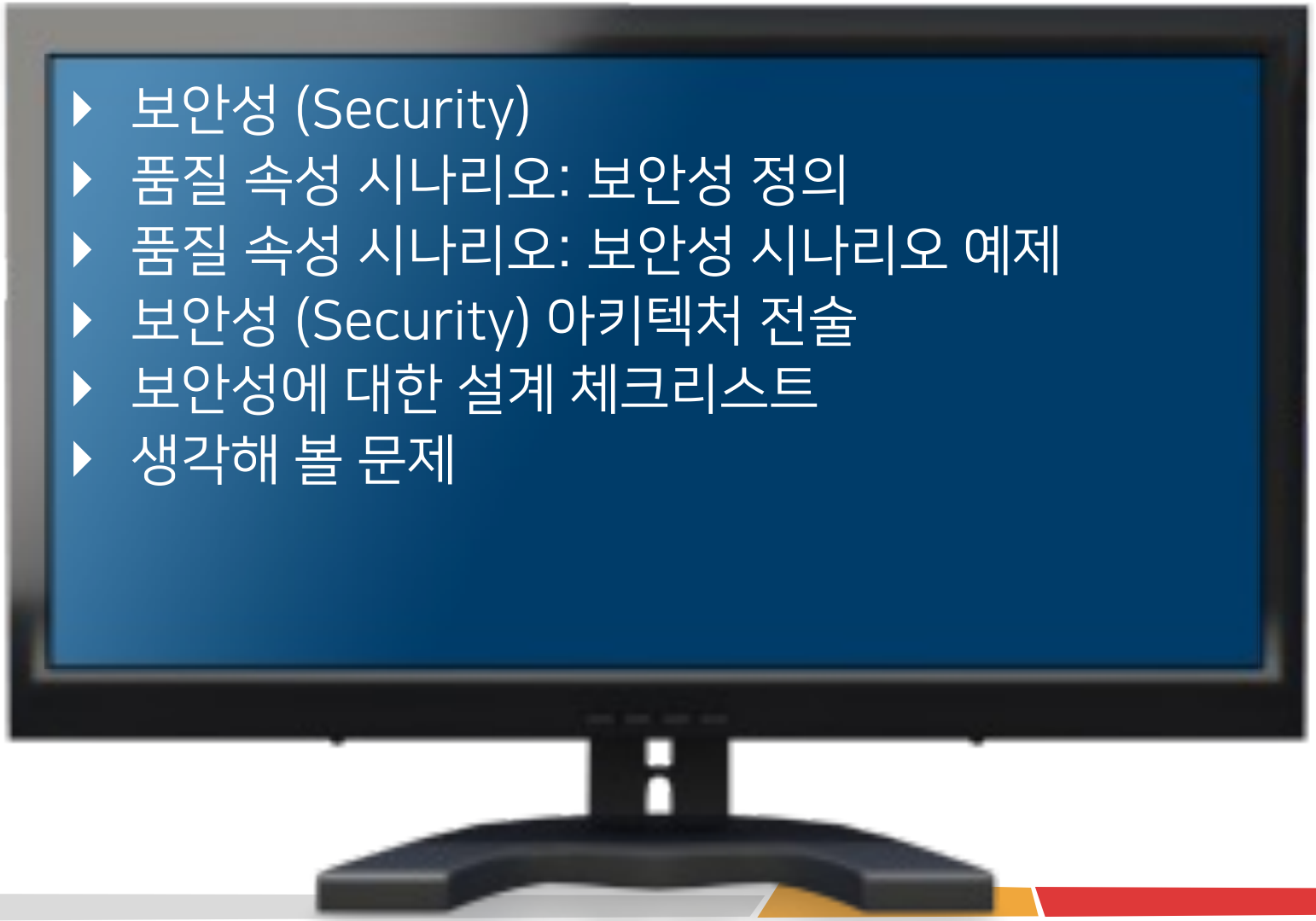
Spring 2023

Security Tactics

Seonah Lee

Gyeongsang National University

보안성 (Security) 아키텍처 전술



Security

- 보안성 **(Security)**
  - 승인 받지 않은 접근으로 부터 데이터와 정보를 보호하는 능력
  - 승인 받은 사람과 시스템으로 부터의 접근을 허용하는 능력
- 공격 **(Attack)**
  - 위해를 가하고자 하는 의도로 컴퓨터 시스템에 취해지는 조치
    - 승인 받지 않은 채 데이터와 서비스에 접근하는 행위
    - 데이터를 수정하는 행위
    - 적법한 사용자가 서비스를 사용하지 못하도록 하는 행위

Security

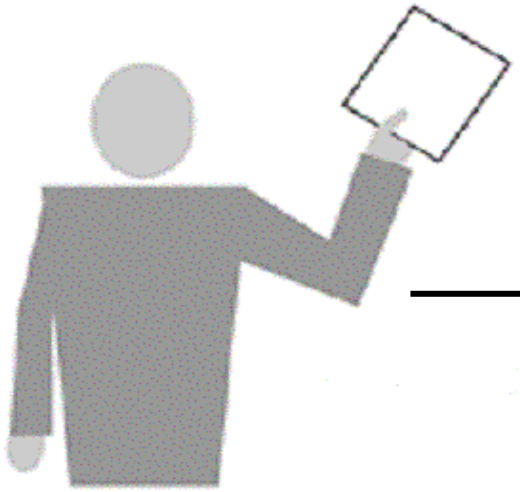
- 보안성 (**Security**)의 특징
  - 기밀성(**Confidentiality**): 인가 받지 않은 접근에서 데이터와 서비스를 보호
    - 예: 해커는 정부의 컴퓨터에 저장된 당신의 세금 정보에 접근할 수 없다
  - 무결성(**Integrity**): 인가 받지 않은 접근에서 데이터와 서비스가 조작되지 않음
    - 예: 학교에서 교사가 학점을 부여한 후 임의로 변경하지 않는다
  - 가용성(**Availability**): 합법적인 사용에 가용함
    - 예: 서비스 거부 공격이 온라인 서점에서 책을 주문하는 것을 방해하지 않는다

Security

- 보안성 **(Security)**의 추가적인 특징
  - 인증**(Authentication):** 트랙잭션의 상대가 실제로 그 상대인지를 인증
    - 예: 만약 은행에서 왔다는 이메일을 받을 경우 인증이 실제 은행에서 왔는지 보증
  - 부인봉쇄**(Nonrepudiation):** 메시지의 송신자가 메시지 송신을 부인하거나 수신자가 메시지 수신을 부인하지 못하도록 개런티 함
    - 예: 인터넷 주문에서 주문자이 주문한 사실을 부인할 수 없거나 판매자가 주문을 받았다는 사실을 부인할 수 없음
  - 인가**(Authorization):** 사용자가 작업을 수행할 수 있도록 권한을 부여함
    - 예: 온라인 은행 시스템이 합법적인 사용자가 본인 계정에 접근 가능하도록 함

