)
 - 허락된 사용자 또는 객체가 정보에 접근하고자 할 때 방해 받지 않도록 하는 것



정보보호의 3요소

6대 목표는 아래 3항목 추가

- 책임추적성(Accountability)
- 인증성(Authentication)
- 신뢰성(Reliability)

정보보호의 기본 목표(6대 목표 추가분)

- **책임추적성(Accountability)**

- 각 객체의 행위를 유일하게 추적할 수 있음을 보장하는 것

- **인증성(Authentication)**

- 어떤 주체나 객체가 틀림없음을 보장할 수 있는 것이며 정보시스템 상에서 이루어지는 어떤 활동이 정상적이고 합법적으로 이루어진 것을 보장하는 것

- **신뢰성(Reliability)**

- 의도된 행위에 대한 결과의 일관성을 유지하는 것으로 정보나 정보시스템을 사용함에 있어서 일관되게 오류의 발생 없이 계획된 활동을 수행하여 결과를 얻을 수 있도록 하는 환경을 유지하는 것

정보보호의 특성 및 중요성

• 정보보호의 특성

“정보는 유출, 접근 불능, 변형 또는 잘못된 공개와 같은 여러 종류의 취약점을유발하는 각종 위협으로부터 피해를 입지 않도록 보호되어야 함”

• 정보보호의 목적

“정보를 필요로 하는 사람들의 이익 및 정보를 전달하기 위한 정보시스템을 가용성, 기밀성 및 무결성의 실패로 인한 피해로부터 보호하는 것”

컴퓨터 보안 용어

용 어	의 미
공격자	시스템을 공격하거나 위협하는 존재
공격	시스템의 보안 서비스를 회피하여 보안 정책을 위반하려는 의도된 시도
대응	위해를 최소화하거나 적절한 대응을 위해 탐지, 보고하여 위협, 노출, 공격을 제거하거나 방지하는 행위, 장비, 기법
위험	특정 위협이 가져올 확률적으로 표현되는 예상되는 손실
보안 정책	시스템이나 기관이 민감하고 중요한 시스템 자원들에 보안 서비스를 제공하기 위해 명시한 규정과 업무
시스템 자원 (자산)	정보 시스템내의 데이터, 시스템의 서비스, 처리 기능, 통신 대역폭, 시스템 장비(하드웨어, 펌웨어, 소프트웨어, 문서), 시스템 장치 설비
위협	보안을 침해하고 손해를 가져올 수 있는 상황, 행위, 이벤트가 존재할 때 잠재적 보안 위반
취약성	시스템 보안 정책을 위반할 수 있는 시스템 설계, 구현, 혹은 운영, 관리상의 오류 혹은 약점

- 자료: RFC 2828, internet Security Glossary



인증 서비스 (Authentication)

- 통신개체가 주장하는 것처럼 실제 당사자인지를 확인 해주는 서비스
- 인증되지 않은 메시지의 수령이나 전송을 합법적인 것처럼 가장한 제 3자가 통신연결을 방해하지 못하도록 보장해줌

• 데이터 근원지 인증

- 데이터 발신 출처에 대한 보증을 제공하는 서비스
- 데이터의 복제나 변경에 대한 보호는 제공하지 않음
- 통신개체간 비연결적 전송을 하는 전자우편과 같은 어플리케이션 지원

• 피어 인증

- 피어의 식별자에 대한 확증 제공
- 연결 성립 혹은 데이터 전송 시에 제공
- 피어가 매스커레이드나 이전 연결의 재생 같은 행위를 못하도록 보장

접근제어 서비스 (Access Control)



부인방지 서비스 (Non-repudiation)

- 통신 링크를 통한 호스트 시스템과 어플리케이션 접근을 제한하고 제어하는 서비스
- 접근 권한을 부여하기 위해 접근 시도자에 대한 신원을 확인하거나 접근 시도에 대한 인증이 이루어져야 함

- 통신의 한 주체가 메시지를 전송 혹은 수신했던 사실에 대해 부인하는 것을 방지해 주는 서비스
- 수신자는 메시지가 인증된 송신자로부터 발송된 것임을 알 수 있음
- 송신자는 인증된 수신자가 메시지를 수신했음을 알 수 있음



데이터 기밀성 서비스 (Confidentiality)

- 수동적 공격으로부터 전송되는 데이터를 보호하는 것
- 브로드캐스트 서비스는 일정시간 내 두 사용자간에 전송되는 모든 사용자 데이터를 보호
- **연결기밀성**
 - 연결 상의 모든 사용자 데이터 보호

- **트래픽 흐름의 분석 방지**
 - 공격자가 소스, 목적지, 빈도, 길이 혹은 통신 설비상의 트래픽 특성을 관찰하지 못하도록 하게 함
- **비연결 기밀성**
 - 단일 데이터 블록에 대한 모든 상용자 데이터 보호
- **선택적-필드 기밀성**
 - 연결 상의 사용자 데이터 혹은 단일 데이터 블록의 선택된 필드에 대한 기밀성
- **트래픽-흐름 기밀성**
 - 트래픽 흐름 관철에서 파생된 정보 보호



데이터 무결성 서비스 (Integrity)

- 수신된 데이터가 인증된 개체가 보낸 것과 정확히 일치하는지를 확인해주는 서비스
- 비연결 무결성 서비스는 단일 비 연결 데이터 블록의 무결성을 제공하는 서비스로서, 데이터 수정을 탐지하여 이를 보호함

- 연결지향 무결성 서비스는 수신된 메시지가 복제, 추가, 수정, 순서 바꾸기, 재전송 등이 없도록 보호
 - 데이터 제거에 대한 사실 탐지
 - 메시지 스트림 수정과 서비스 거부탐지
- 복구가 있는 연결 무결성과 복구가 없는 연결 무결성 간의 차별화가 있어야 함
 - 복구가 있는 연결 무결성: 예방보다는 탐지에 중점
 - 복구가 없는 연결 무결성: 자동화된 복구 매커니즘들의 병합이 보다 적극적인 대안이 될 수 있음



가용성 서비스 (Availability)

- 시스템 및 자원의 접근이 적시에 제공되게 해주는 서비스
 - 시스템 사양에 따라 인가된 시스템으로 하여금 자원에 접근할 수 있도록 해줌
- 다양한 종류의 공격에 의해 가용성의 손실 또는 손상을 가져올 수 있음
 - 인증이나 암호화는 일부 공격을 처리할 수 있음
 - 그러나, 다른 공격들은 가용성 손실의 예방과 복구를 위한 물리적 대처가 요구됨
- X.800에서는 가용성을 보안 서비스와 연관하여 다루고 있음
- 서비스 거부 공격과 연관된 보안 문제에 역점을 둠
- 시스템 자원의 적절한 관리와 제어에 중점을 둠

컴퓨터 보안 전략

명세서 / 정책

하고자 하는것은
무엇인가?

구현 / 메커니즘

어떻게 하는가?

정확성/ 확실성

잘 동작되고
있는가?

보안 정책

- 시스템이나 조직이 민감하고 치명적인 시스템 자원에 제공하는 보안 서비스 방법에 대한 일반적 형식의 규칙이나 관행
- 고려 사항:
 - 보호하고자 하는 자산의 가치
 - 시스템 취약점
 - 잠재적인 위협과 공격 가능성
- 고려해야 할 절충사항:
 - 사용의 용이성 VS 보안성
 - 보안 비용 VS 오류 및 복구 비용



보안 구현



1-2. 보안 위협

- 2.1. 보안 취약점, 위협, 정보보호대책
- 2.2. 컴퓨터 보안 위협
- 2.3. 인터넷 보안 위협
- 2.4. 모바일 보안 위협
- 2.5. 주요 보안침해 사례

2.1 보안 취약점, 위협, 정보보호대책

보안 취약점(Security Vulnerability)

- 사전적인 의미

“컴퓨터의 하드웨어 또는 소프트웨어의 결함이나 운영체제 설계상의 허점으로 인해 사용자의 허용된 권한 이상의 동작이나 허용된 범위 이상의 정보 열람을 가능하게 하는 약점”

- 넓은 의미

“사용자나 관리자의 부주의 및 사회공학 기법에 의한 약점을 포함한 정보 체계의 모든 위험성”

- 또 다른 의미

“정보자산의 잠재적 속성으로써 위협의 이용 대상”

• 일반적인 보안 취약점은 물리적, 기술적, 관리직으로 구분

구 분		내용
물리적	물리적 취약점	침입자는 정보처리시설과 같이 정보시스템이 설치되어있는 건물이나 서버 또는 개인용 컴퓨터가 설치되어있는 특정장소에 침입 할 수 있음. 일단 침입에 성공하면 시스템 파괴, 부품 탈취와 같은 다양한 수단의 불법 행위를 할 수 있음
	자연적 취약점	정보시스템은 화재, 홍수, 지진, 번개 등의 자연 재해에 취약함
	환경적 취약점	정보시스템은 먼지, 습도, 온도 등의 주변 환경에 취약함
기술적	하드웨어 취약점	하드웨어 오류나 오동작이 전체 정보시스템의 보안에 손상을 입힐 수 있음
	소프트웨어 취약점	소프트웨어의 실패는 시스템을 실패나 오동작으로 보안에 취약하게 만들거나 시스템을 불안정하게 만들 수 있음
	매체 취약점	자기디스크, 자기테이프, 출력물 등은 손실되거나 손상을 입을수 있음
	전자파 취약점	모든 전자 장치는 전자파를 방출하기 때문에 도청자는 정보시스템, 네트워크, 모바일로부터 발생하는 신호를 가로챌 수 있음
	통신 취약점	컴퓨터가 네트워크나 모뎀 등에 연결된 경우 인가 받지 않은 사람이 침입할 위험성이 증가함
관리적	인적 · 관리적 취약점	정보시스템을 사용하거나 관리하는 직원은 가장 위험한 취약점을 보임 관리자가 적절한 교육을 받지 않았거나 보안 의식이 부족한 경우, 컴퓨터 사용자나 운용자 및 기타 직원들의 기밀 정보 누설, 시설물 주요 출입구를 열어 두는 등의 행동 등을 할 수 있음

