2017/01/24, 2017 보안 기초 세미나

Network Security Essentials

- Chapter_9 침입자 -

임연주(yeonjoo@pel.smuc.ac.kr)

상명대학교 프로토콜공학연구실

목 차

침입자

- 침입자(Intruder)
  - 정의
    - 네트워크에 연결된 시스템이 허가되지 않은 접근하는 사용자 또는 프로그램
      - 사용자: 권한 외의 행동을 발생
      - 프로그램(멀웨어): 바이러스, 웜, 트로이 목마 등
  - 침입자 유형의 예
    - 신분위장자(Masquerader)
    - 불법 행위자(Misfeasor)
    - 은밀한 사용자(Clandestine user)

침입자

- 침입자 공격 유형
  - 양성 침입(Benign attack)
    - 손상을 초래하지 않는 바이러스
      - 화면상에 메시지를 띄우거나 키를 누를 때 소리가 나게 함
  - 심각한 침입(Serious attack)
    - 보안이 약한 내부 네트워크로 접속 시도
    - 접근이 제어된 데이터를 열람 또는 수정
    - 시스템을 방해

침입자

- 침입자 행동패턴
  - 침입자 행동 패턴의 예(1/3)
    - 해커
      - 목적
        - 본인 만족을 위해 단순 목표를 찾아 수행
      - 대응 수단
        - 침입 탐지 시스템(IDS, Intrusion Detection System)
        - 침입 방지 시스템(IPS, Intrusion Prevention System)
        - 컴퓨터 비상 대응팀(CERT, Computer Emergency Response Team)
          - 목적: 시스템 취약점 대한 정보 수집
          - 수집된 정보를 시스템 관리자에게 배포

침입자

- 침입자 행동패턴
  - 침입자 행동 패턴의 예(2/3)
    - 범죄형 기업
      - 목적
        - 범죄자(해커 범죄 조직): 악의적인 목적을 가지고 시스템으로 침입
        - 데이터나 유용한 정보를 교환해 수사를 방해
          - 우회를 통해 추적하기 어려우며 흔적을 최소화 함
      - 대응 수단
        - IDS, IPS
        - 민감한 정보가 담긴 데이터 베이스 암호화
          - e.g., 신용카드 정보
        - 지정된 서버 사용 및 주기적인 모니터링
          - e.g., 전자 상거래

침입자

- 침입자 행동패턴
  - 침입자 행동 패턴의 예(3/3)
    - 내부 공격자
      - 목적
        - 시스템 내부 사용자의 실수 또는 고의적 보안 위협/공격
      - 방어 및 감지가 가장 어려움
      - 대응 수단
        - IDS, IPS
        - 접근 권한 범위 최소화(시간, 실질 데이터)
        - 상세한 로그 기록 보관
        - 민감한 데이터 접근 인증을 추가적으로 시행

침입자

- 침입
  - 목적
    - 시스템 접근 허가 획득
    - 주어진 접근 허용 범위 확대
  - 기법
    - 합법적 사용자의 패스워드 파일 획득
      - 최초의 침입은 패스워드 탈취부터 시작
      - 패스워드 파일에 대한 보호
        - 일방향 암호화(One-Way Encryption)
        - 접근 제어(Access Control)

침입자

- 침입 기법
  - 패스 워드 추측 방법 예시
    1. 패스 워드 추측
       - 로그인 시도를 해야 함
    2. 트로이 목마를 이용해 보다 높은 권한 획득 후, 패스 워드 추측
    3. 하드웨어로 도청
  - 탐지(Detection) 및 예방(Prevention)을 위한 보안을 구축해야 함

