NETWORK SECURITY ESSENTIALS

- 침입자 -

Ki woon Moon

Protocol **E**ngineering **L**ab. **Sangmyung** University

2015. 02. 26

Content

- 침입자
- 침입탐지
- 패스워드 관리

침입자

보안 위협

- 가장 잘 알려진 두 가지 보안위협
  보통 해커나 크래커라고 알고 있는 침입자
  바이러스

침입자의 유형

- **신분위장자** (masquerader)

  컴퓨터를 사용할 권한이 없고 합법적 사용자의 계좌를 이용하기 위해 시스템의 접근제어를 뚫고 침투해 들어온 사람

침입자

침입자의 유형

- **불법행위자 (misfeasor)**

  낮은 권한을 가진 합법적 사용자로서 접근권한이 있어야만 접근할 수 있는 데이터, 프로그램, 그리고 자원에 접근하는 사람
  혹은 접근이 허락되었지만 권한을 남용하는 사용자

- **은밀한 사용자 (Clandestine user)**

  시스템의 관리 통제권을 장악하고 이 통제를 이용하여 감사와 접근제어를 피하거나 감사 수집(audit collection)을 못하도록 억제하는 사람

침입자

침입자의 공격 유형

- **양성 침입** (benign attack)

  손상을 초래하지 않는 장난용 바이러스
  화면상에 간헐적인 메시지를 띄우거나 키를 누를 때 소리가 나게 함

- **심각한 침입** (serios attack)

  민감한 정보의 열람
  보안이 안된 내부 네트워크에 접속
  데이터를 불법적으로 수정
  시스템을 방해하는 행위

침입자

컴퓨터비상대응팀의 설립

- **컴퓨터비상대응팀 (CERT : Computer Emergency Response Team)**
  - 침입자 문제에 대한 인식이 확대 되면서 컴퓨터비상대응팀이 설립됨
  - 시스템 취약점들에 대한 정보를 수집
  - 수집된 정보를 시스템 관리자들에게 널리 배포

✓ 시스템 관리자는 취약점에 대한 패치를 신속하게 진행
✓ 자동화된 업데이트 권장

침입 기법

침입자의 목적

- **침입자의 목적**
  - 시스템에 대한 접근 허락을 획득
  - 시스템에 대한 접근 허용 범위를 확대 하고자 함

- **침입자가 목적 달성을 위해 필요한 것**

  ✓ 일반적으로 침입자는 보호된 정보를 획득해야만 함
  ✓ 일반적으로 보호된 정보라 함은 사용자의 패스워드로 생각 할 수 있음
  ✓ 패스워드를 획득하면 침입자는 합법적 사용자에게 주어진 권한을 이용가능

침입 기법

패스워드를 알아내기 위한 기술

1. 시스템 설치 시 사용했던 기본 패스워드를 시도
   (많은 관리자들은 이 기본 패스워드를 바꾸는데 신경을 쓰지 않음)

2. 짧은 패스워드들을 모두 시도

3. 시스템의 온라인 사전에 있는 단어나 흔히 사용할 것 같은 패스워드를 시도
   (흔한 패스워드의 예들은 해커 전자 게시판에서 구할 수 있음)