보안 위협(Security Threats)

• 정의

“자산에 손실을 초래할 수 있는, 원치 않는 사건의 잠재적 원인이나 행위자”

• 일반적인 보안 위협

- 내부자에 의한 중요 기밀정보 유출 위협
- 사회 공학적 공격 위협
- TCP/IP 프로토콜의 취약점 이용 위협
- 서비스거부 공격(DDoS 등)
- 스파이웨어의 위협
- 정보 도청 위협
- 접근통제 위협
- 정보보호 정책 수립 및 이행 등 관리적 위협

• 보안 위협의 분류

분 류		내 용
자연에 의한 위협		화재, 홍수, 지진, 전력 차단 등 자연에 의한 대표적인 위협으로부터 발생하는 재난을 항상 예방 할 수 없지만 화재경보기, 온도계, 무정전 시스템 등을 설치하여 피해를 최소화 할 수 있음
인간에 의한 위협	비의도적 위협	• 정보시스템의 보안 사고를 일으키는 가장 큰 위협으로 인간의 실수와 태만이 주된 원인임. • 패스워드의 공유, 데이터 백업의 부재 등이 대표적인 부주의와 태만으로 간주되며, 이러한 위협은 언론매체에서 크게 다루어지지 않는 않지만 실제 정보보호 문제를 일으키는 가장 중요한 요인임
	의도적 위협	컴퓨터 바이러스, 해커, 사이버 테러리스트 등으로부터 발생하여 도청, 신분 위장에 의한 불법 접근, 정당한 정보에 대한 부인, 악의적인 시스템 장애 유발 등이 있음

정의정보보호대책(Countermeasure)

• 정의

“위협에 대응하여 정보자산을 보호하기 위한 관리적, 물리적, 기술적 대책”

- 방화벽, 침입탐지시스템 등의 정보보호시스템 뿐만 아니라 정책, 지침, 절차 등의 모든 통제사항이 포함

• 보호대책을 선택 시 중요한 점

- 위험분석을 통해 조직의 환경과 문화에 맞는 것을 선택하는 것

• 비용 산정 시 고려해야 하는 점

- 구축비용뿐만 아니라 운영에 따른 관리비용을 반드시 고려해야 함

2.2 컴퓨터 보안 위협

• 바이러스

- 자기복제알고리즘을 이용하여 시스템을 작동불가 상태로 만드는 특수하게 제작된 프로그램
- 컴퓨터의 운영체제 또는 부트 데이터를 삭제함
- 생물학적 바이러스와 유사하게 컴퓨터와 컴퓨터간 접촉을 이용하여 다른 컴퓨터에 전염시킴

발생기원설

- 1949년 존 폰 노이만이 발표한 자기복제알고리즘이 시초
- 1972년 데이비드제롤드의 공상과학소설에서 구체적으로 언급된 자기복제를 통한 컴퓨터감염이 시초
- 1985년 최초 바이러스발생 (브레인 바이러스)
알비 형제(파키스탄)이 불법소프트웨어에 대해 불만을 품고 유포

• 바이러스의 구분

- 컴퓨터바이러스는 영향 정도에 따라 악성과 양성으로 감염 부위에 따라 부트와 파일 바이러스로 구분함

• 부트 바이러스

- 컴퓨터가 시작될때 가장 먼저 실행되는 부트 지역을 목표로함
- 컴퓨터 부팅이 시작되고 POST 작업을 시작할 때 활동함
- 주로 플로피디스크나 하드디스크의 부트섹터에 감염

* POST 작업

PC전원이 켜지고 가장먼저 문제점 유무를 점검하는 작업으로 BIOS를 통해 실행되고 하드웨어 문제점이 발견되면 비트음으로 사용자에게 문제점을 알림

• 파일 바이러스

- 파일에 직접적으로 감염
- 하드디스크에 저장된 파일을 대상으로 활동함
- 일반적으로 COM이나 EXE와 같은 실행파일 또는 디바이스 파일, 드라이버 파일 등을 대상으로함
- 파일 바이러스는 감염된 실행파일을 실행할때 컴퓨터를 감염시킴

• 바이러스의 감염과 증상

- 컴퓨터 부팅시간 지연 혹은 부팅자체에 오류가 발생
- 특정 프로그램이 느려지거나 실행되지 않음
- 사용자가 실행하지 않은 작업(프로그램)이 실행됨

• USB에 의한 바이러스의 감염과정

- PC를 통한 USB 감염과정

1. 바이러스에 감염된 컴퓨터에 USB메모리 접속



2. USB메모리에 바이러스가 침투



3. 바이러스를 실행하는 autorun.inf를 USB메모리에 생성

- USB를 통한 PC 감염과정

1. 바이러스에 감염된 USB메모리를 컴퓨터의 접속



2. 바이러스 실행

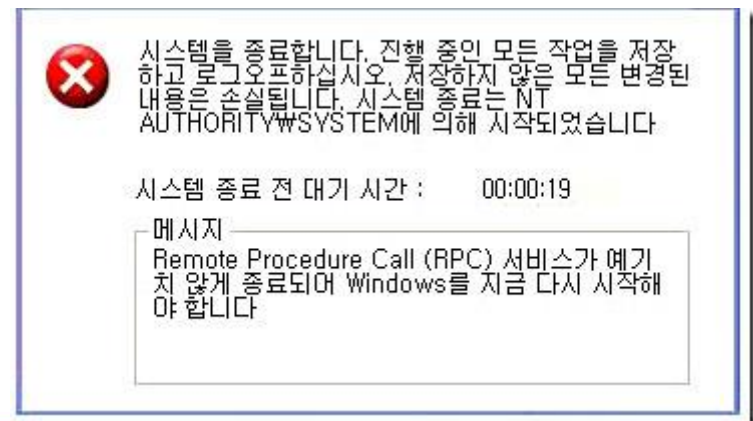
3. 바이러스를 컴퓨터에 복사



4. autorun.inf 파일이 바이러스에 감염

• 웜

- 스스로 자기자신을 복제하는 프로그램
- 직접적으로 다른 프로그램, PC에 악영향을 끼치지 않음
- 복제작업이 무한으로 반복되면서 컴퓨터 자원을 고갈시켜 컴퓨터 시스템을 정지 시킴
- 바이러스와 달리 다른 프로그램에 감염되는 것이 아닌 독립된 형태로 프로그램이 존재하며 동작함
- 확산 속도 및 범위가 바이러스보다 넓으며 스스로 전파함
- 대표적인 웜으로 모리스, 님다, 슬래머, 블래스터 웜이 있음



1. 모리스 웜(Morris Worm)

- 최초의 웜으로 1988년 11월에 발생함
- 당시 인터넷에 접속된 6만여대의 PC중 약 10%정도 감염시켰으며 피해액이 최대 1천만달러에 이름
- 배포자 로버트 모리스는 수사과정에서 인터넷의 크기를 파악하려는 의도로 배포하였다고 주장함.

2. 님다 웜 (Nimada Worm)

- 2001년에 등장한 웜으로 클라이언트와 서버를 통해 전파됨
- 발생 22분만에 인터넷을 장악하였고 E-mail을 통해 배포
- 당시 MS사의 Outlook또는 IE에서 파일을 실행하지않고 메일을 보기만 해도 자동으로 감염되었음

3. 슬래머 웜(SQL Slammer)

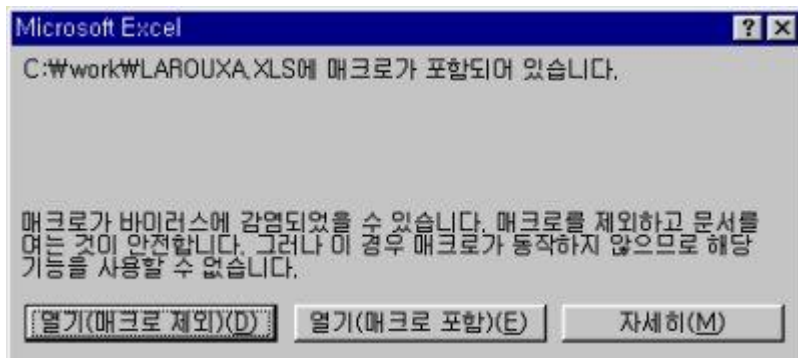
- 2003년 1월 인터넷 호스트에 서비스 거부 공격(Dos)를 실시한 웜
- 30분만에 급속도로 확산되어 전세계 7만 5천여대를 감염
- 이메일이나 메신저로 전파되는 기존 웜과 달리 시스템 취약점을 기반으로 웜코드가 실행되어 인터넷 대란을 일으킴

4. 블래스터 웜(Blaster Worm)

- 2003년 MS사의 윈도우 NT계열을 통해 급속하게 확산된 웜
- PC메모리 소모를 일으켜 운영체제를 파손
- 감염 현상으로 오류 메시지와 함께 윈도우 재부팅을 유도
- 전세계 20만대나 감염되었으며 국내에서도 피해가 많이 발생됨
- 메일, 운영체제 보안취약점에 전파되기도 하지만 메모리에 상주하고 있다가 전파되는 웜 형태도 있음

• 매크로 바이러스

- 1997년 발생하였으며 특정기능을 자동화시키는 약식 프로그램 (매크로)을 악의적 목적으로 감염시킨것을 말함
- 기존 EXE, 드라이버 실행파일 뿐만 아니라 엑셀, 워드와 같은 문서의 매크로 기능을 이용하여 문서파일에도 감염
- 전자 우편 파일 첨부, 디스크, 네트워크, 모뎀, 인터넷등 다양한 방법을 통하여 확산함
- 자동화된 키놀림으로 프로그램 종료, 사용자 인증 등을 시도 및 방해 하고 메일, 문서 등에서 찾은 주소록 등을 통해 자동으로 스팸 메일, 메시지를 발송하는 등 2차 보안 위협을 발생시킴