목 차

- 침입자
- 침입탐지 개요
- 침입탐지
- 패스워드 관리

침입탐지 개요

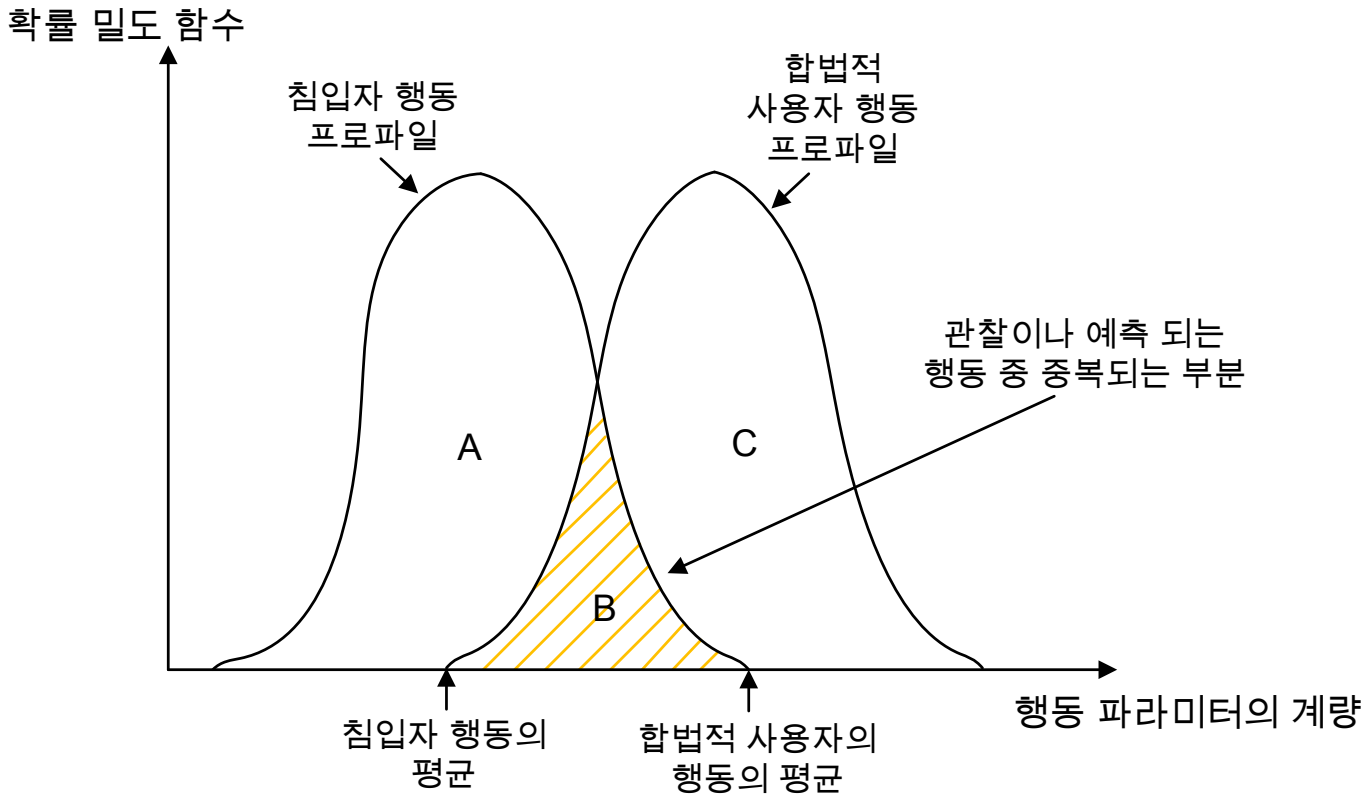
- 침입 탐지 시스템(IDS, Intrusion Detection System)
  - 개요
    - 정의
      - 침입의 패턴 데이터베이스와 Expert system을 사용해 이벤트를 모니터링하고 침입을 탐지 및 대응하는 자동화 보안 시스템
    - 등장배경
      - IP 주소와 포트 번호 만으로 침입·차단하는 방화벽의 한계
      - 신속한 탐지 및 대응
      - 침입 방지 시스템과 함께 구현하여 보안 시스템을 구축 필요성 증가

침입탐지 개요

- 침입 탐지 시스템(IDS, Intrusion Detection System)
  - 개요
    - 주요 기능
      - 네트워크나 시스템의 사용을 실시간 모니터링(Monitoring)
      - 침입 발생여부를 탐지(Detection)
      - 침입자를 조기에 발견하고 실시간으로 처리해 대응(Response)
    - 종류
      - 탐지영역에 따른 IDS 분류
        - H-IDS(Host-based IDS): 호스트 기반
        - N-IDS(Network-based IDS): 네트워크 기반
      - 침입 모델에 따른 기법 분류
        - Misuse Detection(M.D): 특정 이벤트의 관한 분석적 탐지
        - Anomaly Detection(A.D): 알려지지 않은 이벤트 탐지

