KISA

침입탐지 시스템 (IDS)

2000. 9. 19

김민수

mskim@kisa.or.kr

한국정보보호센터
KorealformationSecurityInformation

내용

- 침입탐지
- 수집 정보
- 분석 방법
- 탐지 기술
- 대응
- 기술적 이슈
- IDS 특징과 기능
- IDS와 네트워크 구성요소
- Forensics

침입탐지

- (R. G. Bace) *Intrusion detection is the process of monitoring the events occurring in a computer system or network.*
- (B. Mukherjee) *An intrusion detection system is a system that attempts to identify intrusions, which we define to be unauthorized uses, misuses, or abuses of computer systems by either authorized users or external perpetrators.*
- (D. Denning) *An Intrusion detection system is a software with the functions of detecting, identifying and responding to unauthorized or abnormal activities on a target system.*

침입탐지 시스템

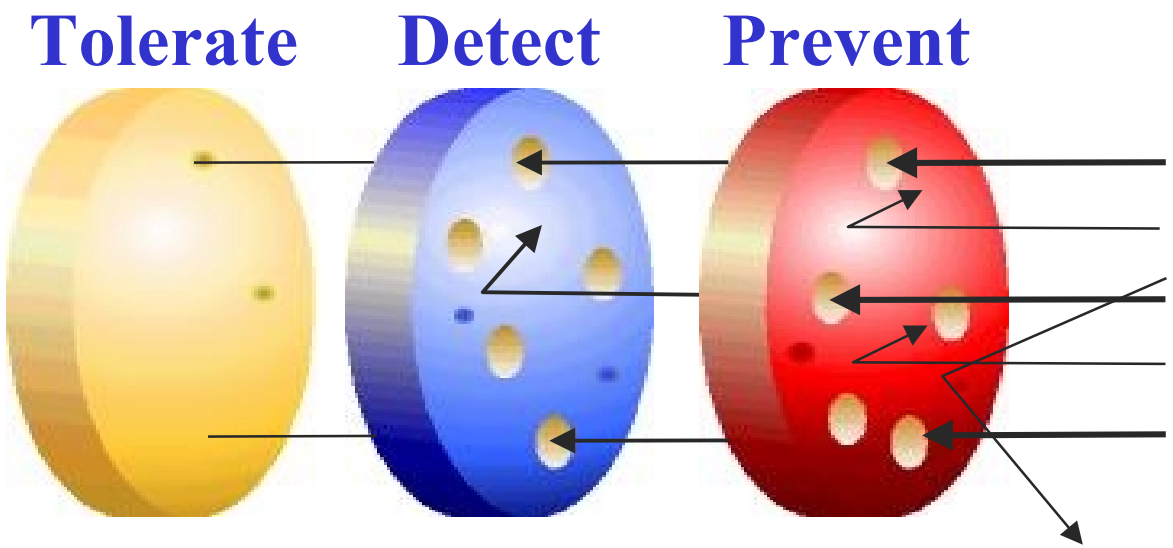
- Intrusion detection systems help computer systems prepare for and deal with attacks.
- Functions:
  - monitoring and analysis of user and system activity
  - auditing of system configurations and vulnerabilities
  - assessing the integrity of critical system and data files
  - recognition of activity patterns reflecting known attacks
  - statistical analysis for abnormal activity patterns
  - recognition of user activity reflecting policy violations

평가 요소

- False positive : detection of non-attacks.
- False negative : non-detection of attacks.
- Real-time detection
- Scalability
- User Interfaces

Layered Defense

- An ounce of prevention is worth a pound of detection



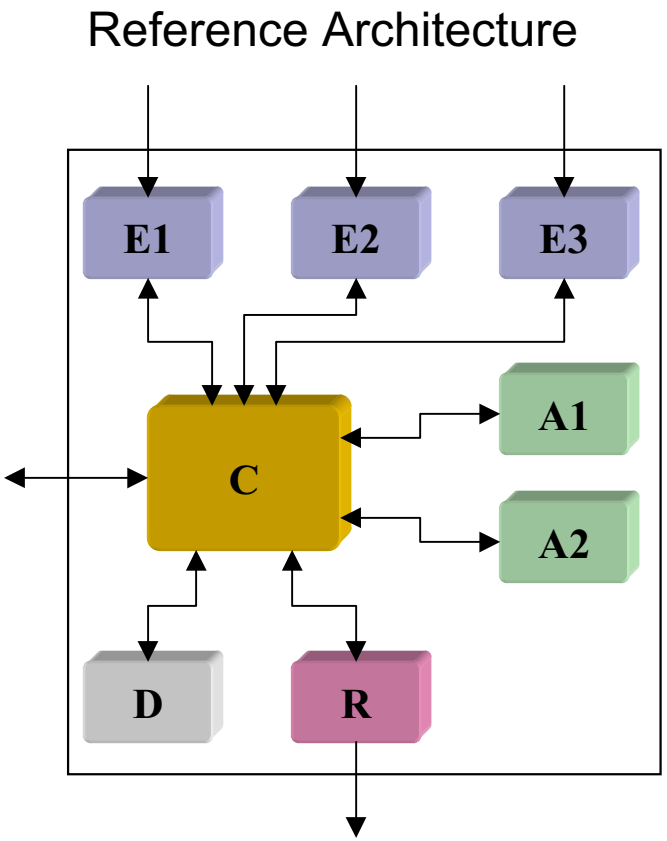
IDS 배치

- 공격탐지(Attack Detection)
  - 보안 구성요소 외부에 IDS를 두는 것
  - attacks should not affect it!
- 침입탐지(Intrusion Detection)
  - 보안 구성요소 내에 두어 부적절한 행위를 탐지
  - When the IDS alarm goes off, it's a red alert
- 현실적으로 침입탐지를 먼저 하는 것이 좋다.
  - 공격탐지는 관리 비용이 많이 든다.

데이터 수집

- IDES
- Audit
- Inline
- Hybrid(a mix of both Audit and Inline)

Common Intrusion Detection Framework

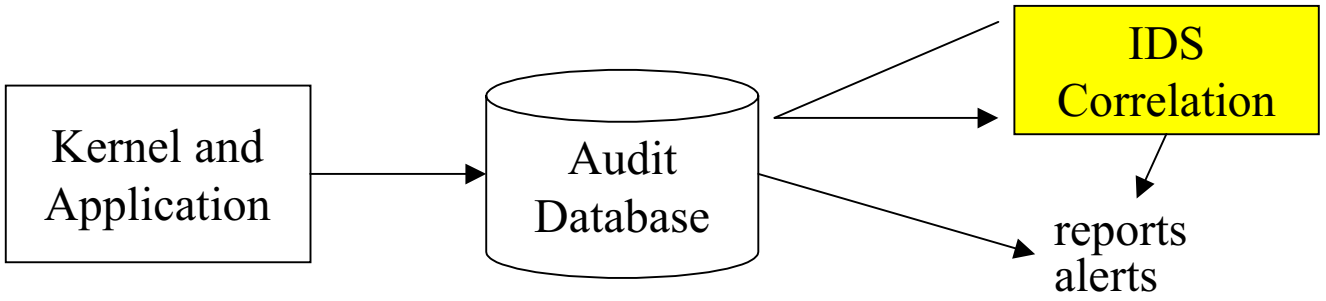


- Standard Interface (IDWG)
  - an Interconnection Framework for data collection, analysis, and response components
  - extensible architecture
  - reuse of core technology
  - facilitate tech. transfer
  - reduce cost

E : Event generators
A : Event Analyzers
C : System-specific Controller
D : Event Databases
R : Response units