Quality Attribute Scenario for Security

- 보안성: 권한 없는 접근으로부터 데이터를 보호하지만, 권한을 갖는 사람과 시스템은 접근할 수 있게 하는 시스템의 능력



자극의 근원:
공격을 하는 사람 혹은 시스템

자극:
공격

대상(Artifact):
시스템

환경:
시스템 상태

응답:
공격으로부터의 회복

응답 측정:
공격으로 손상되는 정도

Quality Attribute Scenario for Security

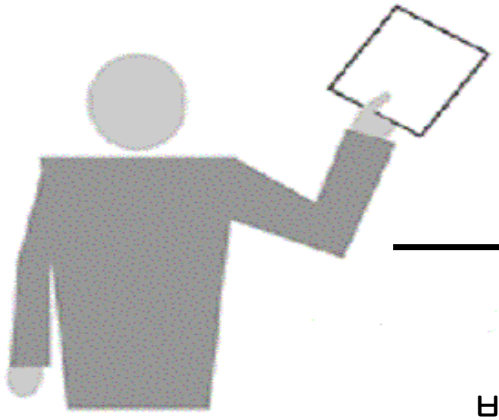
Component	Description
자극의 근원 (Source)	공격을 하는 주체로서 사람이나 시스템 • 올바른 사용자, 부적당한 사용자, 알려지지 않은 사용자 • 내부/외부 사용자
자극 (Stimulus)	시스템에 대한 공격이나 보안을 깨려는 시도로서 인증되지 않은 사람이나 시스템의 다음과 같은 행위: • 정보를 디스플레이 하려 함 • 정보를 변경하거나 삭제하려 함 • 시스템 서비스에 접근하려함 • 서비스의 사용성을 감소시키려 함
환경 (Environment)	공격받는 시스템의 상태 • 온라인/오프라인 • 네트워크에 연결/연결되지 않음 • 방화벽 내에 존재함/공개
대상 (Artifact)	공격의 대상 • 시스템 서비스 • 시스템 내부의 데이터 • 시스템에서 생산하거나 소비하는 데이터 • 공격에 취약한 특정 시스템의 컴포넌트

Quality Attribute Scenario for Security

Component	Description
응답 (Response)	**트랜잭션 실행** • 승인되지 않은 접근으로부터 데이터와 서비스 보호 • 권한이 없이 데이터와 서비스가 조작이 되지 않도록 함 • 트랜잭션에 참여하는 상대의 식별 • 트랜잭션에 참여하는 상대가 부인을 못함 • 합리적인 사용에 사용할 수 있는 데이터, 자원, 그리고 시스템 **시스템 추적 활동** • 시스템을 접근하거나 수정하는 기록 • 데이터, 자원, 서비스에 접근하려는 시도 • 공격이 발생했을 때 적절한 개체(사람 혹은 시스템)에 통지
응답 측정 (Response Measure)	• 컴포넌트나 데이터 손상 시 손상되는 시스템의 정도 • 공격 발견 전에 소요한 시간 • 견딜 수 있는 공격 수 • 공격이 성공하게 되면 복구하기까지의 시간 • 특정 공격에 손상이 쉬운 데이터의 양

Quality Attribute Scenario Example for Security

- 보안성 (Security)의 시나리오 예
  - 불만을 품은 직원이 임금률을 외부 지역에서 변경하려고 시도한다. 시스템은 감사 추적을 시작하여 하루 이내에 현재의 데이터를 복구하고 부당 변경자를 식별한다.