침입탐지 개요

- 침입 탐지 시스템(IDS, Intrusion Detection System)
  - 개요
    - 구현 시 고려사항(1/2)
      - 제기되는 문제점 그림



침입탐지 개요

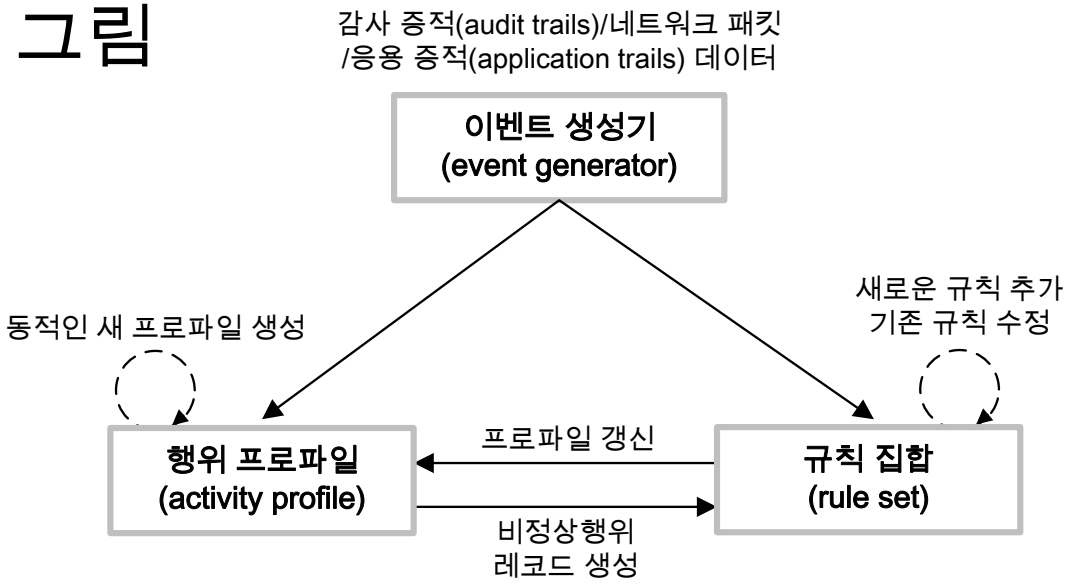
- 침입 탐지 시스템(IDS, Intrusion Detection System)
  - 개요
    - 구현 시 고려사항(2/2)
      - A: 침입자를 침입자로 판별
      - C: 합법적 사용자를 합법적 사용자로 판별
      - B
        - False Positive: 합법적 사용자를 침입자로 판단
        - False Negative: 침입자를 합법적 사용자로 판단

침입탐지 개요

- 감사 기록
  - 침입 탐지를 위한 데이터 수집을 기록
  - 종류
    - 기본 감사 기록(Native audit records)
      - 운영체제에서 제공하는 사용자 행동 정보 기록
      - 보안 감사를 위한 기록이 아닌 데이터도 기록
    - 탐지-전용 감사 기록(Detection-specific audit records)
      - IDS이 요구하는 데이터만 수집해서 감사 기록
      - 기본 감시 기록과 별도로 추가적인 감사 기록임
        - 한 시스템에서 두 감사 기록을 운영해야 함
      - 다양한 시스템에 적용 가능

침입탐지 개요

- 감사 기록
  - 탐지-전용 감사 기록 예시: Dorothy Denning 침입탐지 모델
    - 개요 및 정의
      - 1987년 최초의 침입 탐지 모델 발표
      - 호스트에 관계없이 독립적인 시스템 구조 개발
      - 사용자의 명령어 실행에 대한 시스템 기록
    - 구조 그림