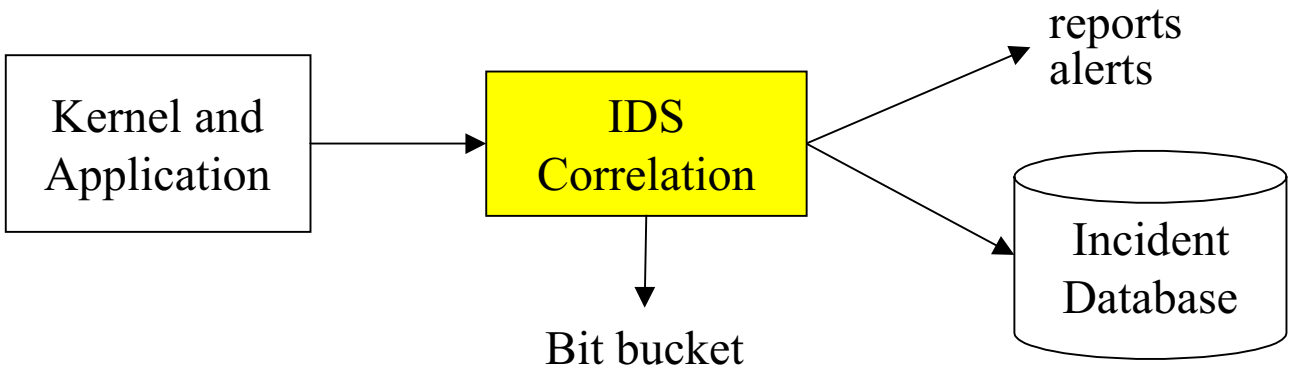
Audit based IDS

- 먼저 로그를 기록한 후 사후 처리.
- 일괄처리 방법이 주로 사용된다.
- 대상
  - Orange book
  - 비정상적인 로그인, 이상한 재부팅과 시간 변경, 비정상적인 에러 메시지, 잘못된 로그인 시도, 이상한 곳으로부터 로그인 등.



Inline IDS

- 전형적으로 중요하지 않은 감사 데이터는 버린다.
- 커널이나 응용프로그램에서 로그를 수집한 후 IDS가 탐지하고 나서 경고 메시지를 보내고 중요한 내용만 데이터베이스에 저장한다.



Information Sources

- 감사(audit)
  - 시스템 이벤트의 날짜순 레코드를 생성하고, 기록하고, 검사하는 과정을 말한다.
- 감사 축약(audit reduction)
  - 감사기록을 필터링하거나 중복되거나 관계없는 정보를 확인하고 제거하는 과정을 말한다.
- 좋은 소스는 무엇인가?
  - 공격의 증거를 알 수 있는 것.

Host-based information sources

- 운영체제 감사 증적(監□ □□)
  - 감사 증적(audit trail)
    - 하나 이상의 감사 파일에서 수집된 시스템 행위에 대한 정보
  - 감사 파일(audit file)
    - 하나의 시스템 이벤트를 표시하는 감사 레코드 집합.
  - 감사레코드(audit record)
    - 사용자 행위나 프로세스에 의해 생성되는 것
    - 여러 감사 토큰(audit token)으로 구성된다.

Host-based information sources
Sun Solaris BSM

- BSM 감사 시스템 구조
  - 이벤트들은 감사 관리 목적에 따라 감사 이벤트 클래스로 그룹화된다.
  - header token, argument token, data token, subject token, return token
- 시스템 감사 관리 도구
  - *auditreduce* : 속성에 따라 감사 파일에서 감사레코드를 선택한다.
  - *praudit* : 이진 형식의 감사 레코드를 문자 형식으로 변환한다.

Host-based information sources
Windows NT

- NT 이벤트 로깅 메커니즘 구조
  - System log : 드라이버 또는 다른 구성요소 실패, 응용 소프트웨어 이상, 데이터 손실 관련 에러
  - Application log : 응용프로그램에 의해서 수행되는 로그
  - Security log : 로그인 로그오프, 시스템 자원 관련 이벤트 (특히, 파일이나 객체의 삭제, 변경)
- 이벤트 기록 형식
  - date, time, user name, computer name, event id, source(software), type, category
- 감사 정책(audit policy)
  - 로그온/로그오프, 객체 접근, 특권 사용, 계정 유지, 정책 변경, 시스템 이벤트, 프로세스 추적

Host-based information sources

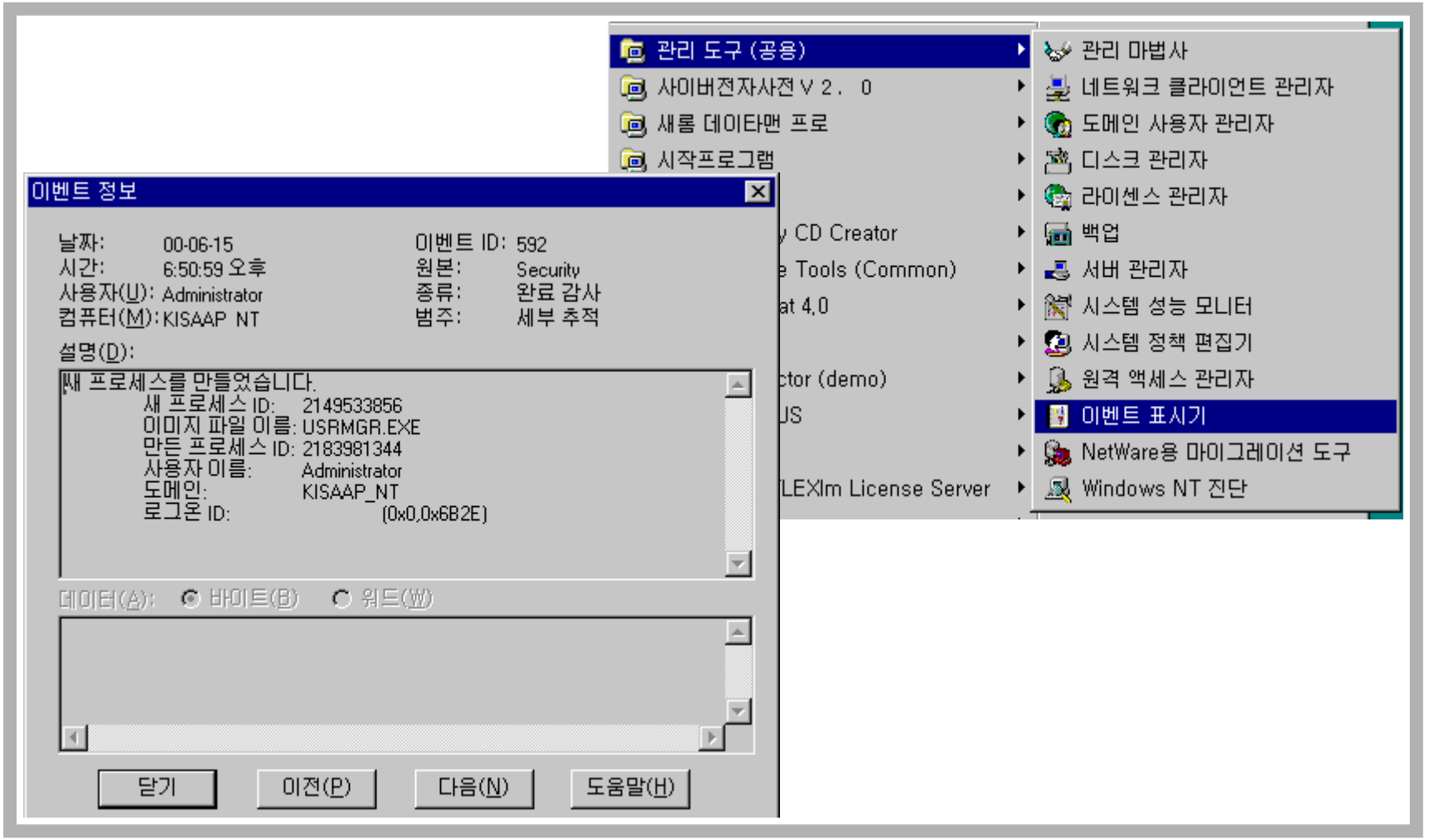
Windows NT (Event Viewer)

₩₩KISAAP_NT의 이벤트 표시기 - 보안 로그

로그(L) 보기(V) 옵션(O) 도움말(H)