3. 인터넷 보안 위협

• 스파이웨어(Spyware)

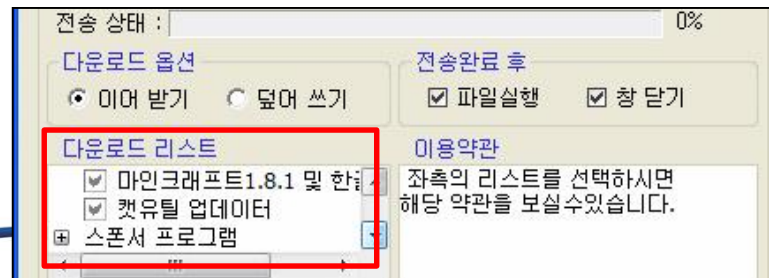
- 자신이 감염시킨 시스템 정보(운영체제, 네트워크)를 원격지의 특정한 서버에 주기적으로 보내는 기능의 프로그램
- 초기에는 사용자가 주요 이용하는 사이트, 검색어 등을 파악하는데 이용되었으나 이후 패스워드, 인증 정보 등 중요한 정보를 가로채는 역할을 수행하는 것으로 확장
- 최근 안티스파이웨어가 성행하고 있어 사용자에게 각별한 주의가 요구됨

* 안티스파이웨어(Anti-Spyware)

- 웹 배너 광고를 통해 스파이웨어에 감염되었다는 메시지를 사용자에게 경고로 보여주고, 스파이웨어를 실제로는 제거하지 않는 프로그램을 설치하도록 유도함
- 위 과정에서 더 심각한 경우, 오히려 실제 스파이웨어를 설치하는 사례도 있음
- 국내의 경우 인터넷 익스플로러의 취약점(ActiveX)을 이용해 웹 서비스를 빌미로 사용자에게 설치를 유도함
- 안티스파이웨어 역시 스파이웨어와 같이 감염 PC에서 중요한 정보를 탈취함

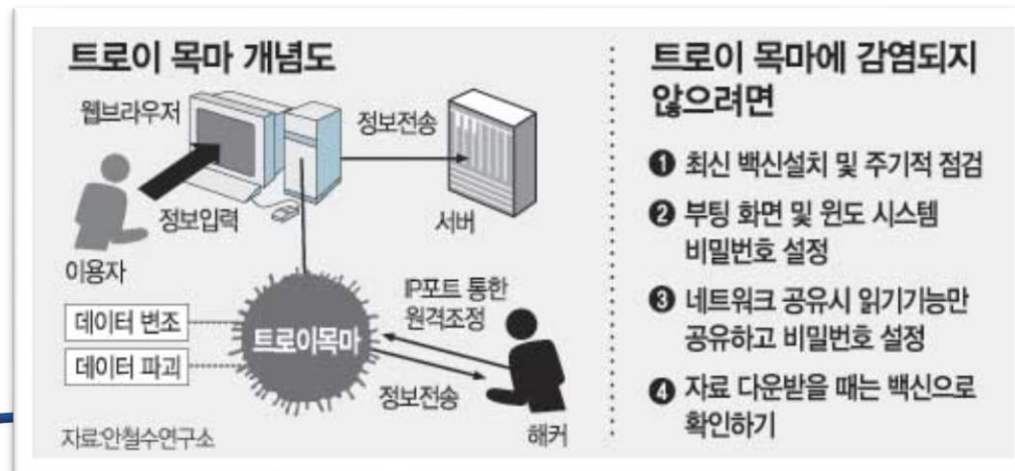
• 애드웨어(Advertising-supported software, Adware)

- 사용자가 의도하지 않은 툴바, 검색 도우미, 팝업창 광고창 등을 설치하는 프로그램
- 인터넷 프로그램이 다운되거나 속도저하, 의도하지않은 웹사이트 방문 및 팝업 실행 등 인터넷 사용에 악영향을 끼침
- 애드웨어의 경우 위협행위에는 속하지 않아 바이러스, 스파이웨어, 웜 등과 달리 정상적인 프로그램이기 때문에 백신으로 치료가 잘 되지 않음
- 일부 애드웨어는 스파이웨어 기능으로 확장하여 사용자가 인터넷에서 사용하는 개인정보를 제3자에게 전송하는 역할도 함
- 최근 무료 응용프로그램 (프리웨어) 설치 등을 할 때 광고 수입을 위해 애드웨어 설치를 같이 유도하는 경우가 일반적이기 때문에 설치 과정에서 애드웨어 설치 항목에 대해 주의가 필요함



• 트로이 목마(Trojan horse)

- 고대 그리스-트로이 전쟁에서 사용된 목마의 활용과 유사함
- 공격자가 원격으로 컴퓨터를 제어하여 파일을 탈취하거나 위협요소를 컴퓨터에 침투할 수 있게 해주는 모든 프로그램을 말함
- 바이러스나 웜처럼 자가복제 또는 컴퓨터에 피해를 주지 않음
- 사용자에게 유용한 목적의 프로그램으로 접근하여 설치를 유도하고 설치 후에 사용자가 알아채지 못하게 PC에 원격 접근하여 2차 보안 위협을 발생시킴
- 최근 트로이 목마는 프로그램 삭제를 시도할 경우 설치된 PC의 시스템을 파괴하거나 무한부팅 등을 발생 시키는 경우가 있어 주의해야함



• 백도어(Backdoor)

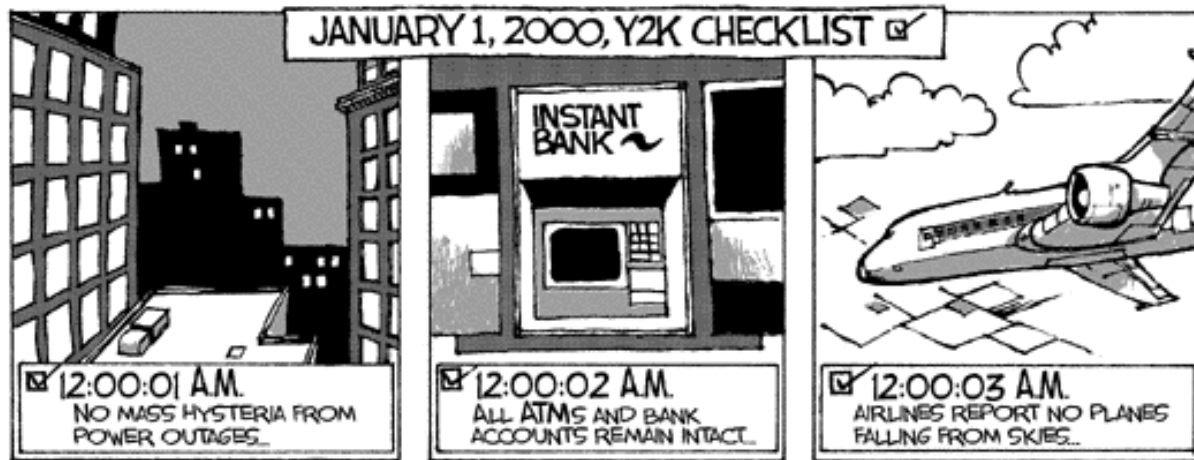
- 운영체제나 프로그램을 생성할 때 정상적인 인증 과정을 거치지 않고, 운영체제나 프로그램에 접근할 수 있도록 만든 통로
- 주로 시스템이 고장났을 경우, 빠른 대응을 위해 보안 절차 없이 접속 및 점검 할 수 있도록 특정 계정이나 코드를 열어놓은 것
- 이후 불순한 의도를 가진 자가 재침입을 위한 시도로써 출입할 수 있는 보안 허점(시스템 침입 통로, 뒷문)을 만들어 놓는다는 의미로 통용됨
- 백도어의 위협은 다중 사용자와 네트워크 운영 체제가 널리 받아 들여지면서 표면화 됨
- 대표적으로 리눅스 개발에서 공격자가 악의를 목적으로 특정부분에 백도어를 생성을 시도하다가 발견된 사례가 있음

• hoax(Hoax)

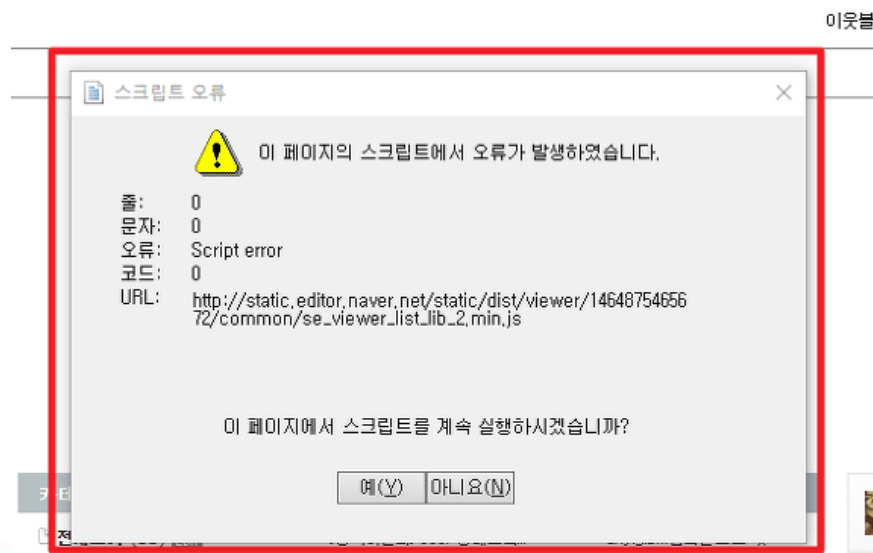
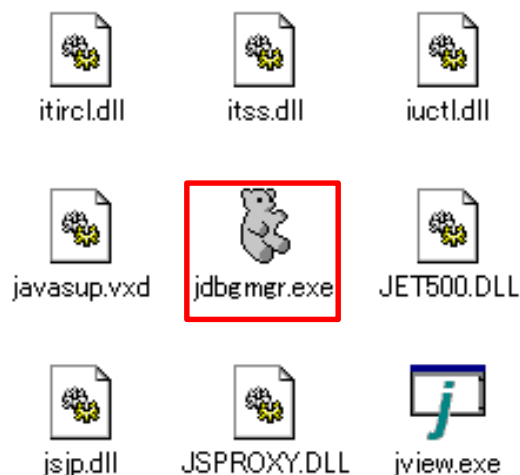
- 인터넷 메신저, 이메일, 커뮤니티 등에 거짓정보나 괴담등을 실어 사용자를 속이는 가짜 컴퓨터 바이러스를 지칭
- 국내에서는 1997년부터 나타나기 시작해 만우절 전후로 많이 발생

