Network Security Essential

- 9장 Intruder -

명 세인(sein@pel.smuc.ac.kr)

상명대학교 프로토콜공학연구실

목 차

- 침입자
- 침입탐지
- 패스워드 관리

침입자

- 침입자(Intruder)
  - 네트워크에 연결된 시스템이 원치 않는 접근을 하는 사용자 또는 프로그램
    - 사용자: 권한 외의 행동을 발생
    - 프로그램: 바이러스, 웜, 트로이 목마 등
  - 침입 유형 예
    - 신분위장자(Masquerader)
    - 불법행위자(Misfeasor)
    - 은밀한 사용자(Clandestine User)

침입자

- 침입자 행동패턴
  - 해커
    - 침입 성공이 목적, 시스템에 문제되는 행동을 하지 않을수 있음
    - 시스템 입장에서는 단순 침입자
    - **침입예방기법, 침입탐지시스템의 설계 원인**
    - 침입 감지 후 처리를 위해, 컴퓨터 비상 대응팀(CERT: Computer Emergency Response Team)의 구성이 필요

침입자

- 침입자 행동패턴
  - 범죄형 기업
    - 악의적인 특정 목적을 갖고 시스템으로 침입하는경우
    - 침입에 대한 예방, 방어가 부실할경우 시스템에 심각한 문제를 발생
    - 패킷 스니핑, 취약점 공격, 트로이목마 등을 응용
    - **침입 예방/방지 시스템을 우회, 추적하기 어려움, 흔적 최소화**
  - 내부 위협
    - 시스템 내부 사용자의 실수 또는 고의적 보안 위협/공격
    - 방어/감지가 가장 어려운 유형

침입자

- 침입 기법
  - 최초의 침입은 패스워드 탈취부터 시작
  - 패스워드 파일에 대한 보호
    - 일방향 암호화(One-way Encryption)
    - 접근 제어(Access Control)
  - 탐지(Detection)와 예방(Prevention) 보안을 구축 해야 함