침입 기법

패스워드를 알아내기 위한 기술

4. 사용자의 이름, 배우자나 아이들의 이름, 사무실의 사진, 취미와 관련된 사무실 안의 책들 같은 사용자와 관련된 정보를 수집

5. 사용자의 전호번호, 주민등록번호 등을 시도

6. 자동차 번호판 번호를 시도

7. 접근제한을 우회하기 위해서 트로이 목마를 이용

8. 원격 사용자와 호스트 시스템 사이의 선을 도청

침입 탐지

침입 탐지의 중요성

1. 만일 침입을 아주 빨리 탐지할 수 있다면 침입자를 식별할 수 있고 시스템에 해를 주거나 데이터들이 위협당하기 전에 시스템에서 제거 가능

   비록 침입자를 탐지해 내는데 시간이 걸렸다 하더라도, 침입자를 빨리 찾으면 빨리 찾을수록 피해는 더 적어질 수 있고 보다 신속하게 피해복구 가능

2. 효과적인 침입탐지 시스템을 갖추고 있으면 침입을 하려는 의도를 단념시키게 되어 침입을 예방하는 효과

3. 침입탐지를 통해 침입예방 시설을 강화하는데 사용할 침입 기술에 관한 정보를 수집 가능

침입 탐지

침입자의 행동 양식

- 전형적 침입자의 행동이 합법적 사용자의 전형적인 행동과 다르기는 하지만 이 행동들에는 겹치는 부분이 존재

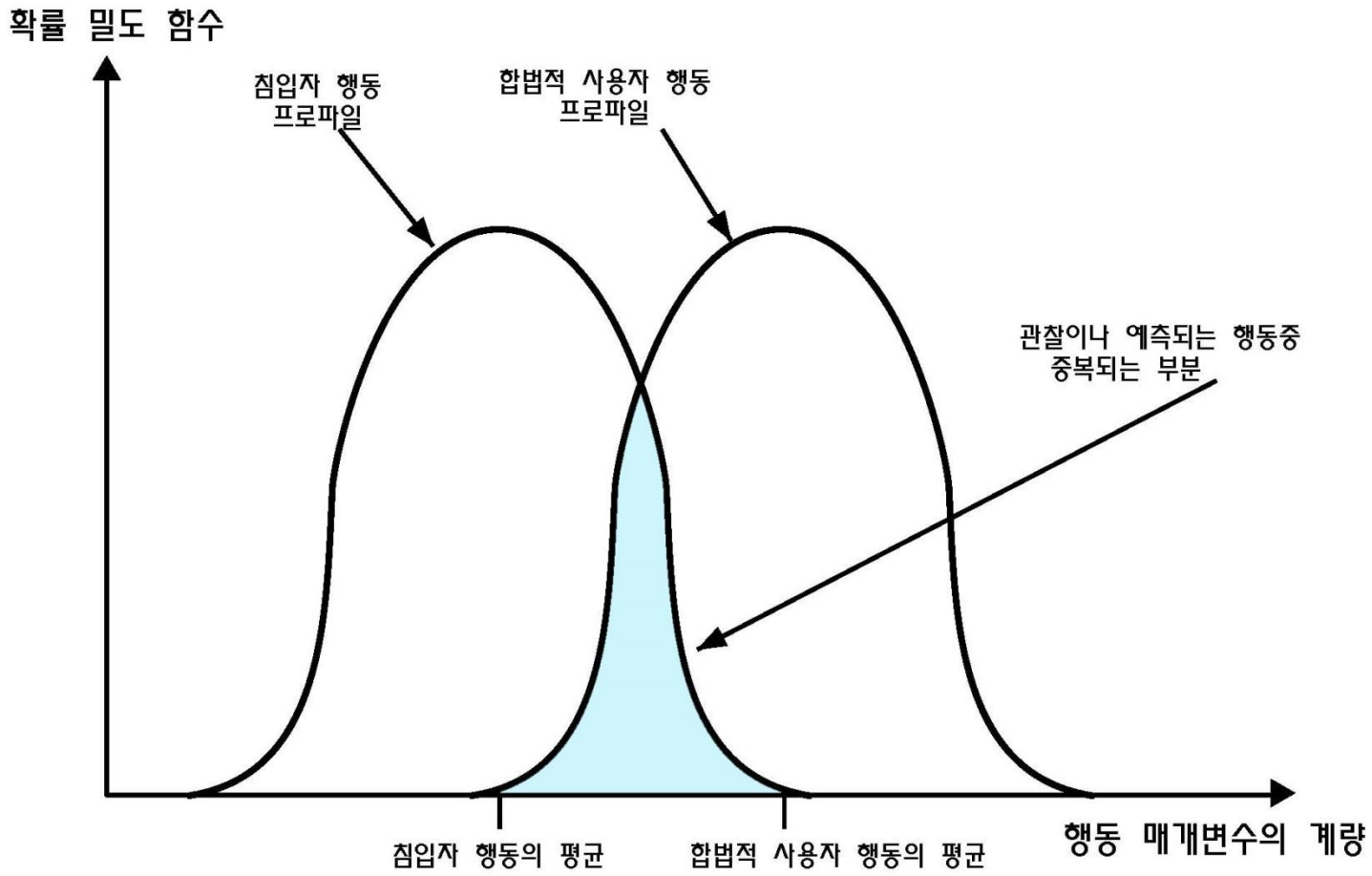
- 침입자의 행동을 넓게 잡다 보면 더 많은 침입자를 찾아낼 수는 있겠지만 어떤 경우에는 합법적 사용자를 침입자로 판단하게 되는 "긍정 오류(false positives)"를 유발