날짜	시간	원본	범주	이벤트	사용자	컴퓨터
00-06-15	6:53:21 오후	Security	권한 사용	578	Administrator	KISAAP_NT
00-06-15	6:53:21 오후	Security	세부 추적	592	Administrator	KISAAP_NT
00-06-15	6:52:59 오후	Security	세부 추적	593	SYSTEM	KISAAP_NT
00-06-15	6:52:59 오후	Security	세부 추적	592	SYSTEM	KISAAP_NT
00-06-15	6:52:19 오후	Security	세부 추적	593	SYSTEM	KISAAP_NT
00-06-15	6:52:18 오후	Security	세부 추적	592	SYSTEM	KISAAP_NT
00-06-15	6:51:58 오후	Security	세부 추적	593	SYSTEM	KISAAP_NT
00-06-15	6:51:57 오후	Security	세부 추적	592	SYSTEM	KISAAP_NT
00-06-15	6:51:49 오후	Security	세부 추적	593	Administrator	KISAAP_NT
00-06-15	6:51:29 오후	Security	세부 추적	592	Administrator	KISAAP_NT
00-06-15	6:51:11 오후	Security	세부 추적	593	Administrator	KISAAP_NT
00-06-15	6:51:11 오후	Security	개체 액세스	562	SYSTEM	KISAAP_NT
00-06-15	6:51:01 오후	Security	개체 액세스	562	SYSTEM	KISAAP_NT
00-06-15	6:51:01 오후	Security	개체 액세스	560	Administrator	KISAAP_NT
00-06-15	6:51:01 오후	Security	개체 액세스	562	SYSTEM	KISAAP_NT
00-06-15	6:51:01 오후	Security	개체 액세스	560	Administrator	KISAAP_NT
00-06-15	6:51:01 오후	Security	개체 액세스	562	SYSTEM	KISAAP_NT
00-06-15	6:51:01 오후	Security	개체 액세스	560	Administrator	KISAAP_NT
00-06-15	6:51:01 오후	Security	개체 액세스	562	SYSTEM	KISAAP_NT
00-06-15	6:51:01 오후	Security	개체 액세스	560	Administrator	KISAAP_NT
00-06-15	6:51:01 오후	Security	개체 액세스	560	Administrator	KISAAP_NT
00-06-15	6:50:59 오후	Security	세부 추적	592	Administrator	KISAAP_NT
00-06-15	6:50:50 오후	security	시스템 이벤트	517	SYSTEM	KISAAP_NT

Host-based information sources
Windows NT (Event Detail Dialog)



Host-based information sources

System logs

- UNIX 운영체제는 ***syslog*** 서비스를 이용한 풍부한 시스템 로그를 제공한다.
- Sun Solaris system logs
  - *pacct* : 사용자 수행 명령어와 자원 사용량
  - *loginlog* : 모든 로그인 실패
  - *sulog* : *su* 명령어 사용 내역
  - *utmp*(*x*) : 현재 로그인한 사용자 리스트
  - *wtmp*(*x*) : 로그인/로그아웃, 시스템 시작, 시스템 종료에 대한 시간 기록
  - *nis.trans* : NIS namespaces의 변경 리스트

Network-based information sources

- 네트워크 패킷(network packets)
  - 마구잡이모드(***promiscuous mode***) :

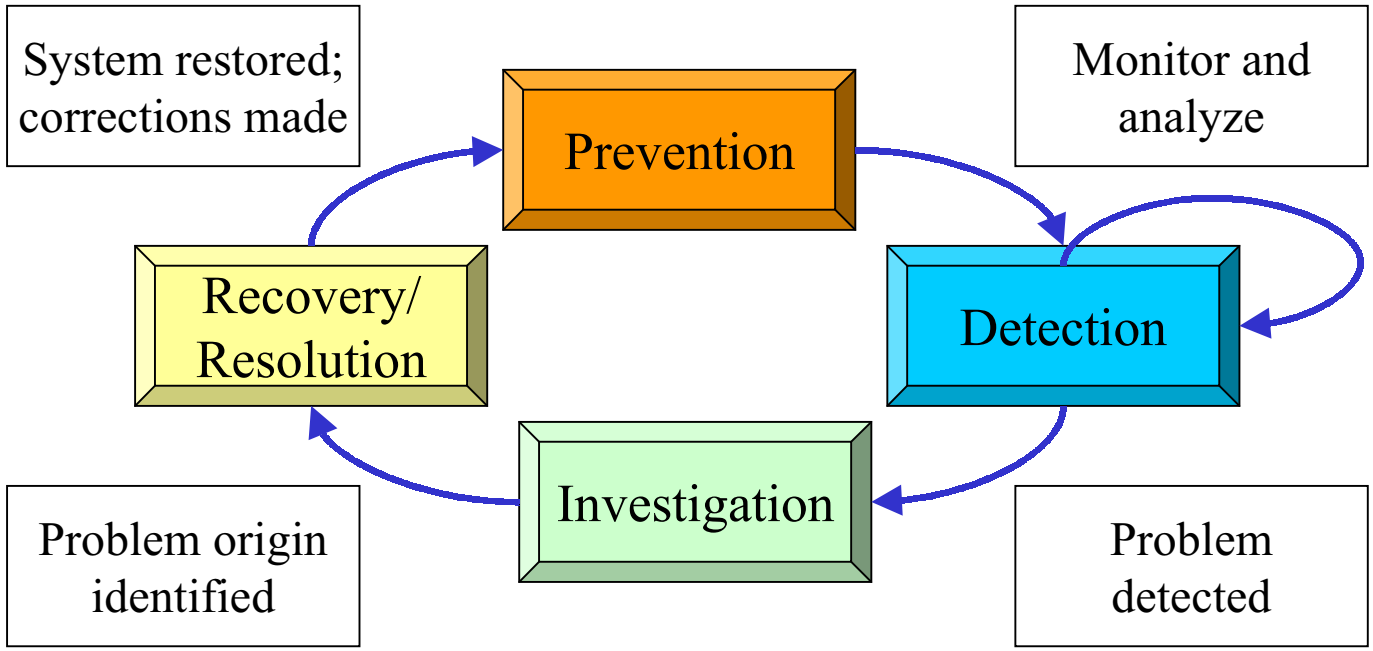
    네트워크 세그먼트를 통과하는 모든 네트워크 왕래 패킷을 가로채도록 하는 네트워크 인터페이스 설정이다.
  - 네트워크 기반 IDS는 네트워크 세그먼트의 왕래 패킷을 검사한다.

Network-based information sources
Packet capture

- Windows/NT packet capture options
  - SMS(Systems Management Server)
- UNIX packet capture options
  - CSPF(CMU/Stanford Packet Filter)
  - BPF(Berkeley Packet Filter)
- Libpcap
  - *tcpdump* 에서 사용되는 packet capture library.
- STREAMS-based packet capture
  - packet capture와 버퍼링(buffering)은 표준 STREAMS libraries (*pfmod* and *bufmod*, in Solaris)로 제공된다.

Analysis Schemes

- 분석(analysis)
  - 사용자와 시스템 행위에 대한 데이터를 분류하고 묘사하여 관심 있는 행위를 확인하는 것.