목 차

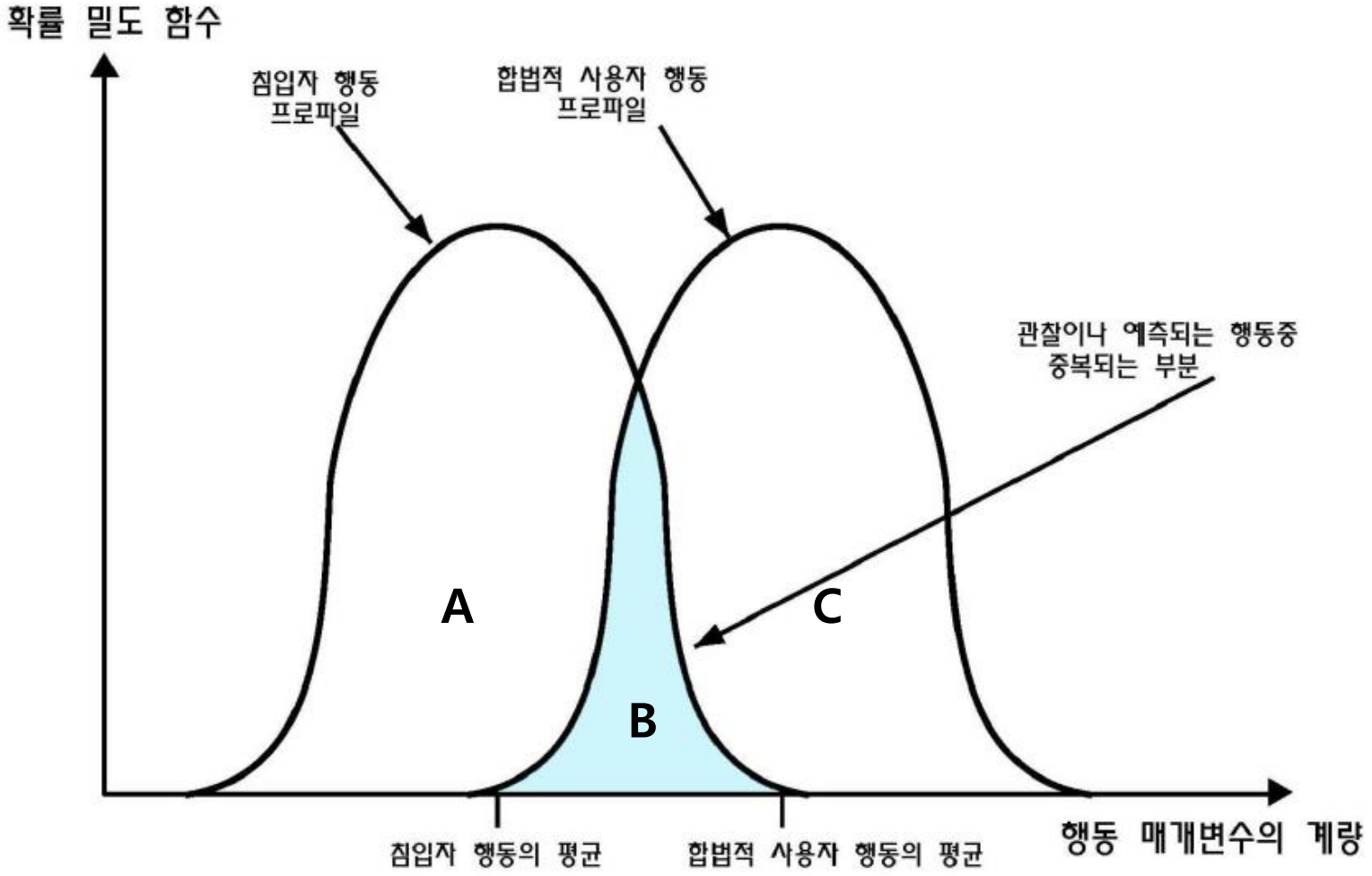
- 침입자
- 침입탐지
- 패스워드 관리

침입탐지

- 침입 탐지 시스템(IDS: Intrusion Detection System)
  - 잘구현된 침입 예방시스템은 결과적으로 무너짐
  - 침입 탐지 시스템을 구현하여 차선의 보안을 구성
  - 결과적으로 IDS와 IPS를 같이 구현하여 보안 시스템을 구축
  - 침입 탐지 활용 사항
    - 빠른 침입자 탐지
    - 효과적인 침입탐지 시스템의 부과 효과
    - 침입탐지 시스템 구현을통한 침입 예방 시스템 강화

침입탐지

- 침입 탐지 시스템(IDS: Intrusion Detection System)
  - 구현시 고려 사항



침입탐지

- 침입 탐지 시스템(IDS: Intrusion Detection System)
  - 구현시 고려 사항
    - A: 침입자를 침입자로 판별
    - C: 정당 사용자를 정당 사용자로 판별
    - B
      - False Positives: 합법적 사용자를 침입자로 판단
      - False Negative: 침입자를 합법적 사용자로 판단

침입탐지

- 침입 탐지 시스템(IDS: Intrusion Detection System)
  - 침입 탐지 기법
    - 통계적 변형 탐지(Statistical Anomaly Detection)
      : 합법적 사용자의 행동에 대한 정보를 수집한 데이터를 기반으로 다음 행동에 대한 합법 여부를 통계적 관점으로 처리
      - 임계값 탐지(Threshold Detection)
        : 사용자와 무관한 시스템 내부의 Event발생 빈도에 대한 임계값 정의
      - 프로파일 기반(Profile Based)
        : 개별 사용자(그룹)의 동작에 대한 프로파일을 구성하고 개별 행동의 변화를 감지

침입탐지

- 침입 탐지 시스템(IDS: Intrusion Detection System)
  - 침입 탐지 기법
    - 규칙-기반 탐지(Rule-Based Detection)
      : 특정 행동이 침입자의 행동인지 결정하기위한 규칙을 정의
      - 변형 탐지(Anomaly Detection)
        : 이전 사용 패턴과 달라진 행동 패턴을 탐지하는 규칙을 정의
      - 침투 식별(Penetration identification)
        : 의심적인 행동을 정의하는 전문가 시스템(Expert System)을 구현

침입탐지

- 침입 탐지 시스템(IDS: Intrusion Detection System)
  - 침입 탐지 기법
    - 실제 보안에 적용하기위해 위 두 가지 기법을 병행적용
      - 통계 기반은 신분위장자 탐지에 효과적
      - 규칙 기반은 불법사용자 탐지에 효과적
    - 광범위한 침입 행동을 탐지할 수 있도록 구현