* 대표적인 예

- 1) 1999년에 사회 전반에서 2000년 1월 1일 자정 이후에 Y2K 전산오류로 산업이나 경제, 전기 등이 중단되어 치명적인 곳에 문제를 일으킬 것이라는 우려. 금융데이터 초기화, 시스템 종말 등 각종 유언 비언 및 괴담과 신문 및 방송 매체 예측 보도로 인해 세계적으로 사회적 파장 및 혼란과 피해를 일으킴. 하지만 컴퓨터는 비트 값(이진수)을 사용하기에 십진수의 자리수 변화로 인한 전산오류는 일어나지 않음.

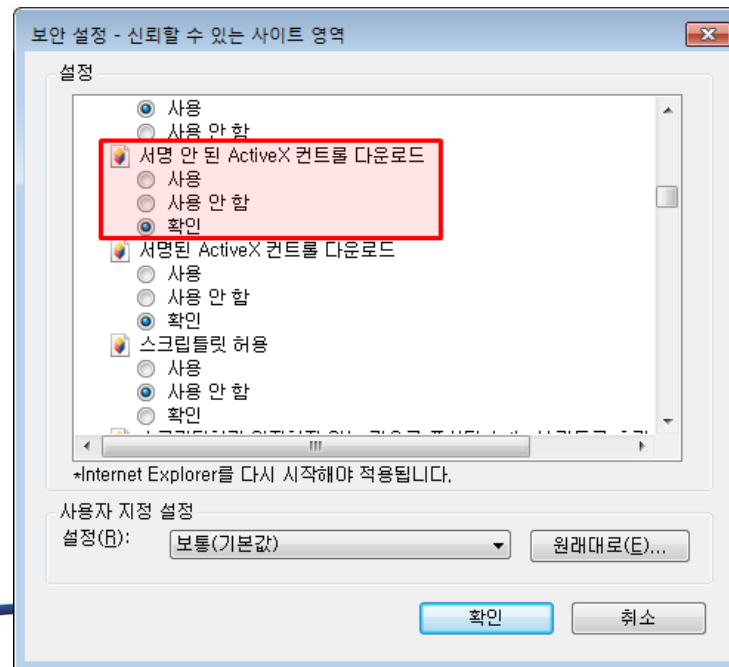


- 2) 조언자를 가장한 공격자가 'jdbgmgr.exe' 파일 이용자들을 속인 사례가 있음.
- 위 파일은 실제로 바이러스 프로그램이었으나 2주 뒤 바이러스 프로그램이 아닌 파일로 변형되었음. 초기 현상으로 인해 바이러스에 감염됐다고 생각하는 사용자 또는 백신들에게 이 파일을 제거하도록 각인 시킴.
 - 이 컴포넌트는 실제로 JDM(Java Debugger Manager)이면서 윈도우 시스템에 설치된 자바소프트웨어의 일부분으로 추가되었으며, 이 파일이 지워지면 일부 자바 애플릿과 자바스크립트가 작동에 오류를 일으킴



• 악성 액티브X

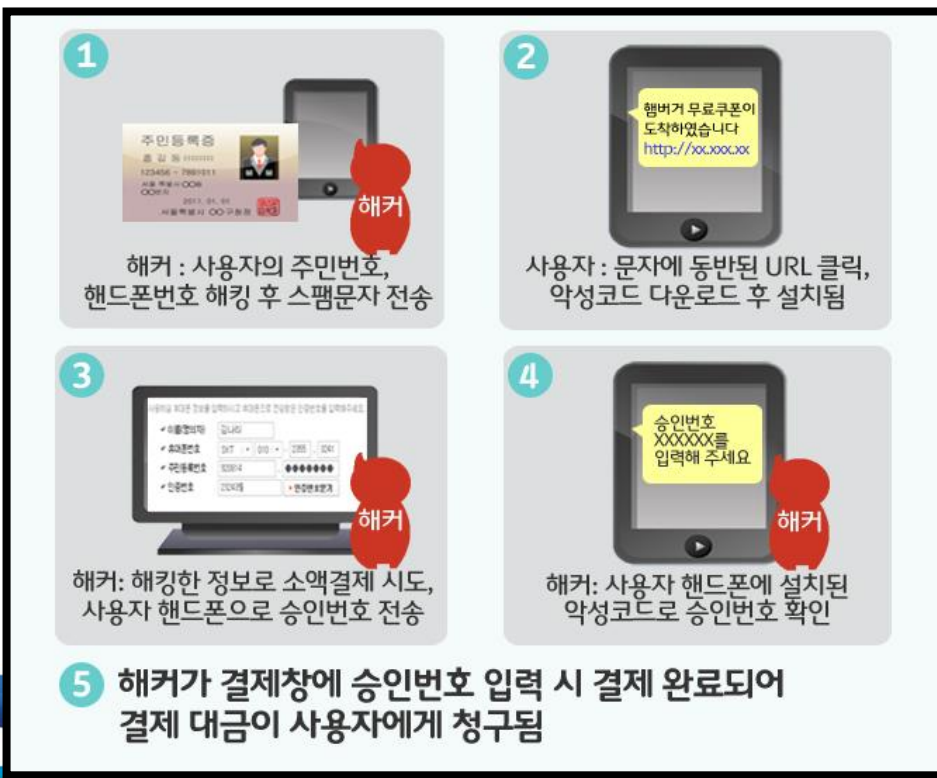
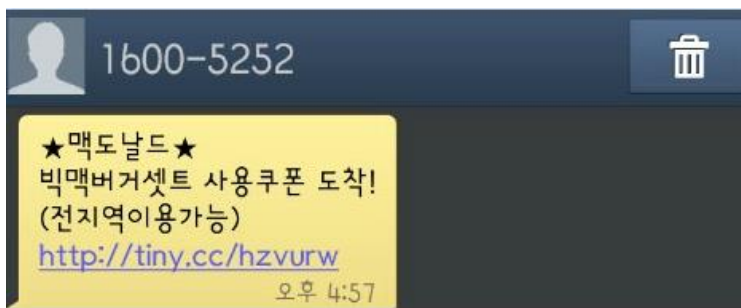
- 액티브X는 MS사에서 배포한 객체지향 프로그래밍을 위한 도구 모음을 지칭
- 악성 액티브X는 인터넷 익스플로러의 시작페이지 변경, 속도저하 등 인터넷 사용을 방해함
- 시스템 비정상 작동을 유발 시켜 운영체제 사용 불능을 발생시킴
- 인터넷 익스플로러의 옵션 설정으로 예방이 가능함



2.4 모바일 보안 위협

• 스미싱(Smishing)

- 스마트폰 사용자를 타깃으로 스팸성 광고 문자를 보내 악성코드를 유포하고 금액을 결제하는 방식으로 금품을 갈취하는 보안위협
- SMS+Fishing이 결합된 이름으로 사용자에게 거짓정보 또는 광고로 URL 링크를 보내고 사용자가 이 링크에 접근할 때 트로이목마 등을 설치하여 사용자 휴대폰을 통제함