침입탐지 개요

- 감사 기록
  - 탐지-전용 감사 기록 예시: Dorothy Denning 침입탐지 모델
    - 모델링을 통한 동작 재구성 시 장점
      - 객체에 영향을 주는 모든 행동 감사 가능
      - 단일-객체, 단일-동작 감사 기록은 모델링과 구현이 단순
    - 감사 기록 필드
      - 예시 감사 기록 그림

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 개요

- 침입 탐지 방법
  - 크게 두 가지로 나뉨
    - 통계적 방법
      - 합법적 사용자의 행동을 정의해 올바른 예상되는 이벤트를 정의
      - 임계 값 탐지, 프로파일 기반 사용
      - 신분위장자 탐지에 적절
    - 규칙-기반 방법
      - 특정 행동이 침입자의 행동인지 결정하기 위한 규칙을 정의
      - 변형 탐지, 침투 식별 사용
      - 불법 행위자 탐지에 적절
  - 실제 침입 탐지를 위해 두 가지 방법을 병행하여 적용

목 차

- 침입자
- 침입탐지 개요
- 침입탐지
- 패스워드 관리

침입탐지

- 통계적 변형 탐지
  - 임계 값 탐지 및 분석
    - 사용자에 무관하게 사건 발생빈도에 대한 임계 값을 정의
      - 일반적인 공격도 탐지 못함
    - 임계 값과 시간 간격을 결정하여 탐지 민감도를 높여 다른 기법과 병행해서 사용
  - 프로파일 기반 시스템
    - 각 동작에 대한 프로파일을 구성해 객체(개인 또는 그룹) 별 행동변화를 감지
    - 파라미터의 집합으로 구성
    - 감사 기록을 통해 평가지수(Mertrics)을 설정한 뒤 침입탐지

침입탐지

- 통계적 변형 탐지
  - 프로파일 기반 시스템
    - 대표적으로 사용되는 평가지수 정리 표

평가 지수	설명	예시
카운터	특정 시간(세션) 동안 이벤트 발생 횟수를 측정	• 한 시간 동안 로그인한 횟수 • 한 사용자가 세션 동안 실행한 명령의 횟수 • 1분당 패스워드 실패 횟수
게이지	특정 객체의 현재 상태 값을 측정	• 특정 응용 프로그램에 지정된 논리적 연결의 수 • 사용자 프로세스로 전송되기 현재 대기하고 있는 메시지의 수
간격 타이머	연관된 이벤트 사이의 시간 간격 길이 측정	• 한 계좌에 연속된 두 개의 로그인 사이의 시간 간격
자원 활용	지정된 시간 동안 소모된 자원의 양 측정	• 세션 동안 인쇄된 페이지 수 • 프로그램 실행에 걸린 총 시간

침입탐지

- 통계적 변형 탐지
  - 평가 지수 프로파일의 해석
    - 현재 작동 상태를 결정하기 위한 검사
  - 검사 방법
    - 평균과 표준편차(Mean and standard deviation)
      - 파라미터들의 평균과 표준편차를 측정
    - 다변수(Multivariate)
      - 두 개 이상의 평가 지수를 가지고 상관관계에서 침입 탐지를 도출
    - 마르코프 과정(Markov process)
      - 마르코프 과정을 사용해 현재와 직전 상태 사이의 의존되는 전이 확률을 이용해 도출

침입탐지

- 통계적 변형 탐지
  - 평가 지수 프로파일의 해석
    - 검사 방법
      - 타임 시리즈(Time series)
        - 특정 시간 간격 안에 너무 빠르거나 느리게 발생하는 연속적인 이벤트를 감지
        - 통계적 검사를 이용해 비정상적 타이밍을 정의
      - 운용 결과(Operational)
        - 일반적인 한계 값을 정의하고 이 한계를 벗어나는 동작을 침입을 탐지
    - 평가 지수와 모델을 사용해 IDS에서 사용된 방법들을 제시할 수 있음

침입탐지

- 통계적 변형 탐지
  - 침입 탐지 방법 정리 표(1/2)