- 침입자의 행동을 너무 좁게 잡으면 침입자를 합법적 사용자로 판단하게 되는 "부정 오류(false negative)"을 유발

- 침입탐지를 실제에 적용할 때에는 절충과 기술의 요소를 적절히 사용해야 함

침입 탐지

침입자의 행동과 합법 사용자의 행동 프로파일



침입 탐지의 기본 도구

감사 기록

- 기본 감사 기록

  대부분의 다중 사용자 운영체제에는 사용자 동작에 대한 정보를 수집하는 어카운팅 소프트웨어가 존재

  ✓ 어카운팅 소프트웨어 : 시스템의 이용시간, 양 등을 측정하고 기록하여 이용도에 따라 요금을 산출하는 소프트웨어

  - 장점

    다른 추가적인 정보 수집 소프트웨어가 필요치 않음

  - 단점

    기본 감사기록이 필요한 정보를 포함 하지 않을 수 있음

    수집된 정보의 형태가 사용할 수 없는 형태의 정보일 수 있음

침입 탐지의 기본 도구

감사 기록

- 탐지-전용 감사 기록
  수집 장치는 오직 침입탐지 시스템이 요구하는 정보만 골라 수집하는 감사 기록을 생성하도록 구현

  - 장점
    다양한 시스템에 붙여 사용할 수 있음

  - 단점 :
    시스템에서 두 개의 수집 소프트웨어를 구동하므로 시스템에 부담이 생김

침입 탐지를 위한 방법

통계적 변형 탐지 (Statistical anomaly detection)

- 상당기간 행동과 관련하여 수집한 데이터를 분석
- 그 행동이 합법적 사용자의 행동인지 아닌지를 판단하기 위해 통계적 점정을 시행

  - 임계값 탐지 (Threshold detection)

    임계값 탐지는 한 개의 시간 간격동안 특정 사건의 발생회수를 세는 방법

    그 회수가 생각하기에 합리적인 수라고 기대되어지는 값을 넘어서면 침입이 있다고 판단

  - 프로파일 기반(Profile based) 시스템

    개별적 사용자들이나 관련된 사용자 그룹의 과거 행동들을 특성화 하는데 중점을 두고 심각한 변화가 있는지를 감지

    프로파일은 매개변수들의 한 집합으로 이뤄지기 때문에 오직 한 매개변수에 대한 변화가 있다고 해서 경고를 해야 할 정도라고 보기 어려울 수 있음

침입 탐지를 위한 방법

프로파일 기반 침입탐지 평가지수

- 카운터

  어떤 사건유형의 발생횟수를 특정 시간 간격 동안 세는 것

  - ✓ 한 사용자가 한 시간 동안 로그인한 횟수
  - ✓ 한 사용자 세션 동안 실행한 명령의 횟수
  - ✓ 분당 패스워드 실패 횟수

- 게이지

  어떤 개체의 현재 값을 측정하는데 사용

  - ✓ 사용자 프로세스로 전송 되기 위해 대기하고 있는 메시지의 수

침입 탐지를 위한 방법

프로파일 기반 침입탐지 평가지수

- **간격 타이머**
  두 개의 연관된 사건 사이의 시간 길이
  - ✓ 연속된 두개의 로그인 사이의 시간 간격

- **자원 활용**
  지정된 시간 동안 소모된 자원의 양
  - ✓ 사용자의 세션 동안 인쇄된 페이지의 수
  - ✓ 프로그램 실행에 걸린 총 시간

침입 탐지를 위한 방법

침입 탐지에 사용되는 검사 방법

방법	모델	탐지되는 침입유형
로그인과 세션 동작		
일별 시간별 로그인 빈도수	평균과 표준편차	침입자는 일과시간 이후에 침입을 시도할 것이다.
장소별 로그인 빈도수	평균과 표준편차	침입자는 특정 사용자가 드물게 사용하거나 사용하지 않는 장소에서 침입을 시도할 것이다.
마지막 로그인 이후 경과시간	운용적	"사용 정지된(dead)" 계좌에 침입
세션 당 소요시간	평균과 표준편차	유의수준의 편차가 있다면 위장이 있음을 말해 줄 것이다.
장소의 출력 양	평균과 표준편차	과다한 양의 데이터가 원격지로 전송되면 중요정보가 누출되는 것을 나타낸다.
세션 자원 활용	평균과 표준편차	프로세서나 I/O 가 비 정상적 레벨이면 침입자가 있음을 말해준다.
로그인에서 패스워드 실패	운용적	패스워드 추측을 통한 침입시도
특정 터미널에서 로그인 실패	운용적	침입시도