침입탐지

- 감사 기록
  - 침입 탐지를 위한 데이터 수집
  - 기본 감사기록(Native Audit Records)
    - 운영체제에서 제공하는 사용자 행동에 대한 기록 소프트웨어
    - 특정 IDS구현에 필요한 정보가 누락되어 응용이 어려움
  - 탐지-전용 감사 기록(Detection-Specific Audit Records)
    - IDS에 필요한 정보만을 수집
    - 다양한 시스템에 응용 가능
    - 한시스템에 기본감사기록과 함께 두개의 감사 기록을 운영해야 함

침입탐지

- 감사 기록
  - 탐지-전용 감사 기록(Detection-Specific Audit Records)
    - 도로시 데닝(Dorothy Denning)
      - Smith사용자의 명령어 실행에 대한 시스템 기록

COPY GAME.EXE TO <Library>GAME.EXE

Smith	execute	<Library>COPY.EXE	0	CPU = 00002	11058721678
Smith	read	<Library>GAME.EXE	0	RECORDS = 0	11058721679
Smith	execute	<Library>COPY.EXE	write-viol	RECORDS = 0	11058721680

침입탐지

- 통계적 변형 탐지
  - 임계값 분석
    - 일반적인 공격도 탐지하지 못하는 수준
    - 임계값과 시간 간격을 결정하여 탐지 민감도를 올림
    - 합법사용자에대한 오류나 불법사용자에 대한 오류 발생 가능

침입탐지

- 통계적 변형 탐지
  - 프로파일 기반
    - 사용자(그룹)의 과거 행동을 특성화
      - 매개변수들의 집합을 정의
    - 평가지수(Metric)의 개수를 지정하여 특정 행동량의 많고 적음을 구별
    - 평가지수의 예
      - 카운터(Counter): 특정 시간 간격에 대해 세션동안 명령 횟수, 로그인 횟수, 패스워드 실패 횟수등을측정
      - 게이지(Gauge): 특정 개체의 현재 값을 측정(로그인 수, 대기하는 메시지의 수)
      - 간격타이머(Interval timer): 두 개의 연관된 사건의 시간 간격(다음 로그인 간격)
      - 자원활용(Resource Utilization): 지정 시간동안 소모된 자원의 양

침입탐지

- 통계적 변형 탐지
  - 평가지수 프로파일의 해석
    - 현재의 작동이 허용 범위안에 있는지 결정하기 위한 검사
    - 평균과 표준편차(Mean and Standard Deviation)
      : 측정된 과거 정보를 특정 시간 간격동안의 매개변수의 평균과 표준편차를 측정, 평균적인 행동과 상태를 규정하여 변화를 감지
    - 다변수(Multivariate)
      : 두 개 혹은 그 이상의 변수 사이의 상관관계를 통해 침입자를 가려냄
      (예: 프로세스 시간-자원활용, 로그인 빈도-세션 경과시간)

침입탐지

- 통계적 변형 탐지
  - 평가지수 프로파일의 해석
    - 마르코프 과정(Markov Process)
      : 마르코프과정 모델을 사용하여 다양한 상태(State)사이의 전이확률(Transition Probability)를 구성
    - 타임 시리즈(Time Series)
      : 시간 간격에 초점을 두어 너무 빠르거나 느리게 발생하는 연속적인 사건을 감지, 통계적 검사를 사용하여 비정상적 타이밍의 특성을 감지
    - 운용 결과(Operational)
      : 감사기록 분석보다는 잘못된 행동을 정의, 일반적인 관찰의 한계값을 정의하고 이 이상의 행동을 침입으로 의심

침입탐지

- 규칙-기반 침입 탐지
  - 시스템 안의 사건을 관찰하여 특정 동작 패턴이 의심스러운지 결정
    - 규칙-기반 변형 탐지
      - 통계적 변형 탐지와 유사, 미래의 행동이 과거 행동과 유사할 것임을 전제
      - 과거 감사 기록을 이용해 사용자 패턴을식별
      - 새로운 행동에 대해 과거 행동과 비교
    - 규칙-기반 침투 식별
      - 의심스런 행동을 정의하는 전문가 시스템의 응용
        - 다른사용자의 개인 디렉토리에 대한 접근(R/W)
        - 지정된 사용 시간외의 접근
        - 디스크 접근을 상위계층 운영체제 유틸리티를 사용
        - 동일시스템 중복 로그인
        - 시스템프로그램 복사