방법	모델	탐지되는 침입 유형
로그인과 세션 동작		
일별 시간별 로그인 빈도 수	평균과 표준편차	침입자는 일과시간 이후에 침입을 시도
장소별 로그인 빈도 수	평균과 표준 편차	특정 사용자가 빈도 수가 낮은 장소에서 침입을 시도
마지막 로그인 이후 경과시간	운용적	사용 정지된 계좌에 침입
세션 당 소요시간	평균과 표준 편차	유의 수준 편차가 있다면 위장을 의심
장소의 출력 양	평균과 표준편차	과다한 양의 데이터가 특정 목적지로 전송되면 중요한 데이터가 유출
세션 자원 활용	평균과 표준편차	프로세서나 I/O가 비정상 레벨이면 침입자 의심
로그인에서 패스워드 실패	운용적	패스워드 추측을 통한 침입 시도 탐지
특정 터미널에서 로그인 실패	운용적	침입 시도

침입탐지

- 통계적 변형 탐지
  - 침입 탐지 방법 정리 표(2/2)

방법	모델	탐지되는 침입 유형
명령과 프로그램실행 동작		
실행 빈도 수	평균과 표준편차	다른 명령을 실행하는 침입자 탐지, 권한 상승에 성공한 합법적 사용자를 탐지
프로그램 자원 활용	평균과 표준 편차	I/O나 프로세서 활용에 영향을 미치는 비정상적인 값을 통해 멀웨어 침입 탐지
실행 거부	운용적	더 큰 권한을 획득하려는 개별 사용자의 침입 시도
파일접근 동작		
읽기, 쓰기, 생성, 삭제의 빈도 수	평균과 표준편차	개별 사용자에 대해 비정상적 읽기와 쓰기를 관찰해 위장을 탐지
읽기 기록, 쓰기 기록	평균과 표준편차	추론이나 축적을 통해 중요한 데이터를 취득하려는 시도 탐지
읽기, 쓰기, 생성, 삭제 실패 횟수	운용적	권한이 없는 파일에 지속적으로 접근을 시도하는 사용자를 탐지

침입탐지

- 규칙-기반 침임 탐지
  - 규칙의 집합을 이용해 시스템 안의 이벤트를 관찰하고 동작 패턴을 분석해 침입을 탐지
  - 두 가지 개념
    - 규칙-기반 변형 탐지(Rule-based anomaly detection)
      - 통계적 변형 탐지와 유사
      - 과거 감사 기록을 이용해 사용패턴을 식별
        - 과거 규칙 집합과 현재 행동을 비교
        - 규칙은 사용자, 프로그램, 권한, 시간 슬롯, 터미널 등 과거 행동을 의미

침입탐지

- 규칙-기반 침임 탐지
  - 두 가지 개념
    - 규칙-기반 침투 식별(Rule-based penetration identification)
      - 전문가 시스템(Expert system)
        - 특정 시스템의 알려진 약점을 이용해 침투하는 것을 탐지
        - 감사 기록이 아닌 보안 전문가을 통해 규칙 생성
        - 의심스런 행동을 정의한 규칙들을 가지고 전문가 시스템에 응용
      - 경험적 규칙 사용 예시
        - 다른 사용자의 개인 디렉토리에 대한 접근 제어
        - 지정된 사용 시간 외 접근은 이전 파일에 접근 가능성이 높음
        - 사용자는 직접적인 디스크 열람보다 상위계층 운영체제 유틸리티에 의존
        - 동일 시스템 중복 로그인 불가
        - 시스템 프로그램 복사 금지