침입 탐지를 위한 방법

침입 탐지에 사용되는 검사 방법

방법	모델	탐지되는 침입유형
명령과 프로그램 실행 동작		
실행 빈도수	평균과 표준편차	다른 명령을 사용하는 침입자를 탐지할 수 있다. 실제의 권한 보다 더 큰 권한을 획득하는데 성공한 합법적 사용자를 탐지할 수 있다.
프로그램 자원 활용	평균과표준편차	I/O 나 프로세서 활용에 부가적 영향을 끼치는 비정상적인 값은 바이러스나 트로이목마의 침입을 나타낸다.
실행 거부	운용적	더 큰 권한을 획득하려는 개별사용자의 침입 시도를 탐지할 수 있다.
파일접근 동작		
읽기, 쓰기, 생성, 삭제의 빈도수	평균과 표준편차	개별 사용자에 대해 비정상적 읽기와 쓰기는 위장이나 관찰이 있음을 나타낸다.
읽기 기록, 쓰기기록	평균과표준편차	추론이나 축적을 통해 중요한 데이터를 취득하려는 시도가 있음을 나타낸다.
읽기, 쓰기, 생성, 삭제 실패회수	운용적	권한이 없는 파일에 지속적으로 접근을 시도하는 사용자를 탐지해낼 수 있다.

침입 탐지를 위한 방법

규칙-기반 침입탐지 (Rule-based detection)

- 시스템 안의 사건들을 관찰하고 주어진 동작패턴이 의심스러운지 아닌지를 판단하는데 규칙들의 집합을 적용하여 탐지하는 방법

  - 규칙-기반 변형 탐지 (Rule-based anomaly detection)

    과거 감사기록을 이용하여 사용패턴을 식별하고 패턴을 묘사하는 규칙을 생성

    현재의 행동을 관찰 한 후 규칙의 집합과 비교하여 과거의 패턴과 일치하는지 판단

    ✓ 규칙은 권한, 시간, 터미널 등의 과거 행동

  - 규칙-기반 침투 식별(Rule-based penetration identification)

    전문가 시스템

    시스템 관리자와 보안 해독가로부터 보안을 위협하는 시나리오와 중요한 사건의 정보를 수집

    ✓ 규칙은 감사기록 분석이 아닌 전문가가 만듦

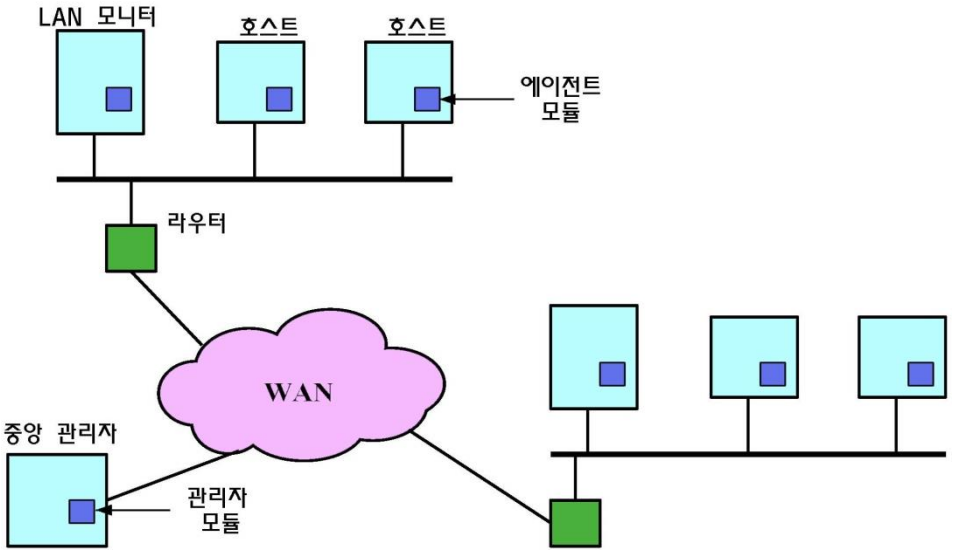
분산 침입 탐지

분산 침입 탐지 시스템의 필요성

- 최근까지 침입탐지 시스템에 대한 생각은 단일 시스템에 국한됨
- 일반적인 기관은 LAN이나 인터네트워크에 의해 분산되어진 호스트들을 집단적으로 방어해야 함

분산 침입 탐지

- **호스트 에이전트 모듈**
  호스트에서 일어나는 보안관련 사건들에 대한 데이터를 수집하고 중앙관리자에게 전송
- **LAN모니터 에이전트 모듈**
  호스트-호스트 연결, 사용된 서비스와 트래픽의 양을 감사하고 중앙관리자에게 전송
- **중앙 관리자 모듈**
  LAN 모니터 에이전트와 호스트 에이전트로부터 보고를 받음
  침입을 탐지하기 위해서 서로 다른 에이전트 간의 감사기록을 연관지음
  전문가 시스템을 갖추고 있음