침입탐지

- 규칙-기반 침입 탐지
  - 침입 탐지 방법 정리 표

방법	모델	탐지되는 침입 유형
로그인과 세션 동작		
일별 시간별 로그인 빈도수	평균과 표준편차	침입자는 일과시간 이후에 침입을 시도하거나, 의심되는 장소에서의 침입
장소별 로그인 빈도수	평균과 표준편차	
마지막 로그인 이후 경과시간	운용적	사용 정지된 계좌 침입
세션 당 소요시간	평균과 표준편차	유의수준 편차가 있다면 위장을 의심
장소의 출력 양	평균과 표준편차	과한 트래픽이 전송되면 중요 정보 누출을 의심
세션 자원 활용	평균과 표준편차	프로세서나 I/O가 비정상 레벨이면 침입자 의심
로그인에서 패스워드 실패	운용적	패스워드 추측을 통한 침입 시도
특정 터미널에서 로그인 실패	운용적	침입 시도

침입탐지

- 규칙-기반 침입 탐지
  - 침입 탐지 방법 정리 표

방법	모델	탐지되는 침입 유형
명령과 프로그램 실행 동작		
실행 빈도수	평균과 표준편차	다른 명령을 실행하는 침입자 탐지, 권한 상승에 성공한 합법적 사용자를 탐지
프로그램 자원 활용	평균과 표준편차	I/O나 프로세서 활용에 부가 영향을 끼치는 값, 바이러스, 트로이목마의 침입을 의심
실행 거부	운용적 모델	권한 상승을 시도하는 개별 사용자의 침입을 의심
파일 접근 동작		
읽기/쓰기/생성/삭제의 빈도수	평균과 표준편차	비정상적 행동, 위장이나 관찰을 의심
읽기/쓰기 기록	평균과 표준편차	추록,축적을 통해 중요 데이터 획득 시도
읽기/쓰기/생성/삭제의 실패 횟수	운용적	권한이 없는 파일에 대한 접근 탐지

침입탐지

- 기본-비율 오류 (Base-Rate Fallacy)
  - IDS는 잘못된 경고 비율을 수용 레벨로 유지하면서 높은 비율로 탐지하여야함
    - 가짜 경고가 많은 경우 관리자가 무시하거나 가짜 분석을 위해 시간을 낭비
    - 가짜경고를 줄이기 위해 탐지율이 떨어진다면, 시스템이 공격당하는 문제 발생
    - 이러한 문제는 어려우며 현재 시스템에서 극복하기 힘듦