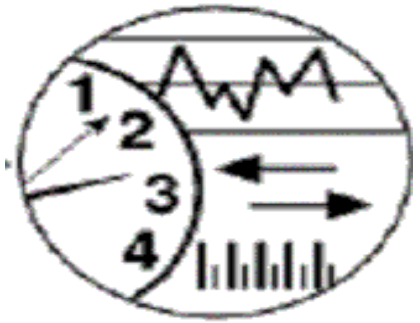
자극의 근원 :
불만을 품은
직원

자극:
임금률
변경 시도

대상(Artifact) :
시스템의
데이터

환경 :
정상 운영

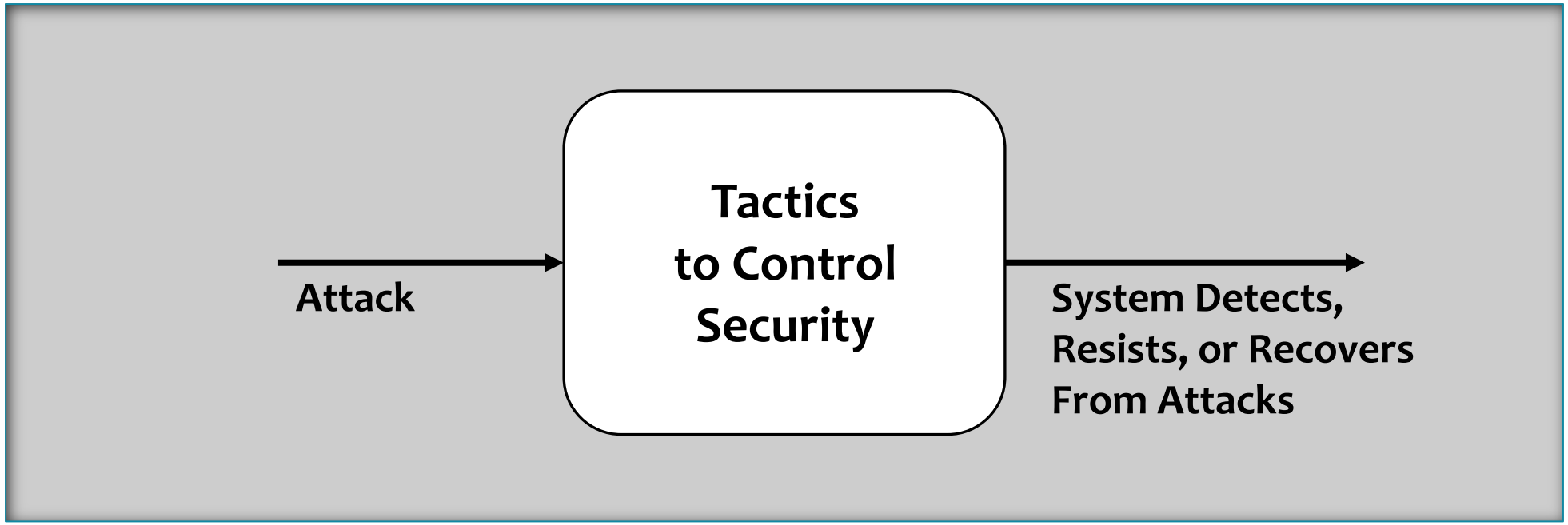
응답 :
감사 기록 유지



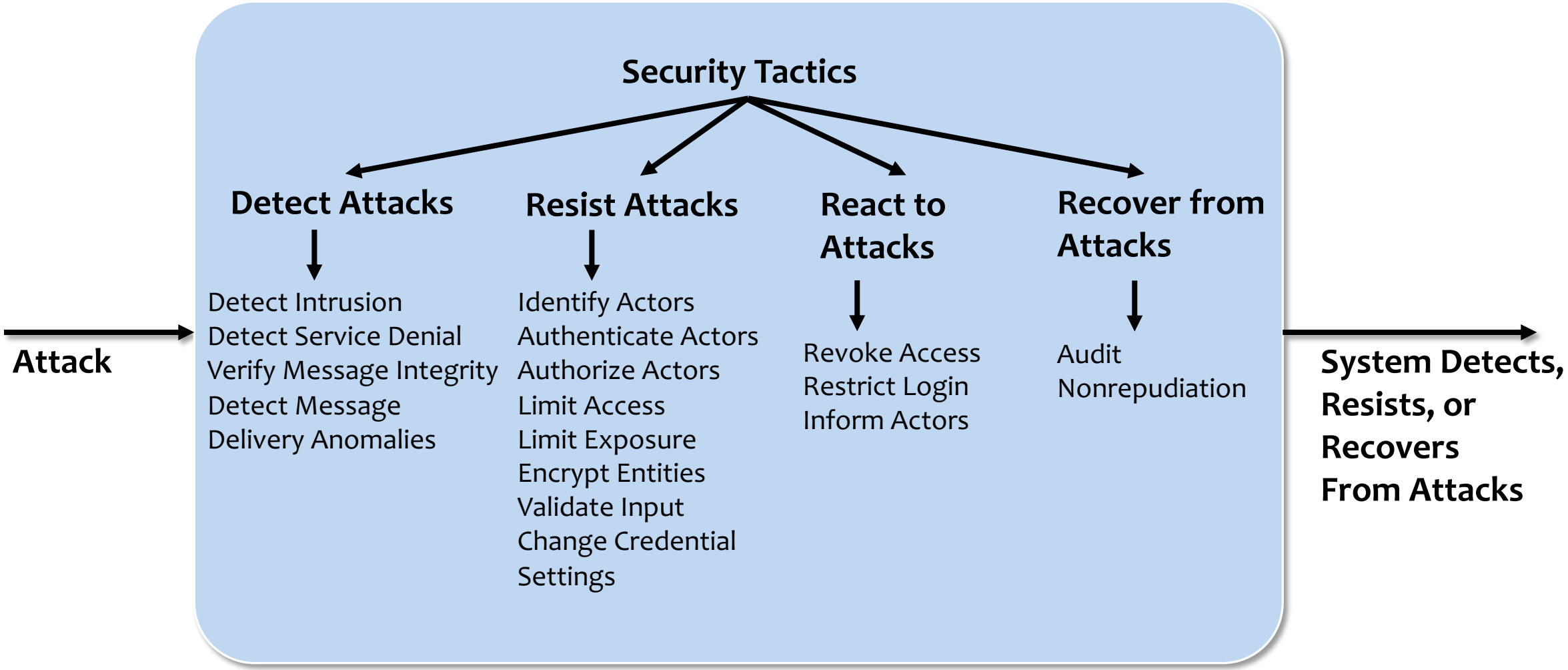
응답 측정 :
하루 이내 올바른
데이터 복구
부당 변경자 식별

Security Tactics

- 공격이 발생했을 때, 막아내거나, 공격을 탐지하거나, 공격에서 회복하는 능력에 대한 고려이다.



Security Tactics



Security Tactics

- 공격 감지 (**Detect Attacks**)
  - **침입 감지 (Detect intrusion)**
    - 요청된 네트워크 트래픽/서비스를 시그너처 혹은 데이터베이스에 등록된 악의적인 행위 패턴과 비교
      - 프로토콜, **TCP** 플래그, **Payload** 크기, 애플리케이션, **Source/Destination** 주소, 포트 번호 등
  - **서비스 부인/거부 감지 (Detect service denial)**
    - 네트워크 트래픽의 패턴 혹은 시그너처를 알려진 서비스 부인/거부 공격 프로파일과 비교

Security Tactics

- 공격 감지 (**Detect Attacks**)