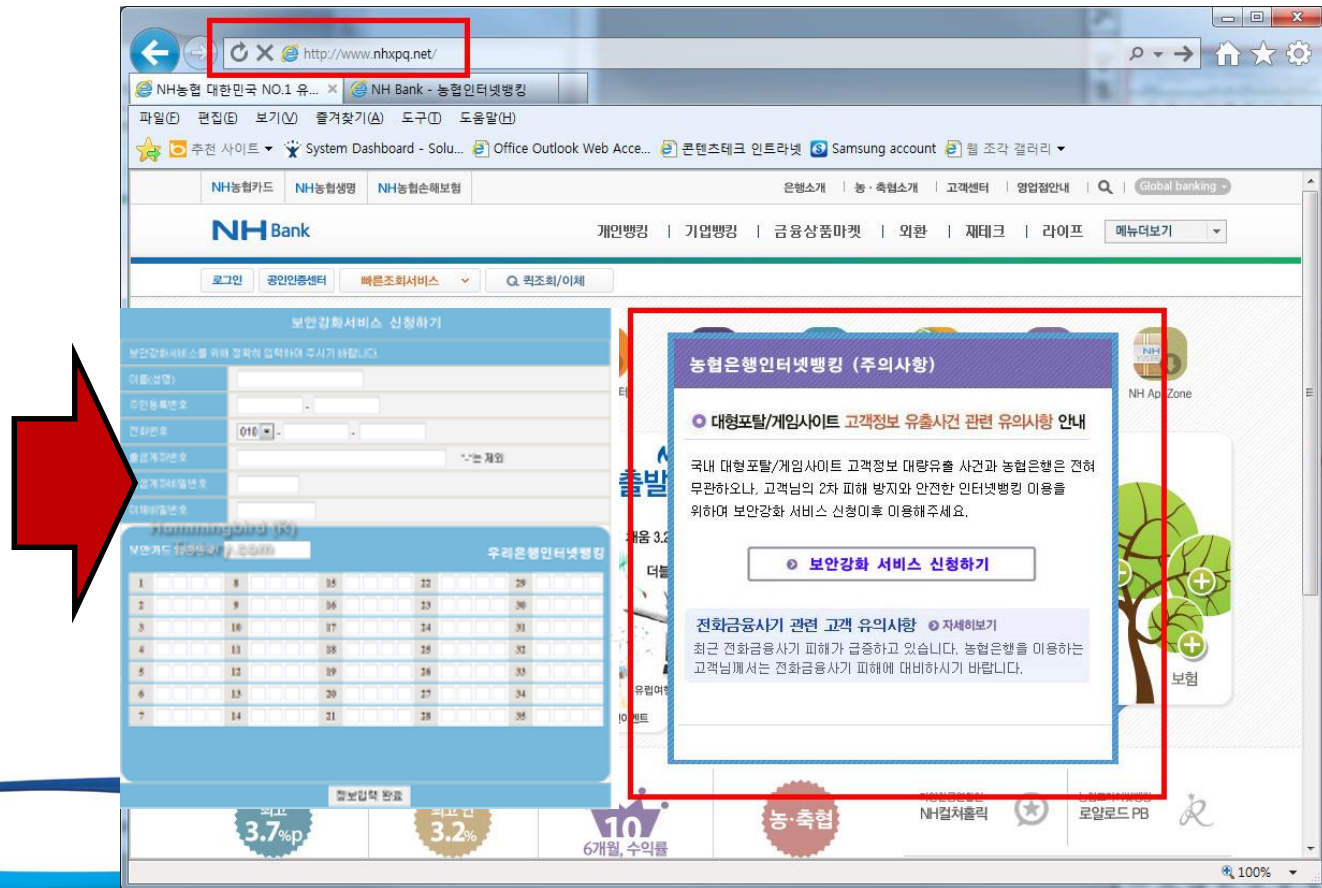


• 피싱(Phishing)

- 피싱은 경찰서나 법원 금융 기관등으로 위장하여 사용자 주요 개인정보를 빼내 불법적으로 이용하는 공격
- 스미싱과 같이 유사 URL로 사용자를 속여 위장한 기관 웹사이트를 접속하게 한후 주요 개인정보 입력을 유도하여 정보를 탈취함

• 공식 사이트와 다른
도메인 주소

• 특정 서비스를 미끼
로 개인정보 입력을
유도함



• 파밍(Pharming)

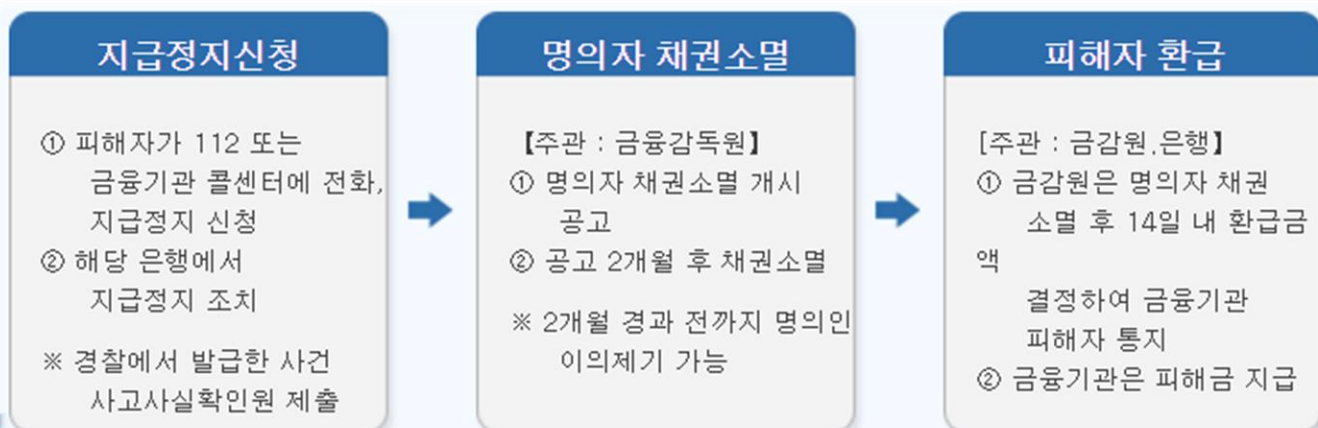
- 파밍은 피싱에 이어 등장한 공격 형태로 해당사이트가 공식적으로 운영하는 도메인 자체를 중간에서 탈취
- 합법적인 사용자의 도메인을 탈취하거나 프록시 서버의 주소를 변조하여 진짜 사이트로 오인하게 하여 유도함
- 피싱보다 발전된 형태라 볼 수 있으며 합법적인 도메인을 사용하기 때문에 사용자들이 쉽게 속게 됨



• 파밍 방지법

- 사이버경찰청, 한국인터넷진흥원(KISA)에서는 다음과 같이 권고하고 있음
- 1. OTP(일회성 비밀번호생성기), 보안토큰(비밀정보 복사방지) 사용
- 2. 컴퓨터·이메일 등에 공인인증서, 보안카드 사진, 비밀번호 저장 금지
- 3. 보안카드번호 전부를 절대 입력하지 말 것
- 4. 사이트 주소의 정상 여부 확인
※ 가짜 사이트는 정상 사이트 주소와 유사하나, 문자열 순서·특수문자 삽입 등에서 차이 있음
- 5. 윈도우, 백신프로그램을 최신 상태로 업데이트하고 실시간 감시상태 유지
- 6. 출처불명 한 파일이나 이메일은 즉시 삭제 및 무료 다운로드 사이트 이용 자제

* 피해가 발생하였을 경우 대처



2.5 주요 보안침해 사례

• 제로데이 공격 (Zero-day Attack)

- 보안 취약점이 발견 되었을 때 그 취약점 존재 자체가 공표되기도 전에 해당 취약점을 악용하여 이루어지는 공격을 제로데이 공격이라고 함
- 일반적으로 프로그램에서 취약점이 발견되면 제작자나 개발자가 취약점을 보완하는 패치를 배포하고 사용자가 이를 내려받아 적용하여 대처라는 것이 일반적
- 하지만 제로데이 공격은 대응책 및 패치가 배포되기 전에 공격이 이루어지기 때문에 대응 방법이 없다는 것이 가장 큰 문제로 대두됨
- 최근 발견되지 않은 취약점을 이용한 공격을 차단하는 연구가 활발히 진행중임



제로데이 공격 과정 및 대응

• 사회 공학적 공격 (Social engineering Attack)

- 사회의 절차나 제도, 사람의 심리 등을 악용하여 특정인이 어떤 행동을 하게하거나 비밀 정보를 노출하게 하는 공격 기법
- E mail, 웹과 같은 기존 악성코드를 활용하여 사용자의 관심 사항, 궁금증 등을 악용하여 불특정 다수에게 URL 전송 및 파일 등을 내려 받게하거나 특정 개인정보를 입력하도록 유도
- 탈취한 정보를 이용하여 2차 보안 공격으로 확장하며 서비스 혹은 금전 피해를 발생 시킴
- 최근에는 사용자가 친숙해 질 때까지 정상적인 메일, 광고 등을 지속적으로 유포한 후 충분한 시간이 지나면 공격을 감행함

구분	기법	
인간기반	직접적인 접근	고위층 위장, 친밀한 관계, 지인을 통한 접근
	도청	도청장치설치, 유선전화 Tapping, 원격감시
컴퓨터기반	시스템 분석	휴지통, 파일복구등을 통한 기밀 데이터 탈취
	악성코드	정상 소프트웨어로 위장 PC 및 USB 감염
	인터넷 이용	구글 검색, SNS를 통한 개인정보 탈취
	피싱	메일, 이벤트 사이트를 통한 개인정보 탈취
	파밍	도메인 만료기간을 이용한 도메인 탈취

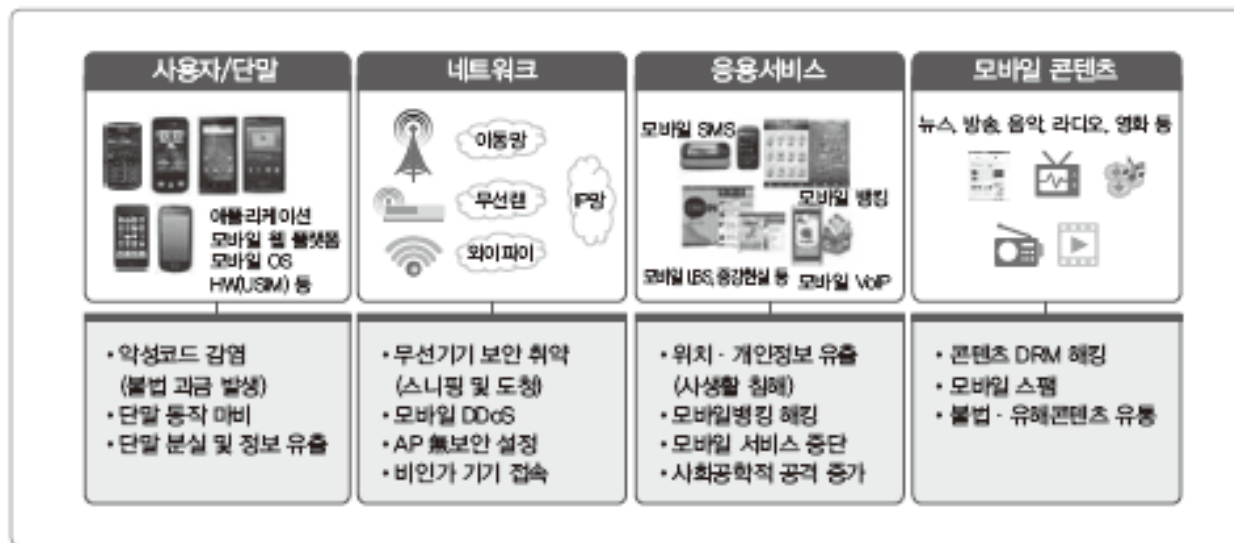
1-3. 최근 ICT 서비스 보안 위협

- 3.1 모바일 보안
- 3.2 클라우드 서비스 보안
- 3.3 빅데이터 보안
- 3.4 사물인터넷 보안
- 3.5 핀테크 보안
- 3.6 OWASP Top 10 RISK
- 3.7 APT 공격
- 3.8 블록체인

