1. CC(common Criteria)의 개념
   1. 보안
      1. 위협으로부터 자산을 보호하는 것
   2. 자산소유자
      1. 자산을 보호하기를 원함
   3. 공격자
      1. 자산 소중히 하며 자산을 악용할 방법을 찾음
   4. 자산 소유자
      1. 위협 분석 → 적용 대상 결정
         1. 비용이 들 수도 있다
         2. 이를 통해 대응책을 선택할 수 있고 취약점을 찾을 수 있다
   5. 취약점 → 잔여 위협을 남김 → 소유자는 이를 줄이려 함
      1. 실행가능성과 비용과 같은 다른 제약 안에서
2. 보안 요소
   1. 기밀성
      1. 자산에 대해 인가된 사용자만 접근 사용 가능토록 하는 것
      2. 비밀성이라고도 함
   2. 무결성
      1. 송수신되는 정보가 전송도중 삭제, 추가, 변경되지 않음을 확인하는 것
   3. 가용성
      1. 인가된 사용자는 지체없이 서비스를 이용하게 하는 것
   4. 책임 추적성
      1. 보안 사고 발생 시 누구에 의해 어떤 방법으로 발생한 것인지 확인할 수 있어야함
      2. 관여하지 않은 사람에게 엉뚱한 책임을 물어 불이익 당하지 않도록 하기 위함
   5. 인증
      1. 자신의 신분, 행위 증명하는 것
   6. 보안은 전체 시스템 문제임.
      1. 전체 시스템
         1. 소프트웨어, 하드웨어
         2. 물리적 환경
         3. 인력
         4. 기업 및 법적 구조
3. 보호 대책
   1. 예방
      1. 시스템 설계를 통해 보안침해 방지
      2. 보안 기술을 방어수단으로 사용
      3. Ex) 방화벽
      4. 예방은 가장 중요한 보호조치
   2. 탐지
      1. 위반 시도 발생시 감지 하는 것
      2. 데이터도난시 소유자의 엑세스 거부를 의미하지X
      3. 로깅이나 MAC(변경 감지를 위한 파일 해시)로 탐지하는 것이 일반적.
      4. 침입 탐지 시스템
         1. 의심스러운 행동 유무를 모니터링
4. 대응
   1. 보안 위협이 발생하면 복구 계획을 수립하는 것
   2. 대응 범위를 보험, 법률 집행기관에게 통지
5. 기밀성
   1. 접근 제어 시스템을 고려할 때 데이터의 무단 읽기를 방지하는 것
   2. 정보의 무단 습득을 암시
   3. Ex) 의료 기록을 허락없이 입수, 경쟁사의 사업 비밀을 훔침
6. 무결성
   1. 데이터가 악의적으로 바뀌지 않는 것
   2. 컴퓨터 보안에서는 권한 없는 사람에 의해 데이터가 악의적으로 변경되는 것을 막는 것에 초점
   3. Ex) 온라인 지불 시스템에서 전자 수표의 액수가 변경 되는 것
7. 가용성
   1. 소프트웨어의 우발적 OR 악의적 공격뿐만 아니라 다양한 종류의 외부 환경 요소를 포함
   2. 컴퓨터 보안은 전자에 초점
   3. 가용성 보장 -> DDOS 공격 방지를 의미한다
   4. Ex) DDOS, IP라우팅 방해
8. 책임 추적성
   1. 방지 방법 및 엑세스 제어 실패시 보안에 영향을 미치는 작업을 책임자에게 추적할 수 있도록 하는 것
   2. 시스템 해킹 발생 -> 로그 변조 가능성大 -> 시스템로그를 통해 추적 까다로움
      1. 해결방안
         1. 로그파일을 별도의 서버, 물리적으로 격리된 장소에 저장
9. 인증
   1. 사람 또는 신원 확인하는 것
   2. 엑세스 제어 시스템 -> 일부만 엑세스 허용
   3. 인증 방법
      1. 암호
      2. 비밀키
      3. 서명
      4. 생체인식
      5. 엔트리 카드
      6. 위 요소들은 서로서로 결합될 수 있다
10. 보안의 실패이유
    1. 시스템 보안의 경우
       1. 시스템의 복잡성 -> 불가피한 결함
       2. 광범위, 예측 불허한 인간의 요인
       3. 정교하고 전문적인 공격자
    2. 엔지니어링 관리 측면
       1. 처음부터 poor한 보안 설계