침입탐지

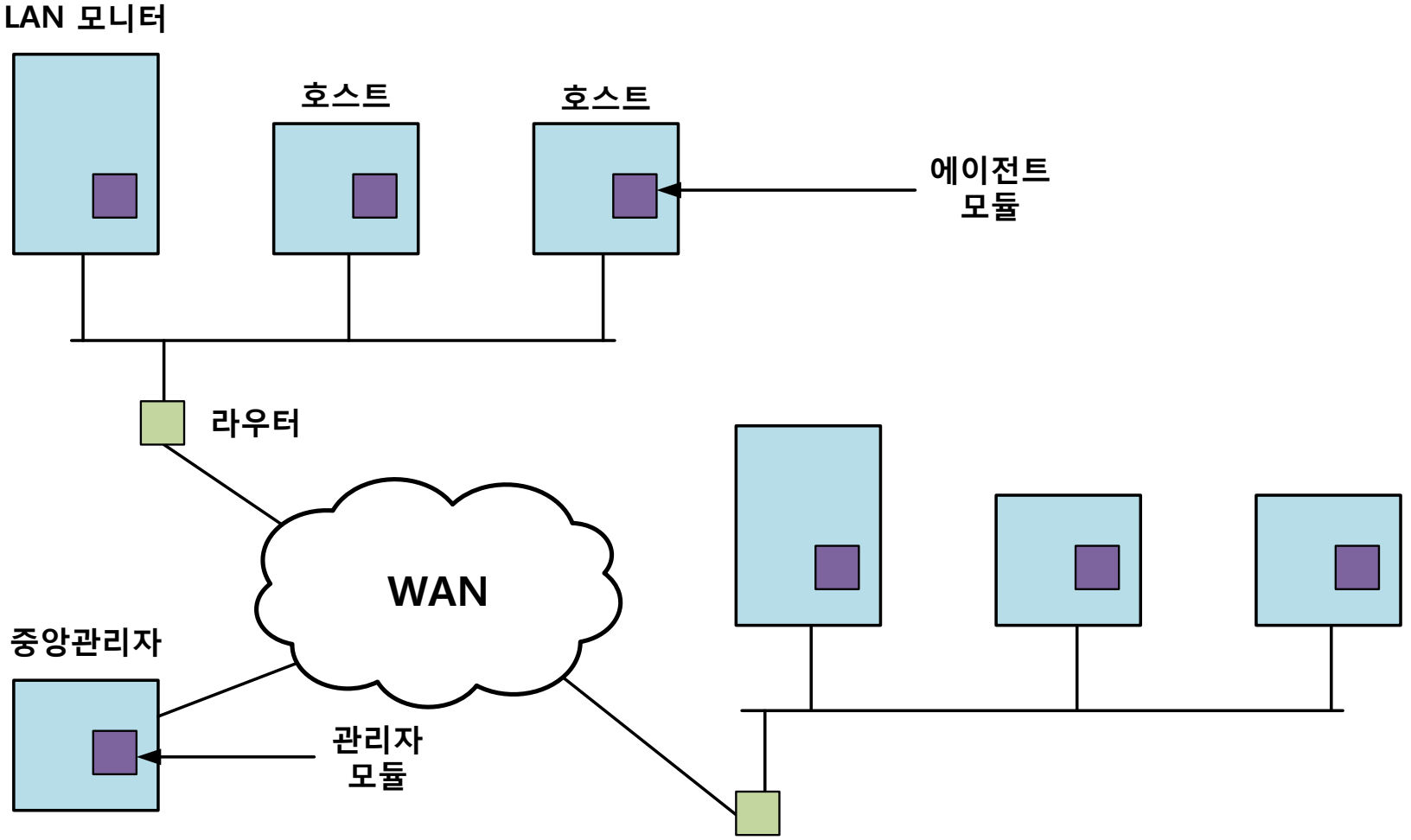
- 분산 침입 탐지
  - 단일 시스템이 아닌 인터 네트워크에 분산되어 있는 시스템간의 IDS구현
    - 서로다른 여러 시스템에서 기본 감사 수집이 이루어지면 보안 관련 감사 기록에도 새로운 포맷 적용이 필요
    - 감사 기록 공유를 위한 통신에서 기밀성, 무결성을 유지 하여야 함
    - 감사기록 분석시 중앙 집중 또는 분산된 방식으로 판단
      - 중앙집중의 경우 보고된 정보의 관계분석이 용이하지만, 병목처리 발생
      - 분산형의 경우 각 분산된 정보의 공유, 협조가 필요

침입탐지

- 분산 침입 탐지
  - Davis에 있는 캘리포니아 대학에서 개발한 분산 IDS
    - 호스트 에이전트 모듈(Host Agent Module)
      :모니터 시스템에서 백그라운드 동작의 감사 수집 모듈, 호스트에서 발생하는 보안 관련 사건의 데이터를 수집하여 중앙 관리자에게 전송
    - LAN 모니터 에이전트 모듈(LAN Monitor Agent Module)
      : 호스트 에이전트 모듈 기능에 LAN트래픽 분석 정보를 함께 전송
    - 중앙 관리자 모듈(Central Manager Module)
      : LAN모니터와 호스트 에이전트의 보고를 처리하고 연관

