정보보안

CH #1 Overview of Computer Security

컴퓨터 보안(Computer Security)

* 정보시스템 자원의 무결성, 가용성, 기밀성을 보전하고자 하는 목표달성을 위해 자동화된 정보시스템에 제공하는 보호
* 컴퓨터 보안, 사이버 보안 또는 정보 기술 보안은 하드웨어, 소프트웨어 또는 데이터의 도난이나 손상, 컴퓨터가 제공하는 서비스의 중단 또는 오용으로부터 컴퓨터 시스템을 보호하는 것을 의미.

CIA Triad (CIA 삼각형)

* **기밀성(Confidentiality)**
  + 데이터 기밀성 : 개인정보 또는 기밀정보가 인증되지 않은 개인에게 제공되거나 공개되지 않도록 보장
  + 프라이버시 : 개인은 자신과 관련된 정보가 다른 사람과 누구에게 공개되는지 제어할 수 있어야 함.
* **무결성(Integrity)**
  + 데이터 무결성 : 정보 및 프로그램은 지정되고 승인된 방식으로만 변경되어야 함.
  + 시스템 무결성 : 시스템은 의도적/무단 조작 없이 기능을 수행해야 함.
* **가용성(Availability) \*\* 가장 중요**
  + 시스템이 신속하게 작동하고 승인된 사용자에게 서비스가 거부되지 않도록 보장해야 한다.

추가 원칙

* **인증(Authenticity)**
  + 정말 그 사용자인지, 시스템이 받은 자료가 신뢰할 수 있는 출처에서 온 것인지 확인할 수 있는 것.
* **책임추적성(Accountability)**
  + 개체의 행동을 추적해서 찾아낼 수 있어야 한다는 것.

컴퓨터 보안이 어려운 이유?

* 보안은 단순한 문제가 아님
* 보안 기능에 대한 잠재적인 공격을 고려해야 함
* 지속적인 모니터링 필요
* 보안 실패가 발생할 때까지 보안 투자의 이점이 거의 감지되지 않음
* 높은 보안성은 종종 사용자 편의적인 운영을 방해하는 것으로 간주됨

Terminology

* 자산(Asset)
  + 보호해야 할 대상
* 보안 정책(Security Policy)
  + 시스템이나 조직이 민감하고 중요한 시스템 리소스를 보호하기 위해 보안 서비스를 제공하는 방법을 지정하거나 규제하는 일련의 규칙 및 관행
* 취약점(Vulnerability)
  + 악용될 수 있는 시스템 설계, 구현 또는 운영의 결함 또는 약점
* 위협(Threat)
  + 취약점을 악용하여 해를 입힐 수 있는 가능한 위험
* 공격(Attack)
  + 자산에 대한 위협 실행
* 대응(Countermeasure)
  + 위협, 취약점 또는 공격을 제거하거나 방지함으로써 피해를 최소화하는 기술
* 공격자(Adversary)
  + 시스템을 공격하거나 위협하는 개체

OSI Security Architecture

* 네트워크를 통해 전송되는 데이터에 대한 보안을 제공하기 위해 OSI 모델의 7개 계층 각각에서 사용할 수 있는 보안 서비스 및 보안 메커니즘을 정의

수동적 공격 (Passive Attack)

* 시스템에서 정보를 탈취하거나 사용하려고 시도하지만 시스템 리소스에는 영향을 미치지 않음.
  + 도청, 감시, 전송
  + 공격자의 *목표는 전송되는 정보를 얻는 것*

1. *메시지 내용 공개 (The release of message contents*
2. *트래픽 분석 (traffic analysis)*

능동적 공격 (Active Attack)

* 시스템 리소스를 변경하거나 시스템의 동작에 영향을 주려고 시도.
* 다양한 잠재적인 물리적, 소프트웨어 및 네트워크 취약성으로 인해 방지하기 어려움
  + Active Attacks의 4가지 유형

1. ***Masquerade****(위장) : 한 개체가 다른 개체인 것처럼 가장할 때 발생.*
2. ***Replay****(재생) : 승인되지 않은 효과를 생성하기 위한 데이터 단위의 수동 캡처 및 후속 재전송을 포함.*

*\*\* a 가 b로 보낸 메시지를 공격자가 가로챈 뒤, 메시지를 b에게 다량으로 전송한다. B는 다량의 메시지에 대한 처리를 수행하다 리소스를 모두 사용하게 된다.*

1. ***Modification of Message*** *(메시지 수정) : 메시지 조작*
2. ***Denial of Service(DoS)*** *: 통신설비의 정상적인 사용 또는 관리를 방해하는 행위*

Security Services

* Authentication(인증)
  + 통신이 믿을 수 있는지 확인 (신원 증명)
    - * X800 정의 인증 서비스
        + ***데이터 출처 인증*** *: 단일 메시지의 경우 수신자가 수신한 메시지가 출처라고 주장하는 곳에서 온 것임을 확인.*
        + ***피어 개체 인증*** *: 지속적인 상호작용의 경우 두 개체가 서로 인증되고, 제 3자가 합법적인 두 당사자 중 하나로 가정할 수 있는 방식으로 연결이 방해되지 않도록 함*
* Access Control (접근 제어)
  + 통신 링크를 통해 시스템 및 애플리케이션에 대한 접근을 제한하고 제어하는 기능
* Data Confidentiality(데이터 기밀성)
  + 데이터 전체를 암호화 하는 경우 : 출처가 불분명
  + 데이터 일부를 암호화 하는 경우 : 헤더 정보 무방비 노출
* ***따라서 적절히 암호화 해야함***
* Data Integrity(데이터 무결성)
  + 무결성 수준이 올라가면 가용성이 떨어짐
    - * 데이터 전체에 대해서 무결성을 제공해 줄 것인지, 실제로 통신과 직접적으로 관련되어 있는 메시지 내용에 대해서만 무결성을 제공해 줄 것인지는 적절히 조정해야 한다.
* Non-repudiation(부인 방지)
  + 보낸 사람이 진짜 보낸 사람인지, 받는 사람이 제대로 받는 사람인지 확인하는 것
* Availability Service(가용성 서비스)
  + 보안시스템을 적용해도 정상적인 동작을 해치지 않도록 보장하는 것

Security Techniques

* 암호 (Cryptography) : 데이터를 변형시켜서 못 보게 하는 것
* 스테가노그래피(Steganography) : 데이터를 감춰서 못 보게 하는 것