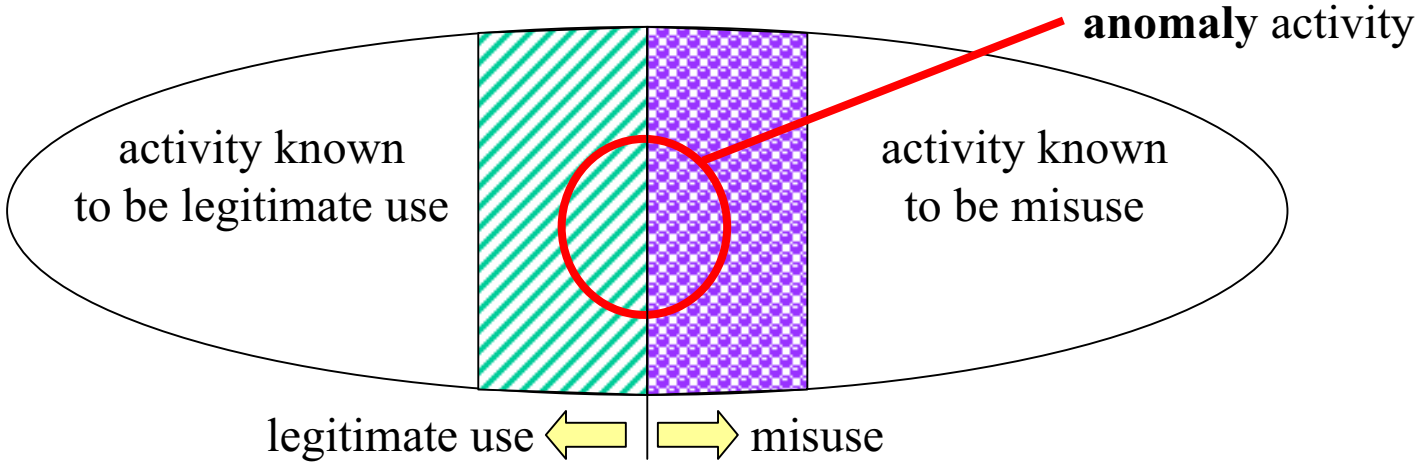


Analysis Paradigms

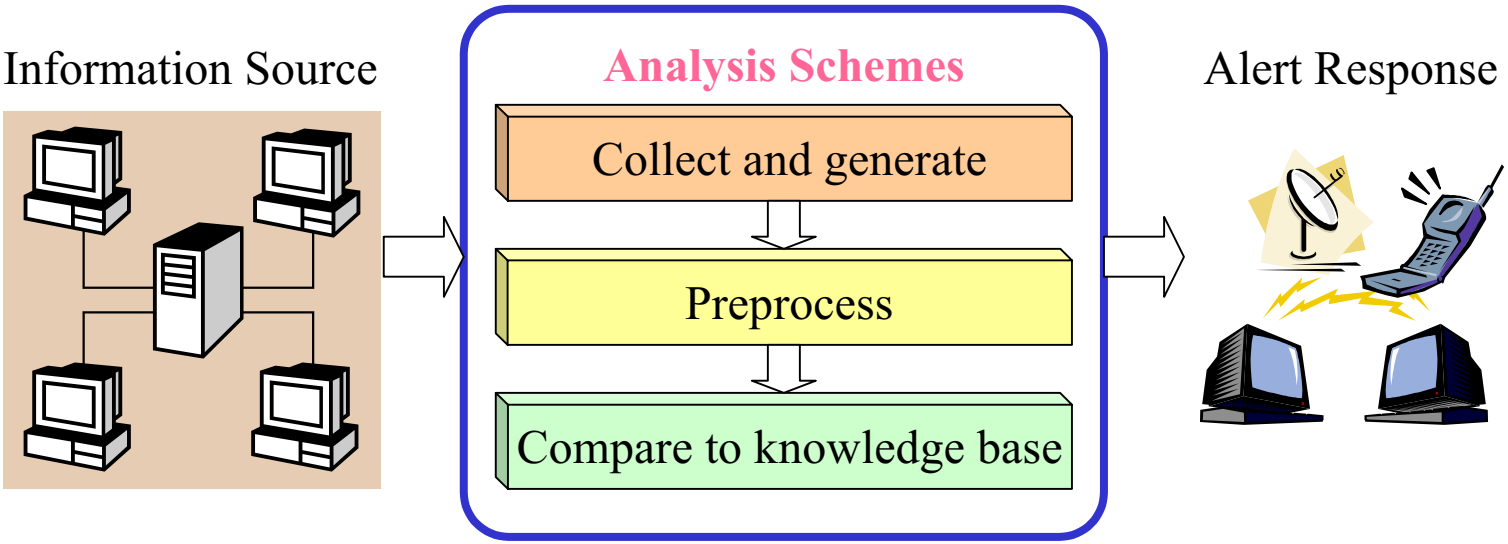
- Anomaly Detection
- Misuse Detection
- Burglar Alarms
- Honey Pots(Decoy or Fishbowl)
- Hybrids

Misuse vs. Anomaly Detection

- 오용탐지(misuse detection)
  - 알려진 공격이나 보안정책 위반하는 행위 패턴을 찾는다.
- 이상탐지(anomaly detection)
  - 비정상으로 보이는 행위 패턴을 찾는다.



정보 분석 스키마


Information Source
Analysis Schemes
Collect and generate
Preprocess
Compare to knowledge base
Alert Response

Collect and Generate

- 오용탐지
  - 침입에 대한 정보를 모은다.
  - 취약점, 공격, 위협, 특별한 공격 도구, 그리고 흥미 있는 관찰 시나리오.
- 이상탐지
  - 실제 돌아가는 시스템이나 비슷하게 설계된 시스템으로부터 이벤트 정보를 모은다.

Preprocess

- 이벤트 정보는 분석 엔진에서 사용할 수 있도록 다양한 변화를 거친다.
- 오용탐지
  - 이벤트 데이터는 항상 규정된 몇몇 형태로 변환된다.
- 이상탐지
  - 이벤트 데이터는 항상 행위 속성을 값이나 기호로 표현되는 행위 벡터로 축약한다.

Compare to Knowledge Base

- 오용탐지
  - 공격 특징과 이벤트 데이터의 패턴이 일치하면 경보를 발한다.
- 이상탐지
  - 사용자 행위가 기록된 정상행위 프로파일에 충분히 가까우면 공격의 징후가 없다고 판정한다.
- 대응
  - 대응 방법으로는 경고, 로그 기록, 자동화된 대응, 기타 다른 행위들이 있다.

Burglar alarm

- Goals:
  - based on site policy alert administrator to policy violations
  - detect events that may not be “security” events which may indicate a policy violation
- 정책을 위반하는 오용을 감시한다.
  - New routers, New subnets, New web servers 등
  - User id 추가, 로그파일 공격, setuid root 프로그램 생성 등.
- Burglar alarms are a big win for the network manager

Honey pots

- 공격자를 유혹하여 그에 대한 정보와 환경을 가져오는 시스템
- Goals:
  - make it look inviting
  - make it look weak and easy to crack
  - instrument every piece of the system
  - monitor all traffic going in or out
  - alert administrator whenever someone accesses the system

Hybrids

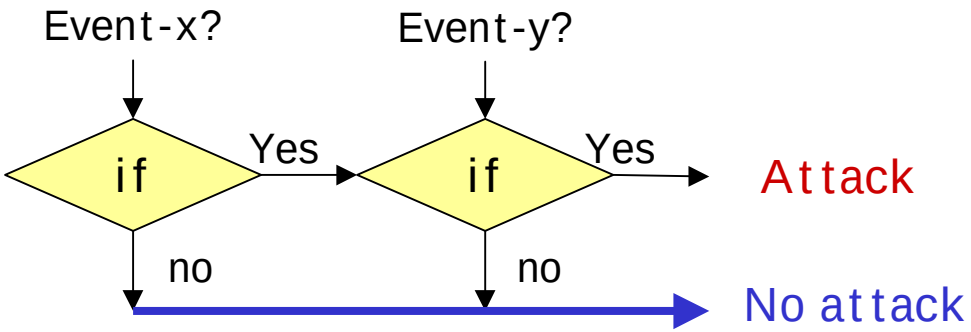
- The current crop of commercial IDS are mostly hybrids
  - 오용 탐지(특징이나 간단한 패턴)
  - 전문가 규칙(일반 공격의 네트워크 기반 추론)
  - 통계적 이상 탐지(threshold 설정)
  - 통계적 이상 탐지는 오용탐지 의 부족한 정보를 보충할 수 있다.
- 궁극적 hybrid IDS는 취약점 스캐너와 협력해야 한다.