3.1 모바일 보안

• 스마트폰 보안 위협

- 최근 폭발적인 스마트폰의 보급과 이용은 우리 삶의 중요한 부분을 담당하고 있음. 그러나 스마트 기기를 대상으로 한 해킹 및 악성코드 감염 등 위협이 증가하고 있음.
- 악성코드뿐 아니라 휴대용 단말이 가지는 특성 등으로 인한 스마트폰의 보안위협은 크게 네 가지로 구분



• 모바일 전자금융서비스 보안 위협

- 모바일 전자금융서비스는 금융 앱을 기반으로 서비스가 제공되기 때문에 앱을 배포하는 경로로 활용될 수 있는 앱 스토어, 블랙마켓, 웹 사이트, 문자메시지, 메신저 등을 이용한 공격이 가능함
- 단말기 자체 특성에 기인하여 PC 등 주변기기와 연동 시 발생할 수 있는 취약점을 이용한 공격 가능성도 존재

• 소셜 네트워킹 환경의 보안 위협

- 스마트 기기의 보급 확대와 함께 소셜 네트워크 서비스(SNS)는 참여하는 구성원 개개인의 다양성을 존중하며 개인과 기업의 새로운 소통의 도구로 자리매김하고 있음
- 소셜 네트워크 서비스에는 많은 개인정보를 담고 있기 때문에 공격자의 주 공격 타겟이며 유출 될 경우 큰 피해를 발생 시킬 수 있음

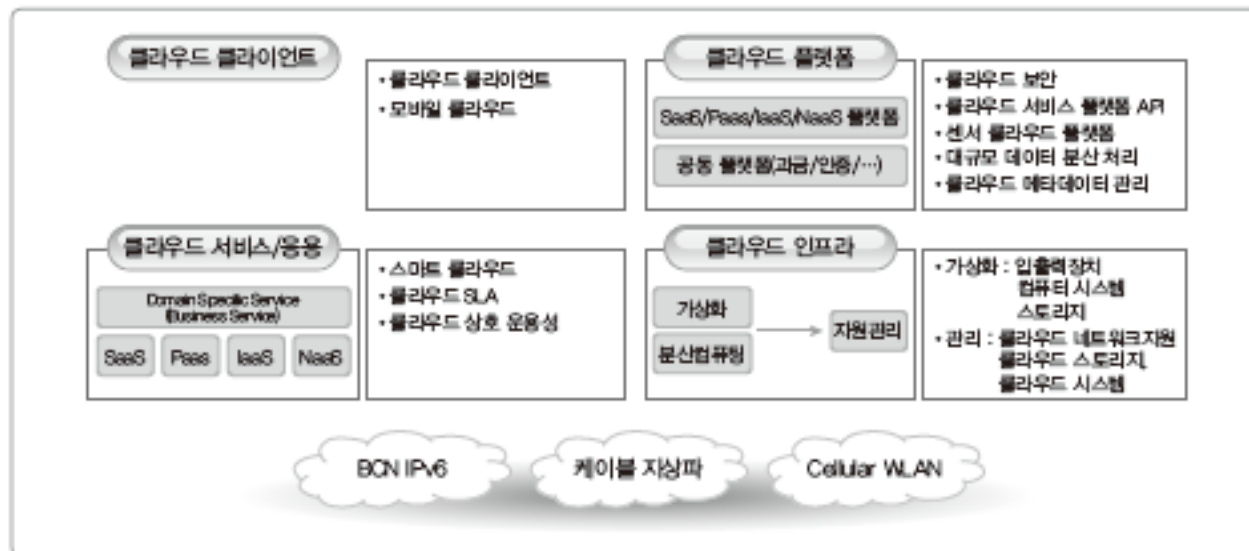
3.2 클라우드(Cloud) 서비스 보안

클라우드 컴퓨팅 개요

- 클라우드 컴퓨팅은 인터넷 기술을 활용하여 IT 자원을 서비스로 제공하는 것으로 IT 자원(소프트웨어, 스토리지, 서버, 네트워크 등)을 필요한 만큼 사용하고 서비스 부하에 따라서 실시간 확장이 가능하며 사용한 만큼 비용을 지불하는 서비스

클라우드 서비스의 보안 위협

- 클라우드 서비스는 기존 IT 환경의 보안 위협과 클라우드 특성에 따른 가상화, 다중 임차(Multi-tenancy), 원격지에 정보 위탁, 사업자 종속, 모바일 기기 접속, 데이터 국외이전, 침해사고 대형화, 데이터센터 안전성 등 신규 공격 위협이 존재



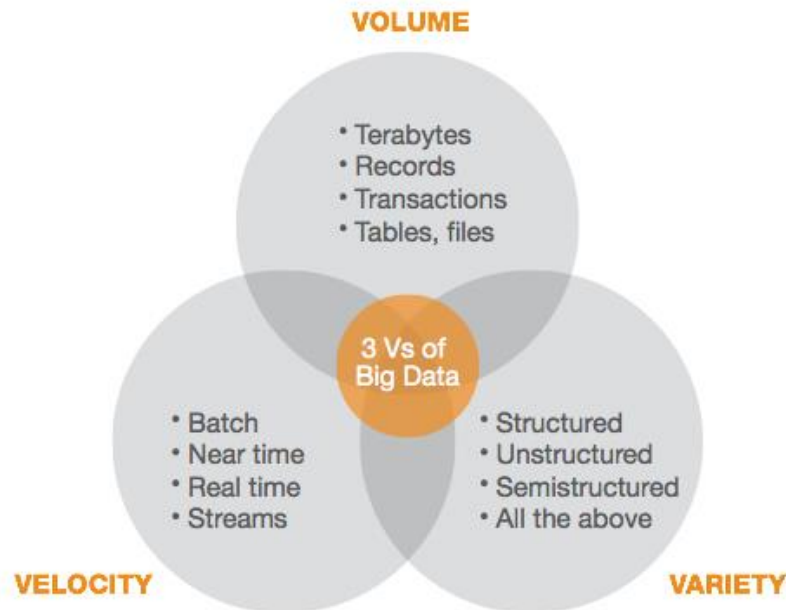
3.3 빅데이터 (Big Data) 보안

- 빅데이터(Big Data)란 ?

- 기존 데이터베이스 관리도구로 데이터를 수집, 저장, 관리, 분석할 수 있는 역량을 넘어서는 대량의 정형 또는 비정형 데이터 집합 및 이러한 데이터로부터 가치를 추출하고 결과를 분석하는 기술

- 빅데이터 3대 요소

- 데이터 양(Volume), 데이터 속도(Velocity), 데이터 다양성(Variety)



• 빅데이터 분석 기술

- 대부분의 빅데이터 분석 기술과 방법들은 기존 통계학과 전산학에서 사용되던 데이터 마이닝(Data Mining), 기계 학습(Machine Learning), 자연 언어 처리, 패턴 인식(Pattern Recognition) 등이 해당됨

• 빅데이터 보안 위협

- 다양한 IT서비스와 플랫폼이 등장하면서 엄청난 양의 데이터가 쏟아지고 있다. 이른바 '빅데이터(Big Data)' 시대가 도래하였고 모바일 기기의 진화와 트위터, 페이스북 등과 같은 소셜 네트워크 서비스의 출현으로 기업들의 기업 내 데이터가 폭발적으로 증가하고 있음.
- 빅데이터의 생성에서부터 서비스에 이르기까지의 단계별 주요 보안 위협
 1. 데이터 생성단계
 2. 데이터 저장·운영 단계
 3. 서비스 단계

3.4 사물인터넷 (IoT, Internet of Things)

• 사물인터넷 개념

- 사물인터넷 IoT(Internet of Things)은 사람, 사물, 공간 등 모든 것들(Things)이 인터넷(Internet)으로 서로 연결되어, 모든 것들에 대한 정보가 생성·수집 되고 공유·활용되는 것을 의미함