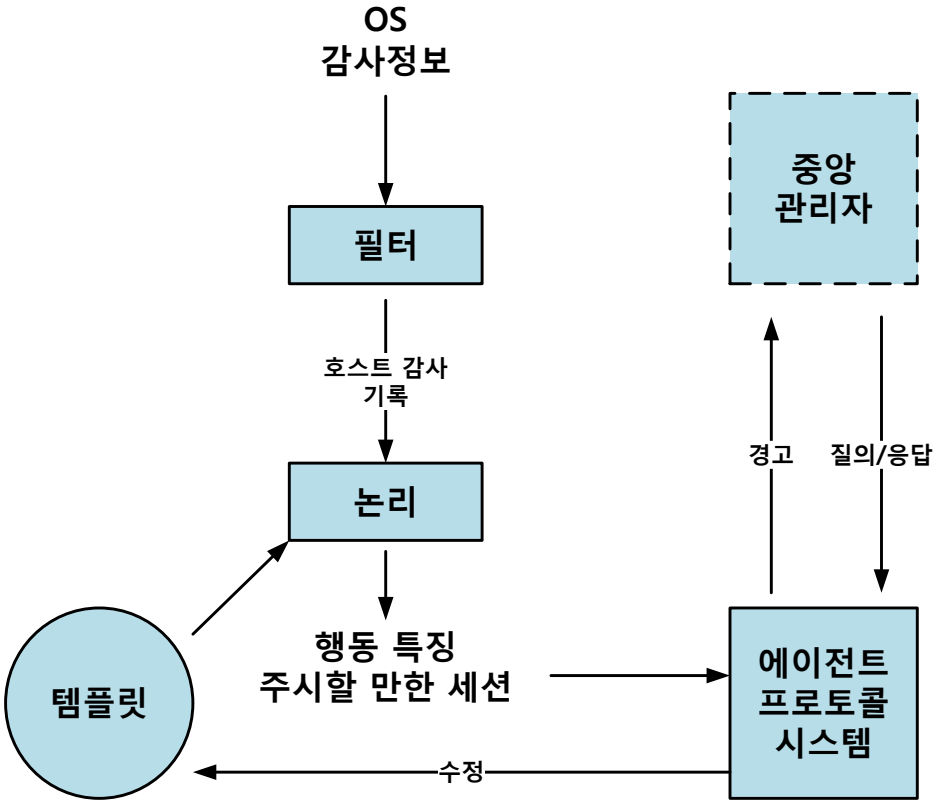
침입탐지

- 분산 침입 탐지
  - Davis에 있는 캘리포니아 대학에서 개발한 분산 IDS



침입탐지

- 분산 침입 탐지
  - Davis에 있는 캘리포니아 대학에서 개발한 분산 IDS
    - 템플릿 –구동 논리
      - 특정행동이 독립적인 의미를 갖는 경우를 분리
        : 실패한/시스템 파일 접근, 파일 접근 제어 변경 등



침입탐지

- 분산 침입 탐지
  - 허니팟(Honeypot)
    - 공격 성향을 갖는 사용자를 중요시스템에서 끌어냄을 전제
      - 중요 시스템에 접근하는 공격자를 다른 방향으로 돌림
      - 공격자의 동작에 관한 정보를 수집
      - 관리자가 반응할 수 있도록 공격자를 시스템에 머물도록 유도
    - 위조된 시스템을 보여주며 중요한 시스템으로 속임
    - 사건 기록기(Event Loggers)를 이용한 행동 감지
    - 초기는 단순 서버를 보여주도록 구현, 현재는 가상의 트래픽을 발생하도록 구현하여 중요 시스템으로 보여지도록 구현