Detection Techniques

- 오용탐지
- 이상탐지
- 다른 탐지 기술

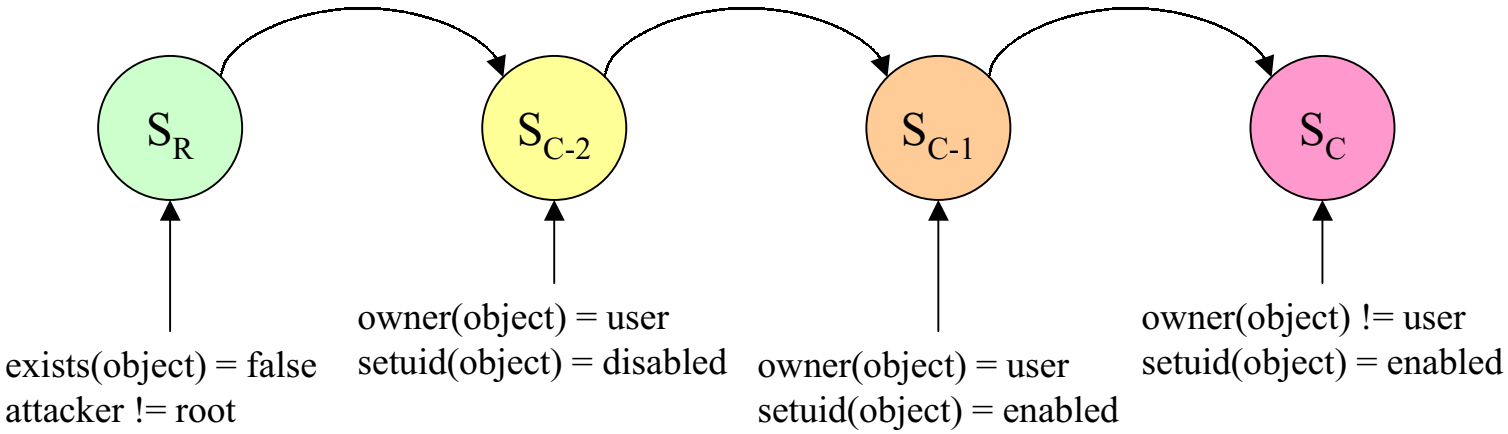
Misuse Detection
Production/Expert systems

- **if-then rules and then enter facts** 형태로 공격을 서술.
- 대량의 데이터를 다루기에는 부적합.
- 순서 데이터를 다루지 않는다.
- 전문 지식(규칙)은 사용자가 만든 것이다.
- 알려진 침입만 탐지할 수 있다.
- 불확실성을 다룰 수 없다.



Misuse Detection
State transition approaches

- 상태전이 방법은 시스템 상태와 상태 전이 표현을 사용하여 알려진 침입을 분류하고 탐지한다.
- 상태 전이 분석, Language/API-based Approaches, 그리고 Colored Petri Nets의 세 가지 주요 방법이 있다.
- 현재의 다른 침입탐지방법보다 빠르고 융통성이 있다.

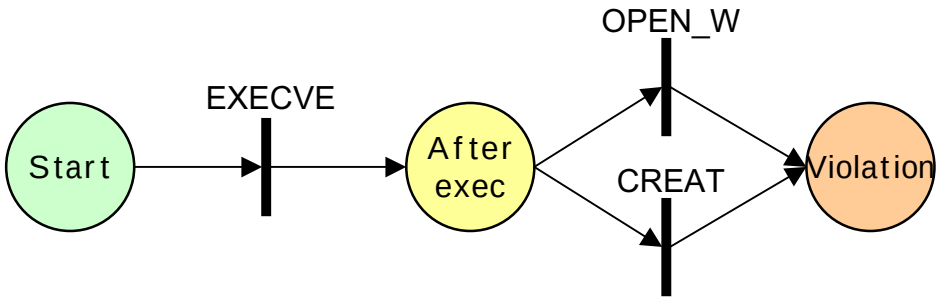


Misuse Detection
State transition approaches (1)

- **상태 전이 분석(State Transition Analysis)**
- 유한 상태 기계를 사용하여 침입을 그래프로 표현한다.
- 장점
  - 직관적이며, 고수준이며, 그리고 감사레코드 독립적.
  - 공격 시나리오를 구성하는데 특징 행위의 전체적인 순서로 표현.
  - 특징 행위의 가장 작은 서브셋을 사용.
  - 침입 시나리오를 표현하기 쉽다.
  - 협동 공격(Coordinated)이나 지연 공격(slow attack)을 탐지할 수 있다.
- 단점
  - 상태 정의 리스트와 특징 행위는 직접 작성해야 한다.
  - 상태 정의와 특징은 정교한 침입 시나리오를 표현할 수 있을 정도로 강력하지 못하다.
  - 어떠한 상태의 전개는 추론엔진에게 추가적인 정보가 필요하다. 시스템 성능을 떨어뜨리게 된다.

Misuse Detection
State transition approaches (2)

- **Colored Petri-Net**
- 상태 전이와 Petri-Net의 차이점
  - 상태 전이에서 침입의 결과가 시스템 상태로 표현될 때 효과적으로 침입을 탐지 한다.
  - 상태 전이에서는 특징은 상태(state)에 표시되지만, Petri-Net에서는 트랜지션(transition)에 연결된다.
- 각 침입 특징은 이벤트와 context 사이의 관계를 표현하는 패턴이다



Misuse Detection
State transition approaches (2)

- **Colored Petri-Net (continued)**
- 장점
  - 빠르다.
  - 감사 형식에 독립적인 패턴 매칭 엔진이다.
  - 특징은 audit trail에 포터블하다.
  - 패턴은 어떻게 매칭되는가가 아니라 매칭에 무엇이 필요하는가에 따른다.
  - 이벤트의 순서와 요소는 직접 표현된다.
  - 성공적인 패턴 매칭에 잘 정의된 스펙을 제공한다.
  - 사용자가 특징에 매칭하는 행위를 기술하도록 한다.

Misuse Detection
State transition approaches (3)

- **Language/API-based Approaches**
- 상업적인 오용탐지 도구를 최적화하는 일반 전략은 탐지 엔진을 사용하기 쉬운 형태로 기술하는 것이다.
- 몇몇 전문가 시스템 언어 (예를 들어, P-BEST and CLIPS) 가 있지만 다른 목적으로 설계되었다.
- 예)
  - ASAX의 RUSSLE 언어
  - Haystack의 STALKER 시스템
  - NFR(Network Flight Recorder)의 N code

Misuse Detection
일괄 분석을 위한 정보검색

- 감사 데이터 기록으로 작업하는 것은 흥미있는 행위 패턴의 증거를 찾거나 특정 객체나 사용자에게 영향을 주는 행위를 분리하는 능력을 제공한다.
- 새로운 공격을 발견하는 IDS와 공격 행위의 증거를 찾는 보안 관리자용 시스템의 기능을 갖는다.
- 이 방법은 사건 후에 감사 정보를 조사하는 단점이 있다.