  - **메시지 무결성 검증 (Verify message integrity)**
    - 메시지, 리소스 파일, 배포 파일, 환경 파일 등의 무결성을 검증
      - 체크섬이나 해시값 등을 활용
  - **메시지 지연 감지 (Detect message delivery anomalies)**
    - 메시지를 중간에 가로채는지 혹은 중간에 변경하는지를 발견하고자 함.
      - 메시지를 전달받는 시간을 검토하여 의심스러운 시간적 행위를 탐지할 수 있음
      - 비 정상적인 연결 및 단절 횟수로 공격을 감지할 수 있음

Security Tactics

- 공격 저지 (Resist Attacks)
  - 사용자 식별 (Identify actors)
    - 시스템의 외부 입력하는 사람/시스템 식별
      - 사용자는 아이디로 식별
      - 시스템은 접근 코드, IP주소, 프로토콜, 포트 등으로 식별
  - 사용자 인증 (Authenticate actors)
    - 사용자가 실제로 그 사용자인지 확인
      - 비밀번호, 일회용 비밀번호, 디지털 인증, 생체 인증으로 인증
  - 사용자 인가 (Authorize actors)
    - 인증 받은 사용자가 데이터나 서비스에 접근하기 위한 권한을 가지고 있는지 확인
      - 이는 주로 시스템 내부의 접근 제어 메커니즘으로 구현(사용자 그룹, 혹은 역할)