목 차

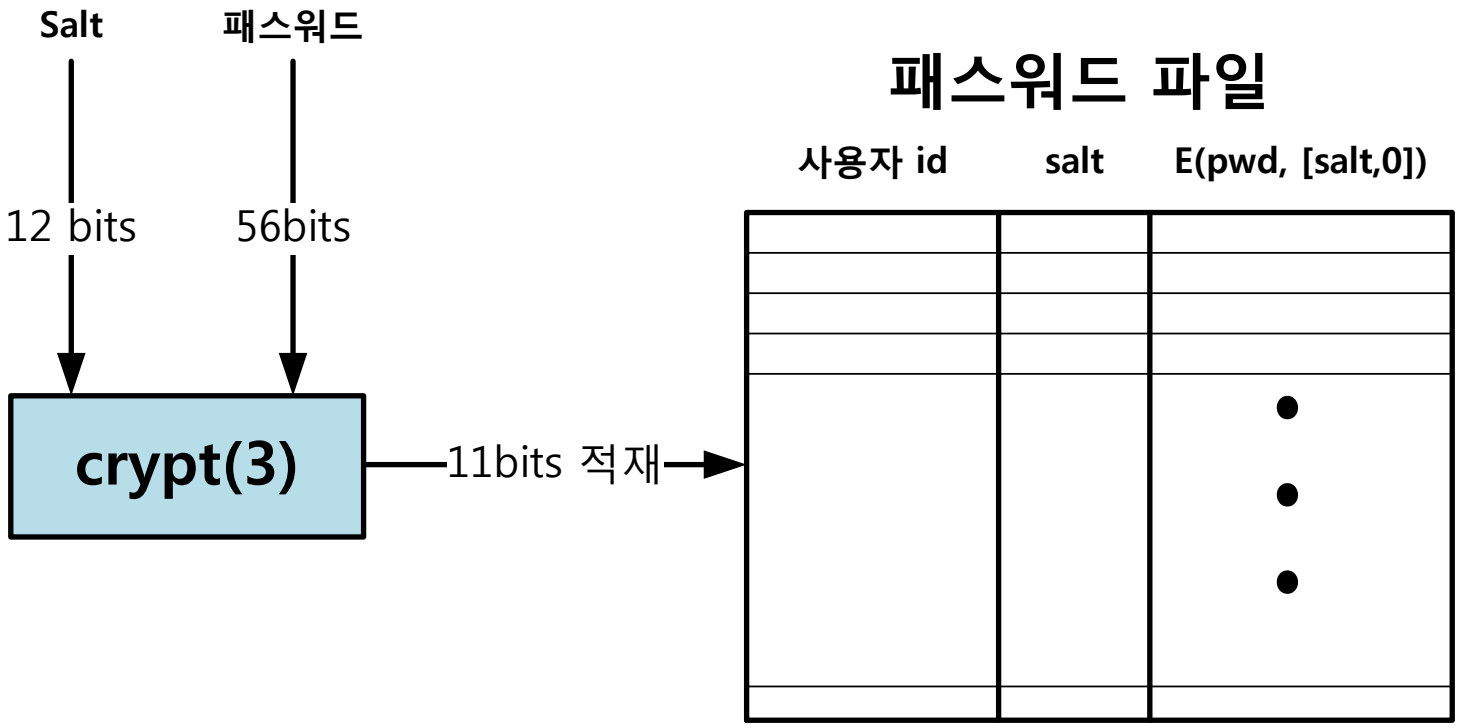
- 침입자
- 침입탐지
- 패스워드 관리

패스워드 관리

- 패스워드 보호
  - 침입자에 대한 최초의 방어는 패스워드 시스템
  - ID는 사용자의 시스템 접근 권한 확인, 특정 시스템은 ID가 신청되어 있는 사람만 접근
  - ID는사용자에게 부여된 권한을 식별하여 권한 수준을 결정
  - ID는 자유 재량의 권한을 부여, 다른 사용자의 ID를 목록화하여 사용자 개인의 파일에 대한 권한을 부여 가능