Anomaly Detection
Denning's original model

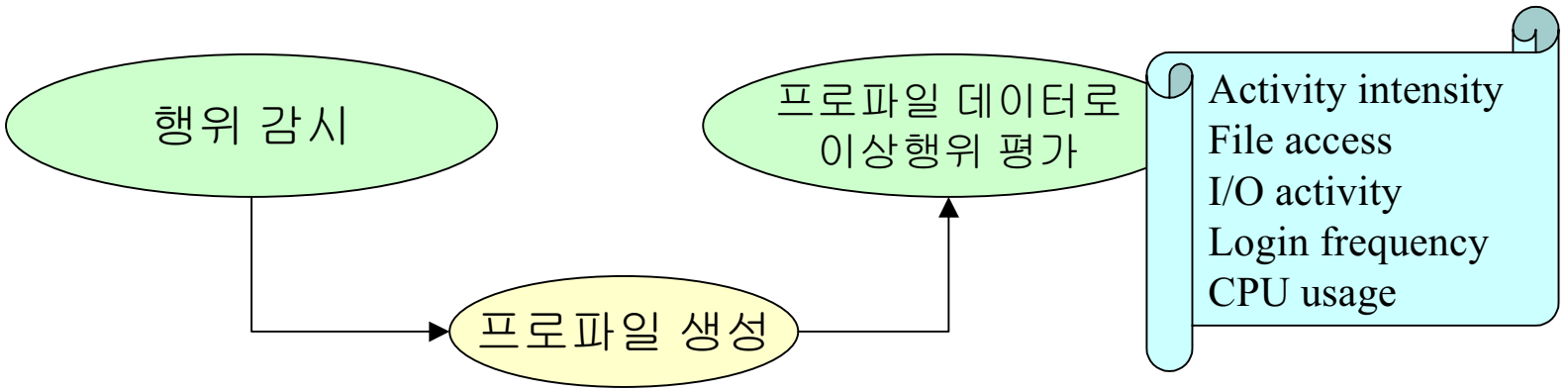
- ***Operational model***
  - 이벤트 횟수와 같은 척도를 적용한다.
- ***Mean and standard deviation model***
  - 시스템 행위 척도는 먼저 발생한 행위에서 계산된 평균과 표준 편차이다.
- ***Multivariate model***
  - 다른 척도와의 연관성
- ***Markov process model***
  - 감사 이벤트를 상태값으로 표현하고 상태 전이 행렬을 사용한다.

Anomaly Detection
정량 분석(quantitative analysis)

- 일반적인 이상 탐지 방법은 정량 분석이다.
- 임계치(threshold)를 사용한다.
  - Heuristic threshold detection
- 대상기반 무결성 검사
  - 설명 불가능한 시스템 객체에 대한 변화 검사
- 정량 분석과 데이터 축약
  - 대량의 이벤트 정보로부터 불필요한 정보를 제거한다.
  - 시스템 부하를 감소시키고 탐지 절차를 최적화한다.

Anomaly Detection
통계적 분석(statistical measures)

- 통계적 분석의 장점
  - 합법적인 사용자로 위장한 침입자를 분석한다.
  - 주기적인 변경이나 유지보수가 필요 없다.
- 통계적 분석의 단점
  - 자동화된 대응을 사용한 피해를 막을 수 없다.
  - 이벤트의 정확한 발생 순서는 제공되지 않는다.
  - 오판율이 높다.

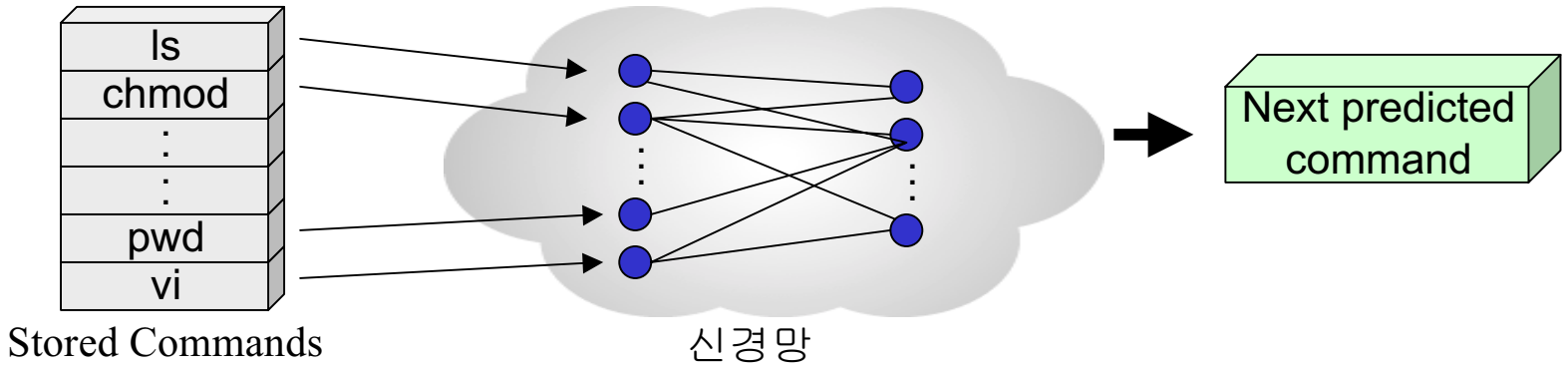


Anomaly Detection
규칙 기반 분석(rule-based approaches)

- 통계적 이상 탐지와 관련이 있다.
- Wisdom and Sense (W&S) - *Bayes' theorem*
  - 기록된 감사 데이터로부터 규칙을 유도한다.
  - 규칙은 시스템 주체와 객체의 과거 행위를 반영하고 트리 구조로 저장된다.
- TIM(Time-based Inductive Machine)
  - TIM은 이벤트 시퀀스에서 패턴을 찾는다.
  - Markov 전이 확률 모델로 구현되었다.
- HMM(Hidden Markov Model)
  - 일련의 시퀀스를 모델링하기위한 방법이다.
  - Hidden은 state가 입력 패턴에 관계없이 모델 내에 숨어 있다는 것을 의미한다.

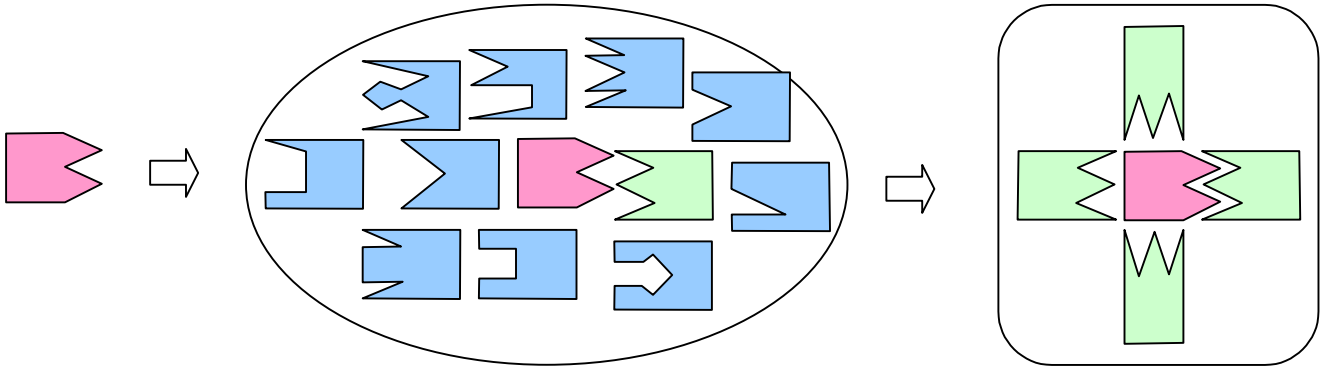
Anomaly Detection
신경망(neural networks)

- 비정상 행위를 특성화하는 적응적 학습 기술
- 신경망은 두 단계를 거친다.
  - 기록된 데이터로 학습하여 네트워크를 생성한다.
  - 이벤트 데이터를 네트워크에 적용한다.
- 단점
  - 왜 비정상인지를 설명할 수 없다.



Alternative Detection Schemes
면역 시스템 분석(immune system approaches)

- 어떻게 컴퓨터 시스템이 스스로 보호할 수단을 갖는가?
- 처음엔 이상 탐지 방법으로 제안되었으나 오용탐지에도 적용된다.
- 특성화된 정상 행위와 다른 점을 찾는다.
- 경쟁 상태(race conditions), 위장(masquerading), and 정책 위반(policy violations)을 탐지할 수 없다.