Security Tactics

- 공격 저지 (**Resist Attacks**)
  - **접근 제한 (Limit access)**
    - 컴퓨팅 리소스로의 접근을 제한하는 것
      - 메모리, 네트워크 연결, 접근 포인트로의 접근을 제한
      - 메모리 보호, 호스트 블록킹, 포트 닫음, 프로토콜 거부 등을 수행
  - **노출 제한 (Limit exposure)**
    - 적대적인 행위(**Action**)에 대한 피해를 최소화함, 수동적인 방어임
      - 하나의 접근 포인트로부터 접근할 수 있는 데이터 혹은 서비스의 양을 줄임
      - 하나의 공격의 피해를 완화시킴
  - **데이타 암호화 (Encrypt data)**
    - 기밀성은 데이터와 통신의 암호화를 통해 성취됨
      - 암호화는 인가로 사용가능한 데이터를 추가적으로 보호, 공개적으로 접근 가능한 통신 보호

Security Tactics

- 공격 저지 (Resist Attacks)
  - 개체 분리 (Separate entities)
    - 서로 다른 개체들을 분리하여 공격의 범위를 제약함
      - 서로 다른 네트워크에 접속하는 서버들의 물리적 분리
      - 가상머신 사용, 혹은 시스템의 서로 다른 부분 연결 안함(air gap)
      - 민감한 데이터의 분리
  - 입력 확인 (Validate input)
    - 입력을 필터링하거나 깨끗하도록 하는 처리를 수행
      - **SQL injection** 등 적대적 코드의 공격에서 강건하도록 함
  - 기본설정 변경 (Change credential settings)
    - 사용자가 기본 설정을 바꾸도록 함 ➔ 공격자가 공개되어 있는 설정으로 시스템에 접근하지 못함

Security Tactics

- 공격 대응 (**React to Attacks**)
  - **접근 철회 (Revoke access)**
    - 공격이 감지되면, 민감한 자원에 대한 접근을 모두 차단
      - 예: 데스크탑이 바이러스에 감염 시, 데스크탑 주인 조차 바이러스 제거까지 일정 리소스 접근 차단
  - **컴퓨터 잠금 (Restrict login)**
    - 반복되는 로그인 실패를 공격으로 간주, 컴퓨터를 일정 시간 잠금
  - **사용자 알림 (Inform actors)**
    - 관련 사용자들이 시스템이 공격을 받고 있음에 대한 정보를 받도록 하여 조치를 취하도록 함

Security Tactics

- 공격 복구 (Recover from Attacks)
  - 식별 (Audit)
    - 감사 추적을 위한 흔적을 기록함
      - 사용자와 시스템 행위, 그리고 행위 결과(**effects**)에 대해 기록
        - 기록을 참조하여 공격자를 찾아내거나 어떤 행위(**actions**)을 했는지 추적 가능
      - 공격자를 적발하거나, 향후의 더 나은 방어를 계획할 수 있음
  - 부인방지 (Nonrepudiation)
    - 신뢰할 만한 제 3자(**third parties**)에 의한 디지털 서명과 인가의 결합을 통해 성취
  - 복구 (Recover)
    - 비밀 번호, 제어 목록, 사용자 프로파일 등의 중복 관리,
    - 데이터에 적용된 일련의 트랜잭션의 복사본 관리

Questions

Q1. 미국에서 페이스북**(Facebook)**은 해당 주에 모든 인터넷 트래픽의 **5** 퍼센트 이상에 대한 책임이 있다.

- 페이스북닷컴에 서비스 거부 공격이 들어올 경우 어떻게 인식할 수 있는가**?**

Q2. 보안과 사용성은 보통 서로 충돌하는 것처럼 보인다.