침입탐지

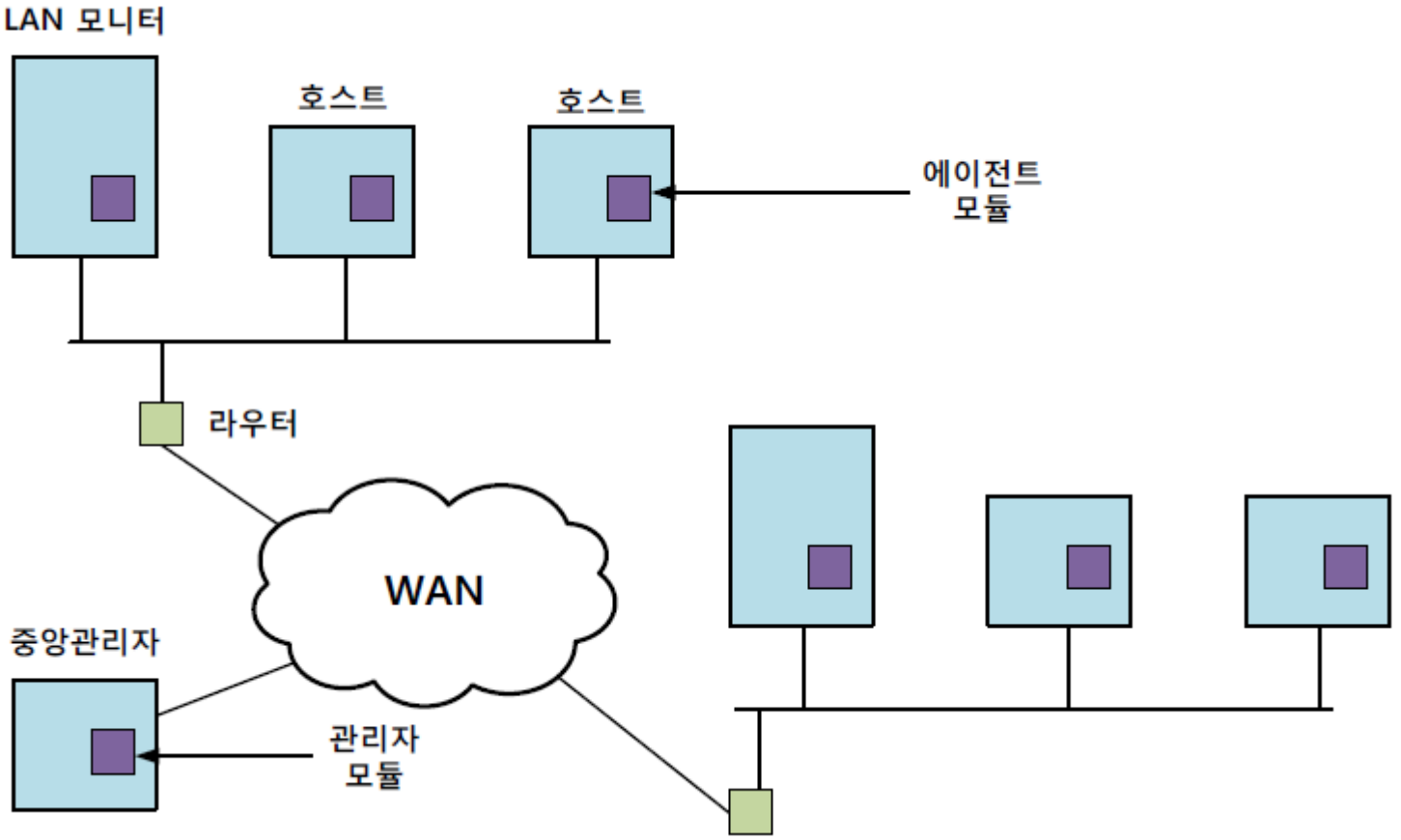
- 기본-비율 오류(Base-Rate Fallacy)
  - IDS는 낮은 낮은 가짜 경고율을 유지하면서 높은 탐지율을 유지해야 함
    - 확률의 기본 특성을 가지고 있기 때문에 만족시키기 어려움
- 분산 침입 탐지
  - 개요
    - 등장 배경
      - 단일-객체나 동작이 아닌 분산되어 있는 집단 시스템을 방어해야 할 필요성 증가
        - 네트워크를 포함해 집단을 관리

침입탐지

- 분산 침입 탐지
  - 개요
    - 문제점
      - 다양한 플랫폼과 환경에 호환될 수 있도록 새로운 보안 관련 감사 기록 포맷을 정의 및 적용해야 함
        - 침입 탐지 교환 형식 표준화 됨
      - 감사 기록을 공유하기 위한 통신에서도 기밀성과 무결성을 제공해야 함
      - 중앙 집중화 또는 비중심화 구조 자체 문제점
        - 중앙 집중화 구조: 병목현상 발생
        - 비중심화 구조: 분산 정보를 교환해야 함