패스워드 관리

- **패스워드 시스템**

  침입자에 대하여 가장먼저 하는 방어시스템

  ✓ 대부분의 다중사용자 시스템들은 사용자에게 식별자(ID)를 제공

  ✓ 패스워드는 시스템에 로그인하는 개인의 ID를 인증하는 역할

패스워드 관리

- **패스워드 시스템 보완**

  - **솔팅 (salting)**

    패스워드를 암호화하여 적재 할 때 패스워드와 솔트를 결합하여
    암호화 루틴으로 암호화 한 후 적재
    - ✓ 솔트 (salt) : 바이트 단위의 임의의 문자열

  - **키 스트레칭 (key stretching)**

    입력한 패스워드의 다이제스트를 생성하고 생성된 다이제스트를 입력값으로 하여
    다이제스트를 생성하고 이런 행위를 반복
    - ✓ Brute-force 공격으로 패스워드를 추측하는 데 많은 시간을 소요하게 함

패스워드 관리

- **패스워드 시스템 보완**

  - **솔팅 (salting)**

    패스워드를 암호화하여 적재 할 때 패스워드와 솔트를 결합하여
    암호화 루틴으로 암호화 한 후 적재
    - ✓ 솔트 (salt) : 바이트 단위의 임의의 문자열

  - **키 스트레칭 (key stretching)**

    입력한 패스워드의 다이제스트를 생성하고 생성된 다이제스트를 입력값으로 하여
    다이제스트를 생성하고 이런 행위를 반복
    - ✓ Brute-force 공격으로 패스워드를 추측하는 데 많은 시간을 소요하게 함

패스워드 관리

- **패스워드의 길이문제**

  어떤 사용자들은 그들의 패스워드를 선택해야 할 때 터무니없이 짧게 만듦
  대략 7,000 개의 사용자의 패스워드 조사

길이(Length)	건수(Number)	비율(%)
1	55	0.4
2	87	0.6
3	212	2
4	449	3
5	1,260	9
6	3,035	22
7	2,917	21
8	5,772	42
총합	13,787	100

패스워드 관리

- **패스워드의 선택문제**
  - 패스워드의 길이는 문제의 아주 일부분
  - 많은 사람들은 패스워드를 선택해야 할 때 쉽게 추측 가능한 정보로 생성
    - ✓ 자신의 이름
    - ✓ 집 주소의 길 이름
    - ✓ 평범한 사전 단어 등

    이런 요인들은 패스워드 크래킹을 쉽게 만듦

패스워드 관리

- **사용자의 패스워드 선택을 돕는 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

- **사용자의 패스워드 선택을 돕는 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

- **사용자 교육**
  - 사용자들에게 추측이 어려운 패스워드를 사용해야 하는 것이 왜 중요한지 알림
  - 강한 패스워드를 선택하는 요령을 알려줌
  - 사용자 교육은 대부분의 경우 별로 좋은 효과를 거두지 못함
  - 많은 사용자들은 그냥 선택요령을 무시함

패스워드 관리

- **컴퓨터 생성 패스워드**
  - 패스워드를 만드는 방법을 랜덤하게 함
  - 사용자들이 기억하기 어려우므로 별도로 기록하게 됨
  - 좋은 효과를 거두지 못함

패스워드 관리

- **반응 패스워드 검사**
  - 시스템이 주기적으로 자체의 패스워드 크래커를 구동하여 추측 가능한 패스워드를 찾아냄
  - 시스템은 취약한 패스워드를 취소하고 사용자에게 알림
  - 이 작업을 수행하려면 많은 자원(CPU 구동)을 필요로 함
  - 반응 패스워드 검사가 끝나기 전 까지 검사전의 패스워드들은 취약함

패스워드 관리

- **주도적 패스워드 검사**
  - 사용자가 자신의 패스워드를 선택할 수 있음
  - 시스템은 사용자가 선택된 패스워드를 검사하여 적합하지 않으면 거절함
  - 추측할 수 없고, 기억하기 좋은 패스워드들을 선택 가능

패스워드 관리

- **주도적 패스워드 검사 방법**

  ◆ 방법 1

  ✓ 모든 패스워드들은 적어도 여덟 문자의 길이를 가져야 함

  ✓ 처음 여덟 문자들 안에 패스워드는 적어도 한 개의 대문자, 소문자, 숫자,구두점 중 하나를 포함해야 함

  ◆ 방법 2

  ✓ "안전하지 않은" 패스워드들을 수집하여 큰 사전을 만듦

  ➢ 단점 : 공간적, 시간적 문제