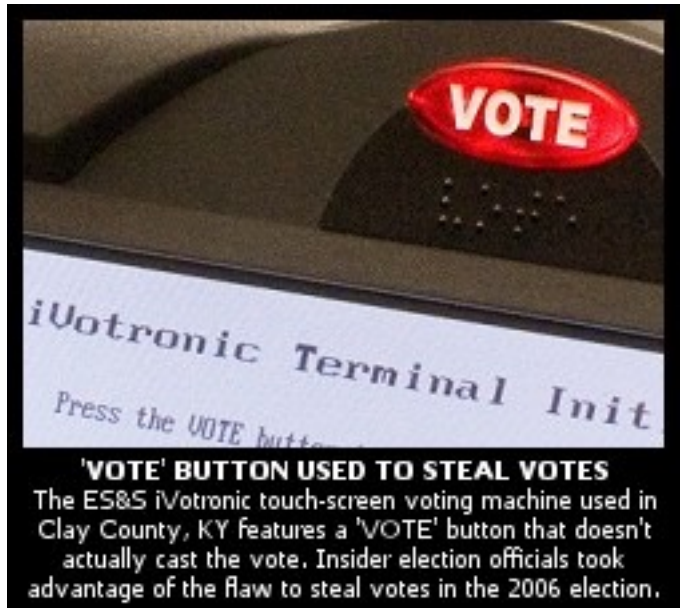
- 일반적으로 보안을 일반적인 사용자에게 필요 없는 오버헤드처럼 보이는 절차와 프로세스를 부과한다.
- 그러나 누군가 보안과 사용성은 서로 관련되어야 한다고 하며, 시스템을 안전하게 사용하기 쉽도록 만드는 것이 사용자에게 보안을 촉진시키는 가장 좋은 방법이라고 주장하였다.
- 이 주장에 대해서 논의하자.

Electronic Voting System

- 미국 켄터키 주에서 2010년 전자 투표 기계 조작에 대한 사건

Electronic Voting System

- 설계 결함으로 인해 허용된 낮은 기술의 "해킹”
  - 큰 빨간색 " 기계 상단에 있는 **VOTE"** 버튼(오른쪽 사진 참조), 버튼을 눌러도 실제로 투표 과정이 완료되지는 않음
  - 유권자들은 이론적으로 투표가 내부적으로 캐스트로 기록되기 전에 "투표 확인"을 위해 터치 스크린에서 또 다른 선택을 눌러야 함
  - 유권자들에게 빨간색 **"VOTE"** 버튼을 누른 후에 투표가 이루어졌다고 알림
  - 투표 심사위원은 기계로 가서 투표를 변경

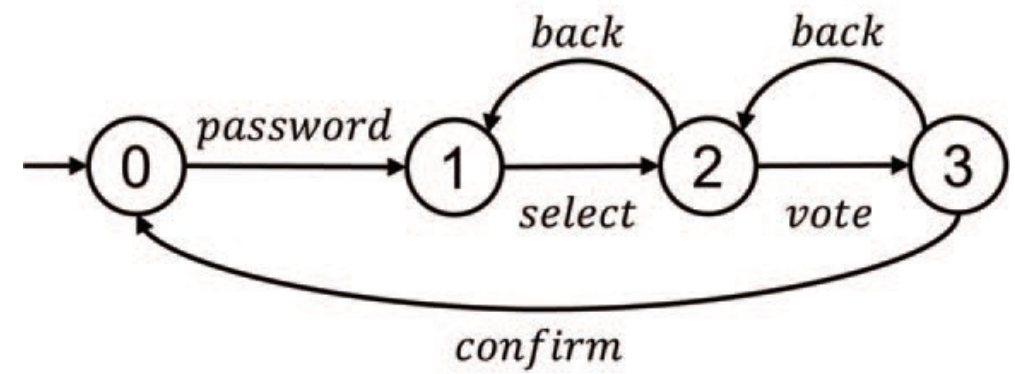


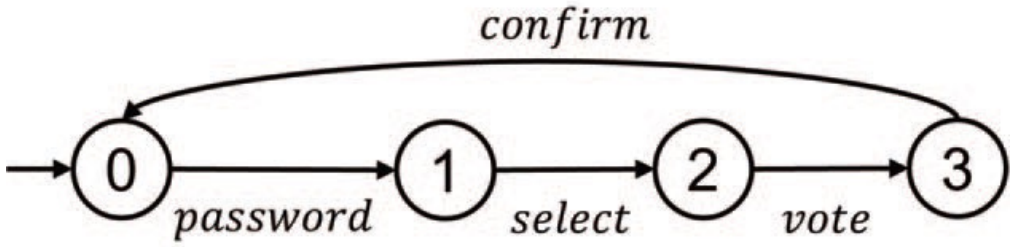
'VOTE' BUTTON USED TO STEAL VOTES
The ES&S iVotronic touch-screen voting machine used in Clay County, KY features a 'VOTE' button that doesn't actually cast the vote. Insider election officials took advantage of the flaw to steal votes in the 2006 election.