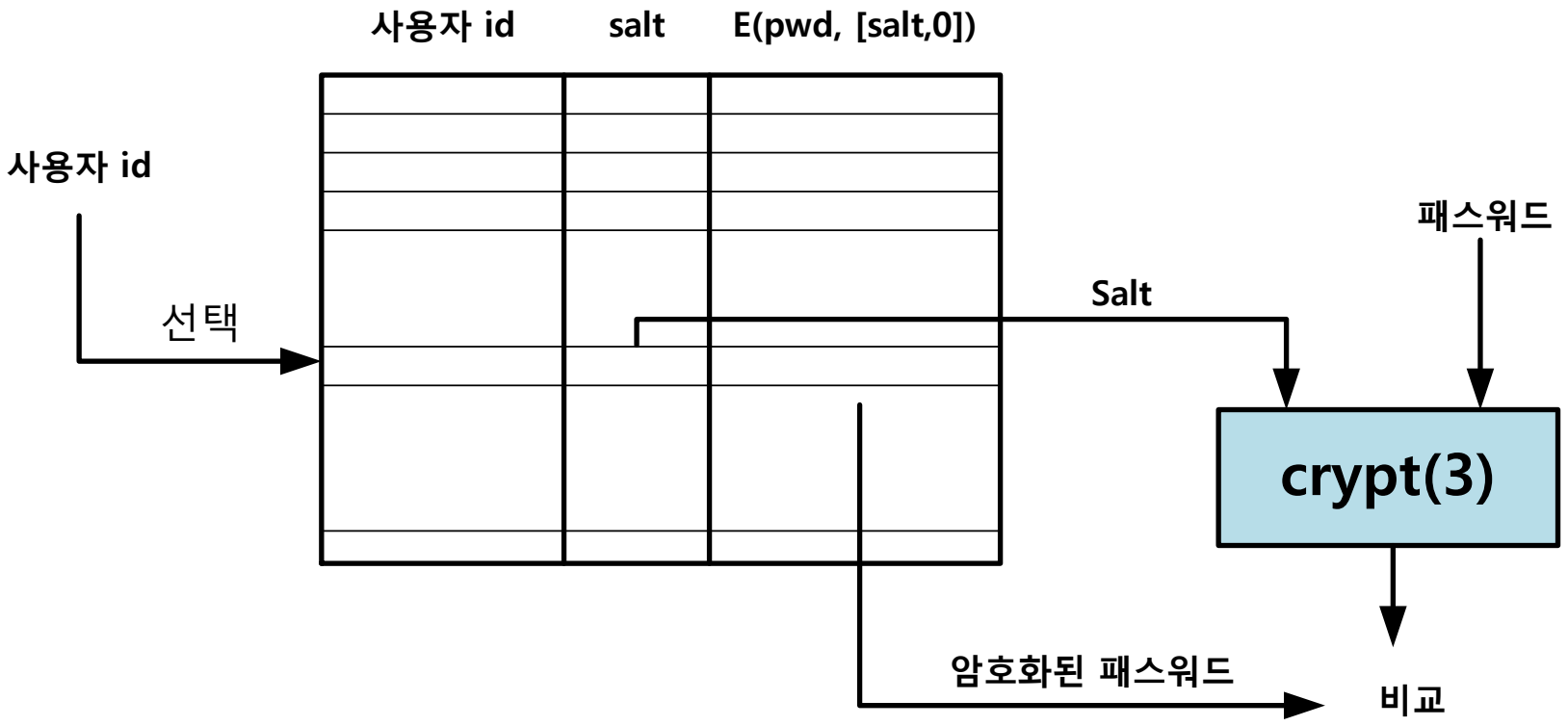
패스워드 관리

- 패스워드 보호
  - 패스워드 취약성
    - UNIX에서 사용되는 패스워드 관리 구조
      - Salt: 추가적인 입력으로 사용하는 난수



패스워드 관리

- 패스워드 보호
  - 패스워드 취약성
    - UNIX에서 사용되는 패스워드 관리 구조
      - Salt: 추가적인 입력으로 사용하는 난수



패스워드 관리

- 패스워드 보호
  - 접근 제어
    - 공격자가 패스워드 파일에 접근하는 것을 막는 것
      - 공격자는 침입에 성공하면 다음 세션을 위해 패스워드 모음 획들을 시도함
      - 단 한번만 노출되면 침입 문제가 생김
      - 사용자가 다른시스템에도 동일한 계정/패스워드패턴을 사용한다면 피해가 확산

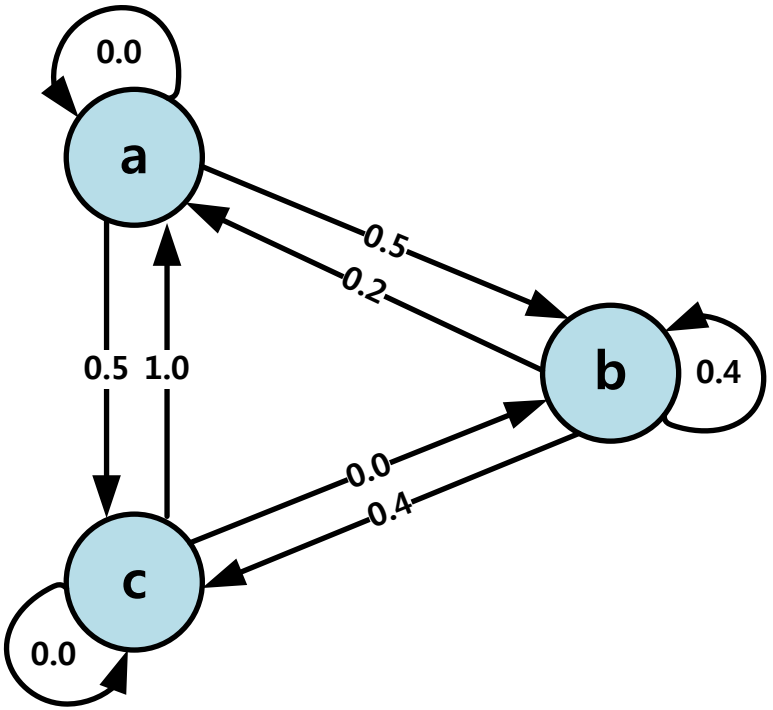
패스워드 관리

- 패스워드 선택 요령
  - 충분히 복잡하여 공격자가 예측할 수 없음
  - 충분히 명료하여 사용자가 기억하기 쉬움

  - 패스워드 생성 기법
    - 사용자 교육(User Education)
    - 컴퓨터-생성 패스워드(Computer-Generated Passwords)
    - 반응 패스워드 검사(Reactive Password Checking)
    - 주도적 패스워드 검사(Proactive Password Checking)

패스워드 관리

- 마르코프 모델
  - 패스워드 조합의 경우의 수 계산
    - A의 다음 문자로 b가 올 확률은 0.5



감사합니다!