• 사물인터넷 기술 요소

- 사물 인터넷의 기술 요소는 센싱 기술, 유·무선 통신 및 네트워크 인프라 기술, 서비스 인터페이스 기술, 보안기술 등 4가지로 구분

1. 센싱 기술

- 필요한 사물이나 장소에 전자태그를 부착하여 주변 상황 정보를 획득하고, 실시간으로 정보를 전달하는 사물 인터넷의 핵심 기술

2. 유·무선 통신 및 네트워크 기술

- 사물이 인터넷에 연결되도록 지원하는 기술로, IP를 제공하거나, 무선통신 모듈을 탑재하는 방식이 대표적인 예

3. 사물 인터넷 서비스 인터페이스

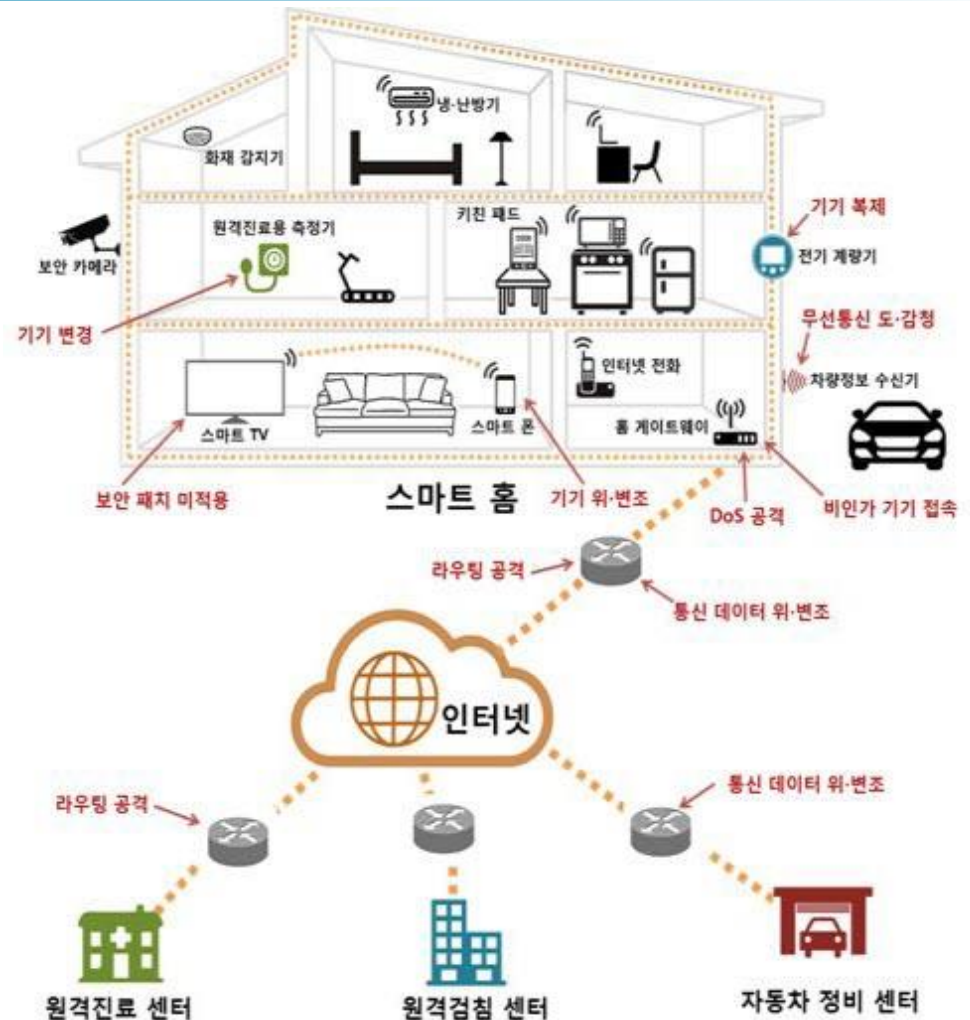
- 사물 인터넷을 구성하는 요소들을 서비스 및 애플리케이션과 연동하는 역할을 수행

4. 보안기술

- 네트워크, 단말 및 센서, 대량의 데이터 등 적용 분야별로 기능·애플리케이션·인터페이스 등이 상이하기 때문에 개별적으로 적합한 보안기술 적용이 요구

• 사물인터넷 보안 위협

- 스마트 홈, 스마트 의료, 스마트 카 등 IoT 서비스가 일상생활로 확산되면서 기존 사이버세계의 위험이 현실세계로 전이(轉移)·확대됨
- 기존 PC, 모바일기기 중심의 사이버 환경과 달리 IoT 환경은 보호대상, 주체, 방법 등에 있어 새로운 정보보호 패러다임으로 접근을 요구함



사물인터넷의 다양한 보안 위협

3.5 핀테크(Fintech) 보안

• 핀테크 개념

- 핀테크는 금융을 뜻하는 '파이낸셜(Financial)'과 '기술(Technique)'의 합성어
- ICT 기술기반 금융서비스 또는 혁신적 비금융기업이 신기술을 활용하여 금융 서비스를 직접 제공하는 현상을 지칭함

• 핀테크 보안

1. 금융 빅데이터 분석 기술

- 핀테크에 있어서 비식별화된 빅데이터를 바탕으로 신 금융상품 개발, 부가서비스 제공, 마케팅 활용, 금융관련 부정행위 방지, 신용평가, 보안 리스크 관리 등 금융 빅데이터 분석기술

2. 이상거래탐지(FDS, Fraud Detection System) 기술

- 전자거래에 사용되는 단말기 정보, 접속정보, 위치정보, 거래내용 등을 종합적으로 분석하여 의심거래를 탐지하고 이상거래를 차단하는 기술

3. 혁신적인 핀테크 보안기술 개발

- 빅데이터와 FDS기술뿐만 아니라 간편결제 보안기술, 사용자 인증기술(PKI, OTP, 생체인식), 암호기술, 내부 정보유출 방지, 모바일 보안, 앱 위·변조 방지 기술

4. 금융 정보보호 거버넌스 체계 구축

- 금융 정보보호 수준 제고를 위해 보안 솔루션과 전사적인 위험관리체계 구축, 경영진의 참여, 지속적인 모니터링, 전담조직 구성 등을 요구

3.6 OWASP Top 10 RISK

- OWASP(Open Web Application Security Project)에서는 각 분야 별 프로젝트에서 가장 심각한 보안 위험 10가지에 대해 발표하고 있음
- 2016각 정보분야별(세로) 가장 심각한 위험(가로)10가지
 - 위험 순위는 OWASP TOP 2013과 동일

OWASP Top 10 – 2013
A1 – 인젝션
A2 – 인증 및 세션 관리 취약점
A3 – 크로스 사이트 스크립팅 (XSS)
A4 – 취약한 직접 객체 참조
A5 – 보안 설정 오류
A6 – 민감 데이터 노출
A7 – 기능 수준의 접근 통제 누락
A8 – 크로스 사이트 요청 변조 (CSRF)
A9 – 알려진 취약점이 있는 컴포넌트 사용
A10 – 검증되지 않은 리다이렉트 및 포워드

OWASP Top 10 Mapping 2016

	A1-Injection	A2-Broken Authentication and Session Management	A3-Cross-Site Scripting (XSS)	A4-Insecure Direct Object References	A5-Security Misconfiguration	A6-Sensitive Data Exposure	A7-Missing Function Level Access Control	A8-Cross-Site Request Forgery (CSRF)	A9-Using Components with Known Vulnerabilities	A10-Unvalidated Redirects and Forwards
C1: Verify for Security Early and Often	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
C2: Parameterize Queries	✓									
C3: Encode Data	✓		✓							
C4: Validate All Inputs	✓		✓							✓
C5: Implement Authentication Controls		✓								
C6: Implement Appropriate Access Controls				✓			✓			
C7: Protect Data						✓				
C8: Implement Logging and IDs	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
C9: Leverage Security Frameworks	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
C10: Error and Exception Handling	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

자료 : OWASP.ORG (OWASP Proactive Controls 2016)

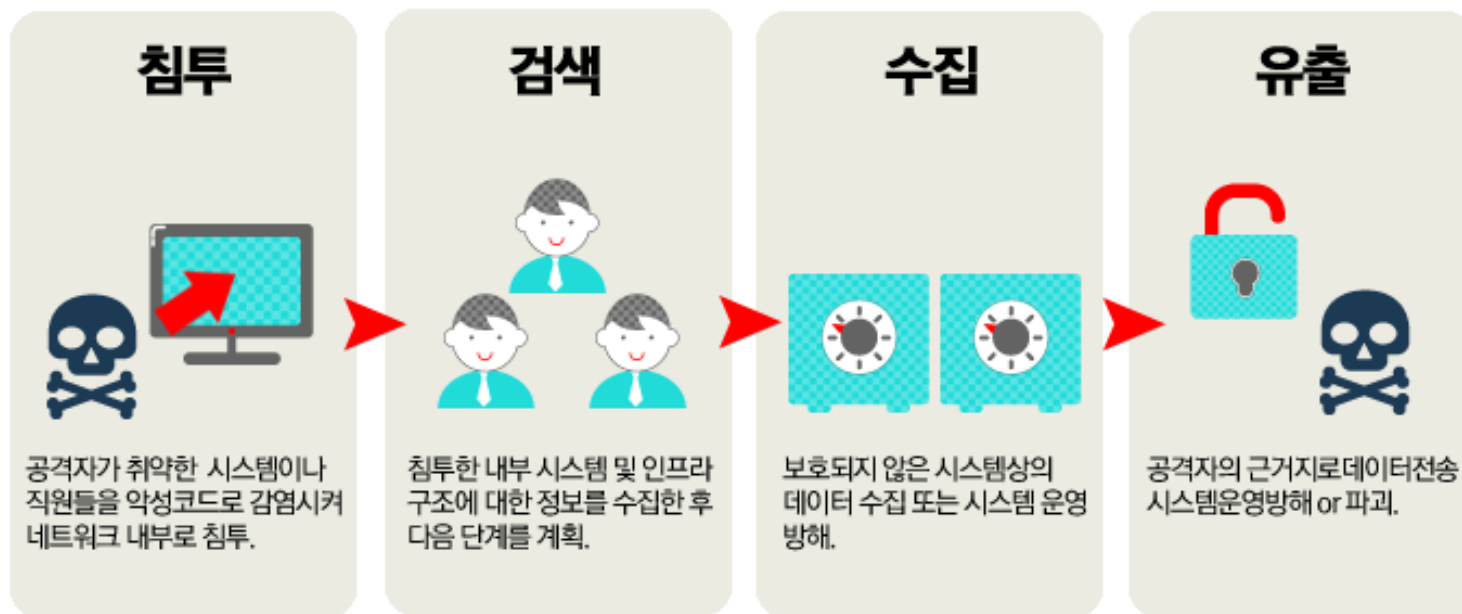
3.7 APT 공격

- **APT 공격이란?**

- 지능형 지속 위협(Advanced Persistent Threat)을 의미함
- 다양한 IT 기술과 방식들을 이용해 조직적으로 경제적인 목적을 위해 다양한 보안 위협들을 생산해 지속적으로 특정 대상에게 가하는 공격 기법