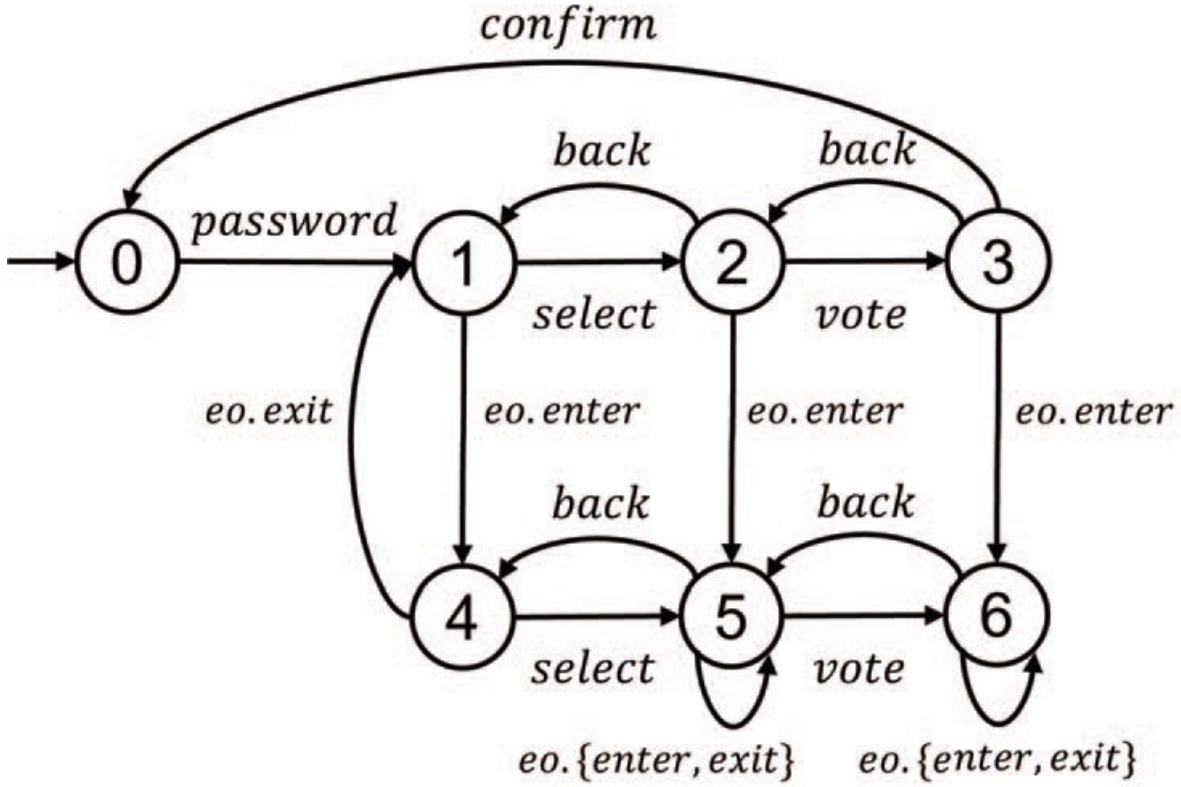
https://www.bradblog.com/?p=8514

Electronic Voting System

- Voting Machine







Zhang, Changjian, Taranj Saluja, Rômulo Meira-Góes, Matthew Bolton, David Garlan, and Eunsuk Kang. "Robustification of Behavioral Designs against Environmental Deviations." (2023).

Question?

Seonah Lee
saleese@gmail.com