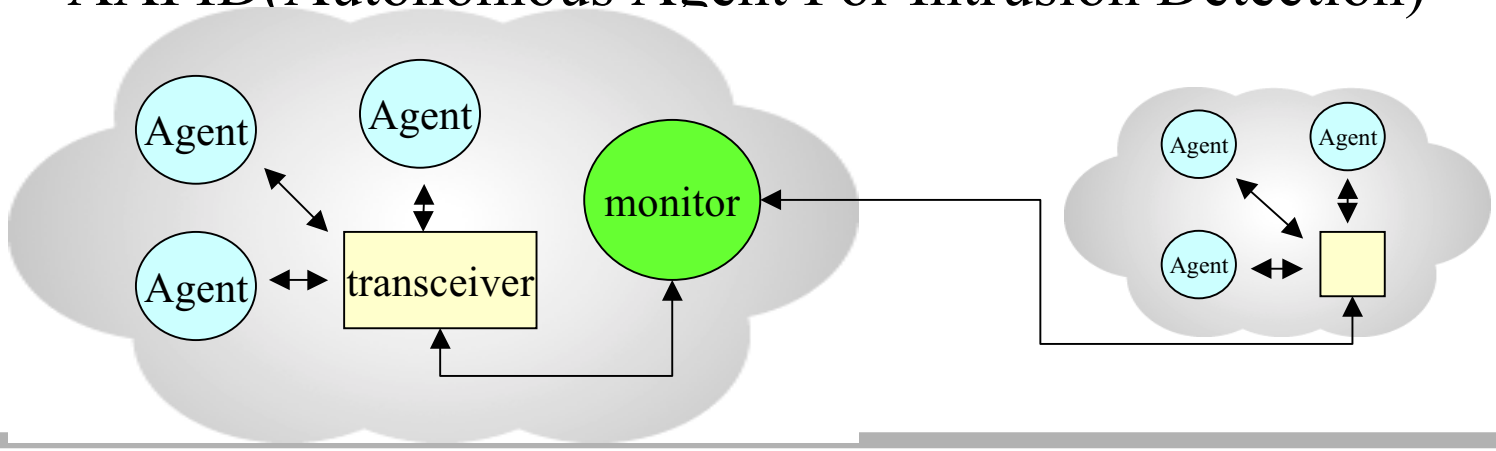


Alternative Detection Schemes
유전 알고리즘(genetic algorithms)

- 진화 알고리즘의 한 분류이다.
- GASSTA시스템에서 가설 벡터 집합을 사용하여 시스템 이벤트를 분류하는 문제에 적용하였다.
- 오용탐지에서의 단점
  - 이벤트 횟수에 관계된 계정 공격을 탐지할 수 없다.
  - 이진 표현 형태때문에 다중의 동시 공격을 탐지할 수 없다.
  - 최적의 가설 벡터를 찾을 수 없다.
  - 감사 증적에서 공격을 간단히 찾지 못한다.
  - 신경망 방법의 단점이 있다. (공격을 설명하지 못함)

Alternative Detection Schemes
에이전트 기반 탐지(agent-based detection)

- 호스트에서 보안 감시 기능을 수행하는 소프트웨어 기반이다.
- 유사한 구조의 다른 에이전트와 통신하고 협력할 뿐만 아니라 경험으로부터 학습하기위해 허용된 행위의 해석을 계속해서 수행한다.
- 오용탐지와 이상탐지 능력을 혼합한 형태이다.
- AAFID(Autonomous Agent For Intrusion Detection)



Alternative Detection Schemes
데이터 마이닝(data mining)

- 이 방법은 프로그램과 사용자 행위를 표현하는 시스템 특징의 유용한 패턴을 발견하는 것이다.
  - JAM (Java Agent for Meta-Learning over Distributed Database)
- 이용 분야
  - 클러스터링(clustering)
  - 분류(classification)
  - 연관성(association)
  - 순차 분석 (sequence analysis)

시스템 이벤트 데이터

UID	Time	System call
1 1	95/06/25 95/06/30	30 90
2 2 2	95/06/10 95/06/15 95/06/20	10,20 30 40,60,70
3	95/06/25	30,50,70
4 4 4	95/06/25 95/06/30 95/07/25	30 40,70 90
5	95/06/12	90

각 사용자 별 순차 규칙

UID	Sequence
1	<(30) (90)>
2	<(10,20) (30) (40,60,70)>
3	<(30,50,70)>
4	<(30) (40,70) (90)>
5	<(90)>

사용자들의 공통적 규칙
(최대 순차 패턴 지지율 > 25 %)

<(30) (90)>
<(30) (40,70)>

Response

- 대응(responses) 요구사항
  - 작동 환경
  - 시스템 목적과 특성
  - 규정이나 법적 요구사항
  - 사용자에게 전문지식 전달

Active responses

- 침입자에 대항한 행위
  - 침입자의 공격 소스를 역추적하고 침입자의 기계나 네트워크 연결을 사용 못하게 한다.
  - User-driven response, Automatic response
- 환경을 개선
  - Self-healing system
- 많은 정보를 수집
  - ‘Decoys’, ‘honey pots’, or ‘fishbowls’

Passive responses

- 경보(alarm)와 알림(notification)
  - 화면에 경고 메시지를 출력
  - 경고 메시지의 원격 통지

    (pagers, cellular telephones, email 메시지)
- SNMP traps과 plug-ins
  - 네트워크 관리 도구와 협력하는 기능

Technical Issues

- Scalability
- Management
- Reliability
- Analysis Issues
- Interoperability
- Integration
- User Interfaces

Scalability

  - How well a particular solution to a problem works when the size of the problem grows.
- Scaling over time
  - To recognize suspicious activity, the intrusion detection system must consider the event stream as a function of time.
- Scaling over space
  - How well it works when the network monitored increases from hundreds of hosts to thousands or even million of hosts.

Management

- Network Management
  - more tightly integrate intrusion detection functions with network management systems as network traffic and complexity levels grows
- Sensor control
  - The centralization of management control of intrusion detection sensors, agents, and analysis engines.
- Investigative support
  - tell that incidents occurred, isolate the intruder, and determine the means and the effect of the intrusion.
- Performance loads
  - load balancing and run-time tuning of IDS

Reliability

- Information sources
  - Encryption mechanisms represent special challenges for IDS. (SSL, VPN, switched network etc.)
  - host level or object level monitor
- Response mechanisms
  - A and B(strategic partners) both run intursion detection system with automated responses set to block sources of certain attacks. And the attacker knows this.
  - If response components are not reliable and robust in the face of attack...

Reliability (continued)

- Analysis engines
  - profile-based systems
  - signature-based systems
  - network-based systems
- Communications links
  - “man in the middle” attack

Analysis Issues

- Training sets for AI-based detectors
- False positive/negatives in anomaly detection
  - false positive : detection of non-attacks.
  - false negative : non-detection of attacks.
- Trends analysis
- Composition of policies

Interoperability

- CIDF/CRISIS effort
- Audit trail standards
  - Orange book
  - Denning's IDES audit format
  - IETF/IDWG

Integration and User Interfaces

- Integration
  - resolving problems in interaction between the components.
  - Integrating an intrusion detection system with an environment that uses multiple network protocols.
- User Interfaces
  - If the user interface is badly designed, so that users find it difficult to interact with the system, users will circumvent or sabotage the system.

IDS Features and Functions

- Monitoring approach
- Timing of information collection and analysis
- Location of analysis
- Types of analysis
- Responses to detection of misuse or attack
- Management functions and deployment issues

Monitoring Approach
Application-based

- Advantages
  - This approach allows targeting of finer-grained activities on the system.
- Disadvantages
  - Application-layer vulnerabilities can undermine the integrity of application-based monitoring and detection approaches.

Monitoring Approach
Host-based (1)

- Advantages
  - monitor information access in terms of “who accessed what”.
  - map problem activities to a specific user id.
  - track behavior changes associated with misuse.
  - operate in switched network environments.
  - distribute the load associated with monitoring across available hosts on large networks.

Monitoring Approach
Host-based (2)

- Disadvantages
  - Network activity is not visible to host-based detectors.
  - Running audit mechanisms can incur additional resource overhead.
  - When audit trails are user as data sources, they can take up significant storage.
  - Operating system vulnerabilities can undermine the integrity of host-based agents and analyzers.
  - Host-based agents must be more platform-specific, which adds to deployment costs.
  - Management and deployment costs associated with host-based systems are usually greater than in other approaches.