- **APT 공격 개요**

- APT 공격 과정 침투, 검색, 수집, 유출로 나눌 수 있음



APT 공격 과정 (자료: 시만텍)

• APT 공격 특징

- 특정 조직에 최적화된 공격 수행
- 충분한 시간과 비용을 투자
- 조직 및 구성원 개인에 대한 충분한 정보 수집 (사회공학적인 방법 이용)
- 탐지 회피 기법을 병행하여 공격 수행
 - low and slow 전략
 - 알려지지 않은 악성코드(Zero-Day Attack) 사용
 - 이상징후를 파악하지 못하도록 장기간에 걸쳐 은밀히 활동
- 다양한 방향으로 공격, 사용자 및 Endpoint에 집중

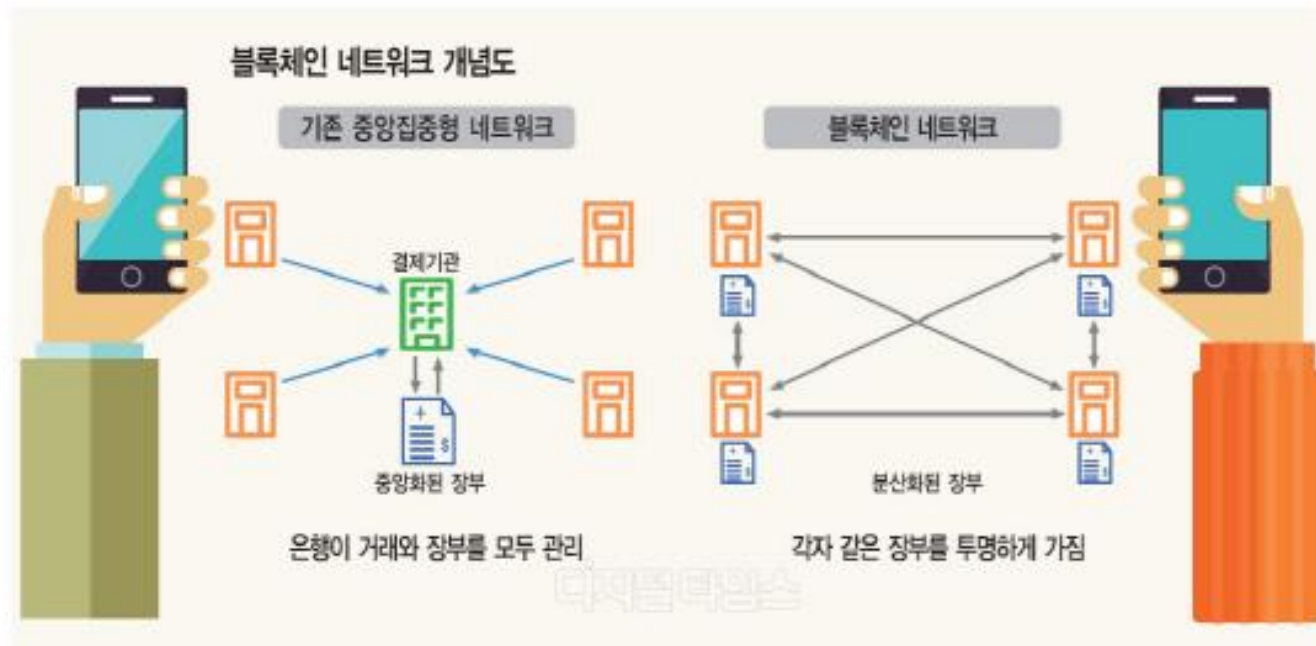
• APT 공격 대응 방안

- 공격자가 원하는 정보에 접근하기 까지 소요 시간 지연
 - 네트워크 분리 (망 분리)
 - 내부 시스템 인증 강화
- 공격자가 원하는 정보에 접근하기 이전 단계에서 탐지/제거
 - 알려지지 않은 악성코드(Zero-Day Attack) 탐지 / 제거
 - 악성코드/원격접속/명령 및 제어 지점 접근 트래픽 탐지/차단

3.8 블록체인

• 블록체인의 개념

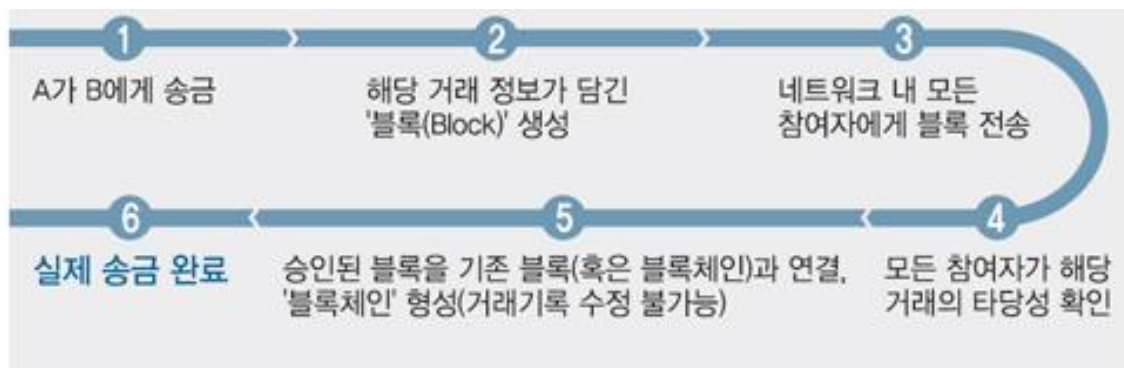
- 여러 건의 거래내역이 일정 시간마다 하나의 블록(Block)으로 묶여, 기존 생성된 블록에 체인(Chain)처럼 계속적으로 연결되는 데이터 구조를 의미
- 승인 없는 분산 데이터베이스(permissionless distributed database)로 정의
- 비트코인 혹은 다른 암호화화폐의 거래가 순차적이고 공개적으로 기록 되도록 하는 디지털 장부 기능을 함



블록체인 개념도 (자료: 디지털타임스, 신한금융투자 연구소)

• 블록체인의 특징

- 특정 시간(현재 10분)동안 발생한 모든 거래 정보가 기록된 '블록(Block)' 을 생성,
- 모든 구성원들에게 전송 후, 전송된 블록의 유효성이 확인될 경우 기존 블록체인2에 연결하는 방식으로 구현
- 블록체인은 가장 최근에 연결된 블록이 과거의 모든 거래 정보(기존의 블록들)까지 포함하고 있음 (비트코인 블록체인은 현재 약 40GByte 이상)
- 과거의 기록을 나거 블록체인에 담긴 거래 기록의 위조 가능성을 낮춤
- 특정 블록에 담긴 거래 기록을 조작하기 위해서는 그 블록 이후에 연결된 모든 블록을 단시간 내에 전부 수정해야 함
- 또한 공개키 암호화(Public Key Encryption)³ 등 암호화 기술 및 '작업증명(Proof-of-Work)'과 같은 거래 검증 메커니즘과 함께 사용가능



블록체인 송금과정 (자료: 파이낸셜타임스, KB 금융지수경영연구소)

• 블록체인의 장점과 단점

구분	특징	내용	효과/제약사항
장점	탈중앙화	P2P 기반으로 중개기관 없이 참여자 간 직접거래 가능	인프라 구축비용 및 중개수수료 절감
	보안성	다수의 참여자가 거래 정보를 공유하여 해킹이 어려움	IT 보안비용 절감
	확장성(오픈소스)	오픈소스를 이용해 구축, 연결, 확장 가능	IT 구축비용 절감
	투명성	모든 거래기록에 공개적 접근 가능	관리감독 및 규제비용 절감
	신속성	거래의 승인 및 기록이 자동적으로 실행됨	신속성 향상
단점	확장성(처리속도)	시간당 거래 처리속도가 제한적	주식시장에서와 같은 대량거래 구현이 어려움
	확장성(저장공간)	모든 거래기록을 저장해야 하므로 저장공간이 점점 증가	저장용량 문제가 나타날 소지가 있음
	비가역성	한 번 집행된 거래는 다시 되돌릴 수 없음	이전된 자산이 강제로 반환될 수 없음

자료: KB 금융지수경영연구소, 한국은행

- Stallings, 컴퓨터보안 (Computer Security(GE), 복두출판사, 2016
- 장상수, 정보보호총론 , 생능출판사, 2015
- 김경신, 정보보안과 사이버해킹의 기초, 복두출판사, 2016
- 전정훈 외 2인, 정보보호개론, 사이텍미디어, 2009
- 이경현외 2인, IT융합을 위한 정보보호개론, 홍릉과학출판사, 2010
- USB에 의한 바이러스 감염, (주)Secudrive 보안 리포트, 2015
- 2010년 Y2K10 문제 , 안철수연구소(Ahn Lab) 보안리포트, 2011
- 멀웨어(바이러스, 웜, 트로이목마), 안철수연구소(Ahn Lab) 보안리포트, 2016
- 백도어, 안철수연구소(Ahn Lab) 보안리포트, 2016
- jdbgmgr.exe virus hoax at the Wayback machine, F-Secure Hoax Information, 2009
- https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab=Top_10_Mapping_2016
- [Special Report] APT 대응 전략, 안철수연구소(Ahn Lab) 보안리포트, 2012
- 블록체인 기술과 금융의 변화, KB금융지수경영연구소 리포트, 2015

Q & A