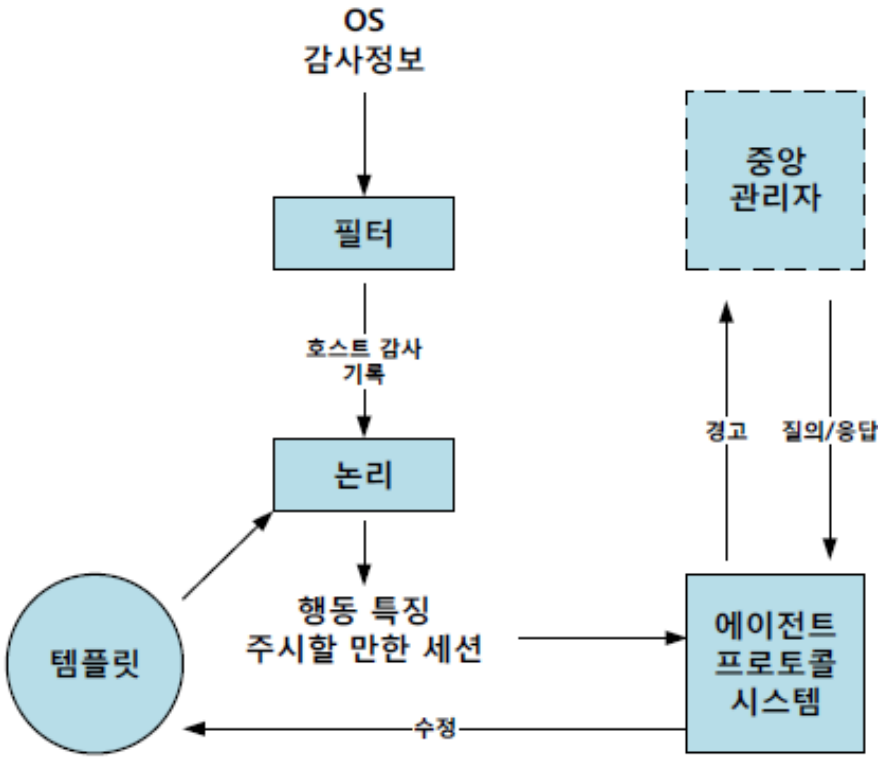
침입탐지

- 분산 침입 탐지
  - 분산 침입 탐지 구조 그림



침입탐지

- 분산 침입 탐지
  - 에이전트 구조 그림



침입탐지

- 허니팟
  - 정의
    - 공격자를 중요한 시스템으로부터 다른 곳으로 끌어내도록 설계한 유도 시스템
      - 허니팟을 향한 모든 공격이 성공된 것처럼 보이도록 설계
    - 시스템 노출 없이 공격자 동작패턴과 추적을 기록 가능
  - 설계 목적
    - 공격자의 행동 정보 수집
      - Event loggers를 이용
    - 관리자가 대응할 시간확보
      - 시스템에 머무르도록 유도
    - 중요 시스템 접근을 막음