Monitoring Approach
Target-based

- Advantages
  - Integrity analysis may detect intrusions that other methodologies do not.
  - useful monitoring systems with modest processing or communications bandwidth.
  - effective for determining which files need to be replaced in order to recover a system.
- Disadvantages
  - Depending on the number of files, system objects and object attributes for which checksums are computed, this approach may still levy an appreciable processing load on low-end systems.
  - The approach is not well suited to real-time detection processes

Monitoring Approach
Network-based

- Advantages
  - The data come without any special requirements for auditing or logging mechanisms.
  - The insertion of a network-level agent does not affect existing data sources.
  - Network-level agents can monitor and detect network attacks. (e.g., SYN flood and packet storm attacks).
- Disadvantages
  - can't tell the outcome of commands executed on the host.
  - can't scan protocols or content if network traffic is encrypted.
  - more difficult on modern switched networks.
  - can't handle high-speed networks.

Monitoring Approach
Integrated-based

- Advantages
  - As agents at applications, host, and network levels are used, the system can target activity at any or all levels.
  - It is easier to see patterns of attacks over time and across the network space
- Disadvantages
  - There are no industry standards with regards to interoperability of intrusion detection components; therefore it is difficult or impossible to integrate components from different vendors.
  - Integrated systems are more difficult to manage and deploy.

Timing of information analysis
Batch or Interval Oriented

- Advantages
  - less processing load on systems than real-time analysis.
  - suited to organizations in which threat levels are low and system resources are limited.
  - be easier to submit system logs collected and processed in batch mode as evidence.
- Disadvantages
  - Users will seldom see incidents before they are complete.
  - There is virtually no possibility of actively countering incidents as they happen in an attempt to minimize damage.
  - The aggregation of information for batch-mode analysis consumes more disk storage on the analysis system.

Timing of information analysis
Real-time

- Advantages
  - Attacks may be detected quickly enough to allow system administrators to interrupt them.
  - System administrators may be able to perform incident handling more quickly.
  - System administrators may be able to collect information that allows more effective identification of intruders in cases that occur on systems where legal remedies are available,
- Disadvantages
  - consume more memory and processing resource
  - serious legal issues associated with automated responses
  - so many false alarms that a real attack goes unnoticed.

Location of analysis

- Host level
  - minimizing network load.
  - Not allowing the detection of broad scale attacks targeting a network of machines.
- Network level
  - offer the capability to detect attacks that involve more than one host on the network.
  - The network load associated with transferring raw host level information to the analysis engine can be crippling.
- The *optimal strategy* is one in which analysis is done at both host and network levels.

Types of analysis
Signature analysis

- Definition
  - Signatures are patterns corresponding to known attacks or misuses of systems.
  - Signature analysis is pattern matching of system settings and user activities against a database of known attacks.
- Advantage
  - allows sensors to collect a more tightly targeted set of system data, thereby reducing system overhead.
  - more efficient than statistical analysis due to the absence of floating point computations.

Types of analysis
Statistical analysis

- Statistical analysis finds deviations from normal patterns of behavior.
- Advantages
  - The system may detect heretofore unknown attacks.
  - Detect more complex attacks
- Disadvantages
  - It is relatively easy for an adversary to trick the detector into accepting attack activity as normal
  - The possibility of false alarms is much grater in statistical detectors.
  - Statistical detectors do not deal well with changes in user activities.

Types of analysis
Integrity analysis

- Integrity analysis focuses on whether some aspect of a file or object has been altered.
- Advantages
  - Any successful attack where files were altered, network packet grabbers were left behind, or rootkits were deployed will be detected regardless of where or not the attack was detected by signature of statistical analysis.
- Disadvantages
  - Because current implementations tend to work in batch mode, they are not conducive to real-time response

Responses to detection of misuse or attack

- Alter the environment
  - terminating the connections used by the attacker and reconfiguring network devices to block further access to the site from the same source address.
- Validation
  - The sensors and/or analysis engine are queried in order to determine whether they continue to work properly
- Real time notification
  - by email or pager messages sent instantaneously with information about the problem.

Management functions and deployment issues

- Configuration
  - A customer acquires an IDS is the installation and setup of the system.
- Audit subsystem management
  - Audit systems offer improve user interfaces to the operating system audit controls.
- Reporting
  - offer the capability to export report data to database for analysis.
- Control
  - control or configuration the IDS.
- Proof of validity
  - Vulnerability assessment products are often used as part of the validation process and they function in synergy with IDS.

IDS and Network component

- IDS and the WWW
- IDS and Firewalls
- IDS and VPN
- IDS and Switches
- IDS and High speed networks

IDS and the WWW

- IDS는 웹 사이트를 보호하는 중요 수단이다.
  - SSL 암호화 스트림에 좋은 방법이 아니다.
  - 웹 서버에는 Host-based IDS를 사용
  - 웹 서버에 대한 스캔을 확인하기 위해 Network-based IDS를 사용
- For critical / paranoid web sites consider:
  - 서버 자체에는 burglar alarm을 설치한다.
  - Secure OS를 설치한다.

IDS and Firewalls

- 방화벽(firewall)과 IDS는 결국 하나의 설비로 결합될 것이다.
  - 많은 방화벽은 잘못된 주소가 보이면 경고할 수 있다.
  - burglar alarm을 설치할 수 있다.

IDS and VPN

- VPN(Virtual Private Networks) encrypt traffic
  - Network-based IDS는 탐지할 수 없다.
  - 많은 VPN 패키지는 좋은 로깅을 제공한다.

IDS and Switches

- 네트워크는 점차 스위치 구조로 변경된다.
  - Network-based IDS는 스위치를 통한 모든 트래픽을 얻기가 어렵다.
  - 해결책은 아직 없다.
    - 현재까지 가장 좋은 방법은 중요 시스템 앞에 허브를 연결하는 것이다.

IDS and High speed networks

- Network-based IDS는 고속 네트워크에서는 적절하지 못하다.
  - Many silently drop packets at over 30mb/s
  - Tcpdump on many systems does too(!)
  - Only way to tell is hardware packet counts versus what IDS claims to see
- IDS를 설치할 때는 성능을 조사해야 한다.

Forensics

- 범죄가 발생 중이거나 후에 증거를 수집하는 방법이다.
  - Reconstructing the criminal's actions
  - Providing evidence for prosecution
- 컴퓨터 네트워크의 forensics는 매우 어려우며 정보의 품질에 달려 있다.

Forensics
Tools

- Tcpdump
- Argus
- NFR
- Tcpwrapper
- Sniffers
- Nnstat
- A line printer
- Tripwire
- Backups

Forensics
Response

- 두 팀으로 나누어 수행한다.
  - A팀은 공격자가 어떤 행동을 하는지 B에게 알려 준다.
  - B팀은 공격자를 막기위한 따돌리기 계획(shutout plan)을 만든다.
  - 팀 A가 중단하고 계획을 수행할 때를 기다린다.

Forensics
복구 방법

- 로그 파일 검사
- 스니퍼 찾기
- 원격제어 프로그램 (backorifice 등) 찾기
- 공유 해커 파일(eggdrop, irc 등) 찾기
- 프로그램 권한(setuid 설정) 찾기
- 파일시스템 변경 (tripwire나 backup으로) 찾기
- cron이나 at 작업 검사
- 불법 서비스(netstat, inetd.conf 확인) 찾기
- 패스워드 파일 변경이나 새로운 user id 찾기
- 시스템과 네트워크 환경 검사
- 이상한 파일 검사
- 호스트(서버) 검사 등 수행

Forensics
Backtracking

- 접근 경로를 숨기는 등 해커들은 점차 정교해지고 있다.
- 해커 흔적을 찾는 방법은 복구 방법을 수행한다.
  - 숨겨진 디렉토리 찾기 (warez)
  - 새로 갱신된 파일 찾기
  - tripwire 사용하기
  - 백업파일 시스템과 비교
  - 해킹 도구 이름으로 찾기

Conclusion

- *Computer security is one of the most important technological issues of this area.*
- Capabilities
  - detection based on descriptions of event semantics
  - integration of intrusion detection functions
- Highly distributed architectures
- 911 for security management
- Silicon Guards