       2. 보안에 대한 투자 小
       3. 표준적인 물건(것)이 애초에 안전하지 x
       4. 환경의 변화
       5. 올바르지 않는 기능의 상호작용
11. 복잡성
    1. 보안의 최악의 적 중 하나
    2. 모든 컴퓨터 시스템 -> 버그, 설계오류 존재함
    3. 버그 중 일부 -> 보안 관련 -> 우발적 위반, 쉬운 악용으로 이어짐
    4. 복잡성이 커질수록 보안버그는 많아짐
    5. 문제 해결 방안
       1. 복잡성 제한
          1. 입증된 설계, 개방형 프로토콜 사용
12. 공격자
    1. 놀이, 홍보, 절도, 사기, 테러 등의 이유로 해킹
    2. 전문성, 자원, 노력을 통한 구분함
       1. Script kiddies
       2. Hobbyist hackers
       3. Determined hackers
       4. Professional consultants
       5. Security services expert
    3. 위험 평가 시 공격자의 수준을 고려하여 보호할 금액을 고려함
13. 인적요인
    1. 매우 광범위함
    2. 엉성한 절차
       1. Ex)쉬운 암호 사용, 보안 검사, 경고 무시
    3. 사회 공학적 공격
       1. Ex)실수로 정보제공
    4. 자신의 행동이 보안적으로 어떤 의미가 있는지 이해하지x
       1. ex)보안이 확보되지 않은 첨부파일 오픈
    5. 보안보다 기능을 택함
    6. 예외적인 상황에 부적절하게 행동함
       1. 보안이 뚫렸다는 상황을 숨김
14. 보안 분야의 엔지니어링 과제
    1. 소프트 엔지니어링
       1. 시스템은 명확하게 지정된 방식으로 작동해야한다
    2. 보안 엔지니어링
       1. 소프트엔지니어링 보다 어려움
       2. 불특정한 다수의 방법으로부터 시스템 오류를 방지해야함
    3. 서비스 배포 전, 알 수 없는 상황에서 시스템 보안과 같은 새로운 속성을 평가할 테스트를 설계하는 것은 매우 어려움
    4. 새로운 속성 -> 매우 취약함 -> 환경변화가 실패의 일반적 원인
    5. 요즘 트렌드 -> 다른 기능과 함께 보안평가를 병행함
15. 보안 분야에 투자
    1. 보안 -> 투자의 우선 순위가 낮을 수도 있음.
       1. 프로젝트는 제한된 예산을 가짐
       2. 클라이언트는 추가적인 보안보다 기능을 선호함
       3. 보안을 이해하거나 제공하는 데 고도의 전문 지식이 필요함
       4. 보안 위험은 작은 것으로 판단됨.
    2. 회사들이 이윤을 위한 행동들이 보안에 영향을 끼침
       1. First-mover advantage (제품을 남들보다 빨리 선보여 이윤을 남기는 것)
          1. 보안이 안정되기 전에 서비스를 출시함\
16. Session Hijacking
    1. 인증된 세션을 실제로 넘겨받는 것과 관련된 복잡한 공격
17. DNS Poisoning
    1. DNS서버의 값을 변조해 클라이언트의 트래픽을 악의적인 웹사이트로 연결하는 작업이 포함
18. 기본 보안 용어
    1. DEVICE
       1. 방화벽
          1. 가장 기본적인 보안 장치
          2. 내부와 외부 네트워크 사이의 벽
          3. 네트워크 트래픽 필터링
       2. Proxy server
          1. 인터넷 호스트의 IP주소를 위장하는 것
       3. Intrusion Detection System
          1. 트래픽 모니터링, 공격 시도 탐지
    2. ACITVITY(보안 위반, 보안 위반 방지와 관련)
       1. Phreaking
       2. Authentication
          1. 가장 기본적인 보안활동
          2. 사용자가 네트워크에 엑세스 가능 여부를 확인하는 과정
    3. Auditing
       1. 로그 등을 검토해 표준을 충족하는지 확인하는 과정

`