목 차

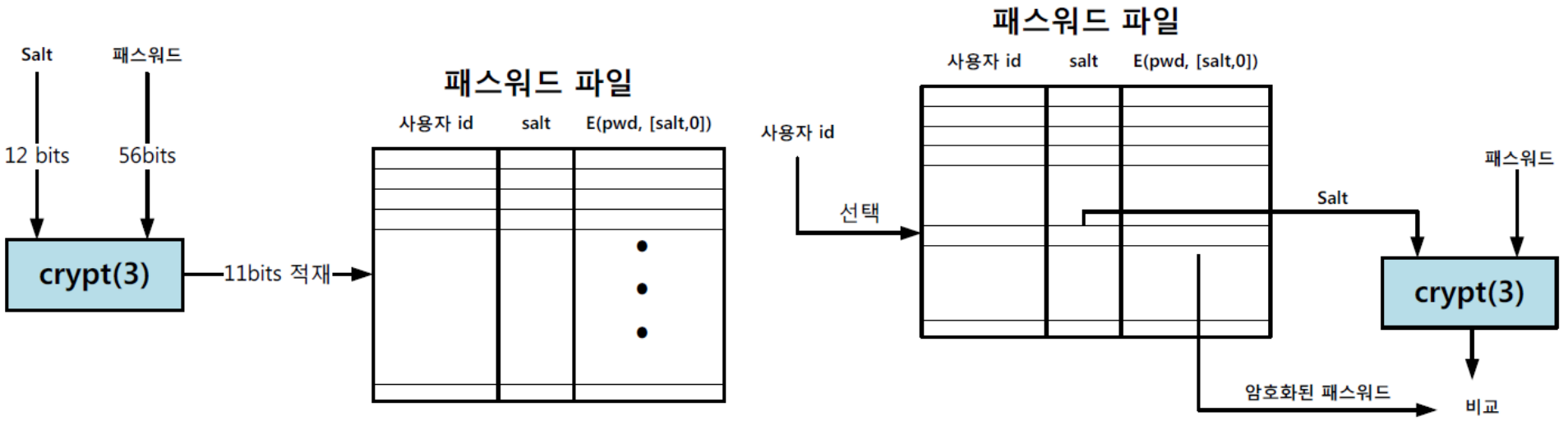
- 침입자
- 침입탐지 개요
- 침입탐지
- 패스워드 관리

패스워드 관리

- 패스워드 보호
  - 패스워드 시스템
    - 침입자에게 가장 먼저 나타나는 방어 시스템
      - 개인의 ID 인증
    - ID가 제공하는 보안
      - 사용자의 시스템 접근 권한 확인
      - 부여된 권한을 식별해 권한 수준 결정

패스워드 관리

- 패스워드 보호
  - 패스워드의 취약성
    - 패스워드-기반 시스템에 대한 위협
      - Salt: 추가적인 입력으로 사용되는 난수
    - UNIX 패스워드 구조 그림



패스워드 관리

- 패스워드 보호
  - 대표적인 보호 방법
    - 솔팅 (salting)
      - 패스워드를 암호화하여 적재 할 때 패스워드와 솔트를 결합하여 암호화 루틴으로 암호화 한 후 적재
    - 키 스트레칭 (key stretching)
      - 입력한 패스워드의 다이제스트를 생성한 뒤, 생성된 다이제스트를 입력 값으로 하여 또 다른 다이제스트를 생성하는 행위를 반복
      - 전수 공격으로 패스워드를 추측하는데 많은 시간을 소요하게 함
    - 접근제어
      - 공격자가 패스워드 파일에 접근하는 것을 막음
        - 여러 번의 정보 노출과 침입 문제를 방지할 수 있음

패스워드 관리

- 패스워드 선택 요령
  - 충분히 복잡하고 공격자가 예상할 수 없어야 하며, 사용자가 기억하기 쉽도록 설정해야 함
  - 패스워드 생성 기법
    - 사용자 교육(User education)
    - 컴퓨터-생성 패스워드(Computer-generated passwords)
      - 패스워드 랜덤성 때문에 외우기가 어려움
      - e.g.,FIPS PUB 181
        - 가장 잘 만들어진 자동화 패스워드 생성기
        - 발음할 수 있는 음절을 생성

패스워드 관리

- 패스워드 선택 요령
  - 패스워드 생성 기법
    - 반응 패스워드 검사(Reactive password checking)
      - 주기적으로 자체의 패스워드 크래커를 구동하여 추측 가능한 패스워드를 검색
        - 검색된 패스워드는 취소하고 해당 사용자에게 통지
      - 작업 수행에 비해 낮은 방어율과 많은 자원이 필요
    - 주도적 패스워드 검사(Proactive password checking)
      - 사용자가 자신의 패스워드를 선택한 뒤, 시스템이 패스워드 적합여부를 판단
      - 다양한 검사기 기법 존재
        - 규칙 조건 검사
        - 사전공격을 통한 비교
        - 마르코프 모델
        - Bloom 필터

감사합니다!