IDS 구성 및 운영

2002. 11. 27

이 강 석
ksalice@kisa.or.kr

한국정보보호진흥원/평가2팀

목 차

침입탐지시스템(IDS)의 이해

* 침입(Intrusion) 정의
* IDS의 정의
* IDS의 필요성
* IDS의 구조

침입(Intrusion) 이란 ?

* 컴퓨터/네트워크 자원의
  * 비밀성(confidentiality)
  * 무결성(integrity)
  * 가용성(availability)을 손상시키려는 시도

By NSA Glossary of Terms Used in Security and Intrusion Detection

침입(Intrusion) 이란 ?(계속)

* 일반적인 정의
  * 자산
    * 각종 서비스를 제공하는 서버
    * 개인용 컴퓨터
    * 네트워크 자원 등
  * 공격 행위
    * 사용 무력화
    * 데이터 파괴
    * 정보유출 등

침입(Intrusion) 이란?(계속)

- 침입발생
  - 외부자의 악의적인 공격
  - 내부자의 악의적인 공격, 권한의 오·남용(실수 포함)
  - 예제
    - 분산서비스거부공격(DDoS)
    - Buffer Overflow, 웜(Worm)...
    - 내부자의 자료유출

침입 탐지(Intrusion Detection)란?

* 컴퓨터 또는 네트워크로 들어오는 침입을 탐지하는 기술
  * 사용자 행위, 보안로그, 또는 감사 데이터에 근거
* 수동 또는 소프트웨어를 통한 침입시도나, 침입한 행위에 대한 탐지

By NSA Glossary of Terms Used in Security and Intrusion Detection

IDS의 정의

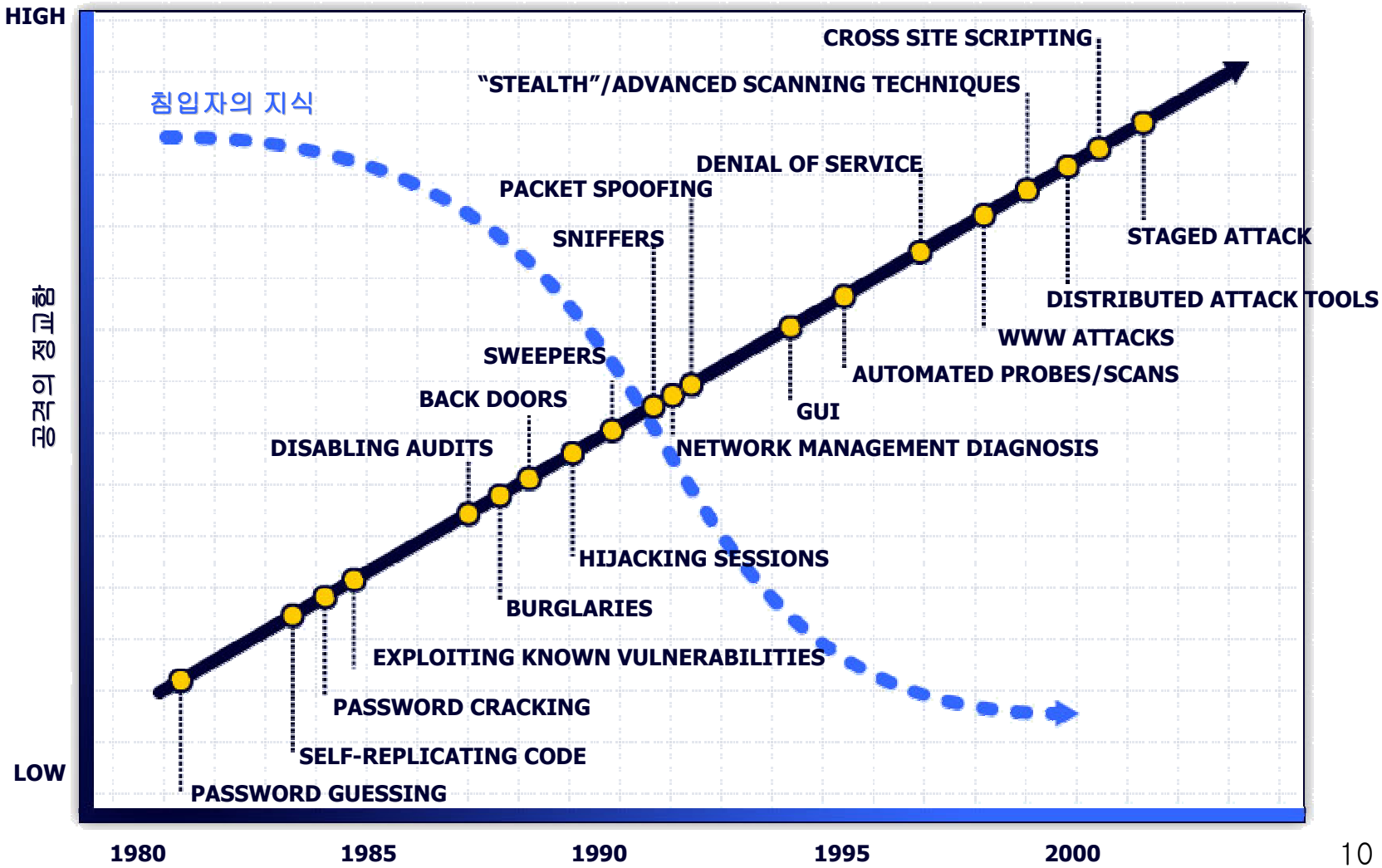
* 외부 침입자가 시스템의 자원을 정당한 권한 없이 불법적으로 사용하는 시도 또는, 내부 사용자가 자신의 권한을 오용, 남용하는 침입시도를 탐지하고 대응하는 것을 목적으로 하는 소프트웨어나 하드웨어

By NSA Glossary of Terms Used in Security and Intrusion Detection

IDS의 필요성

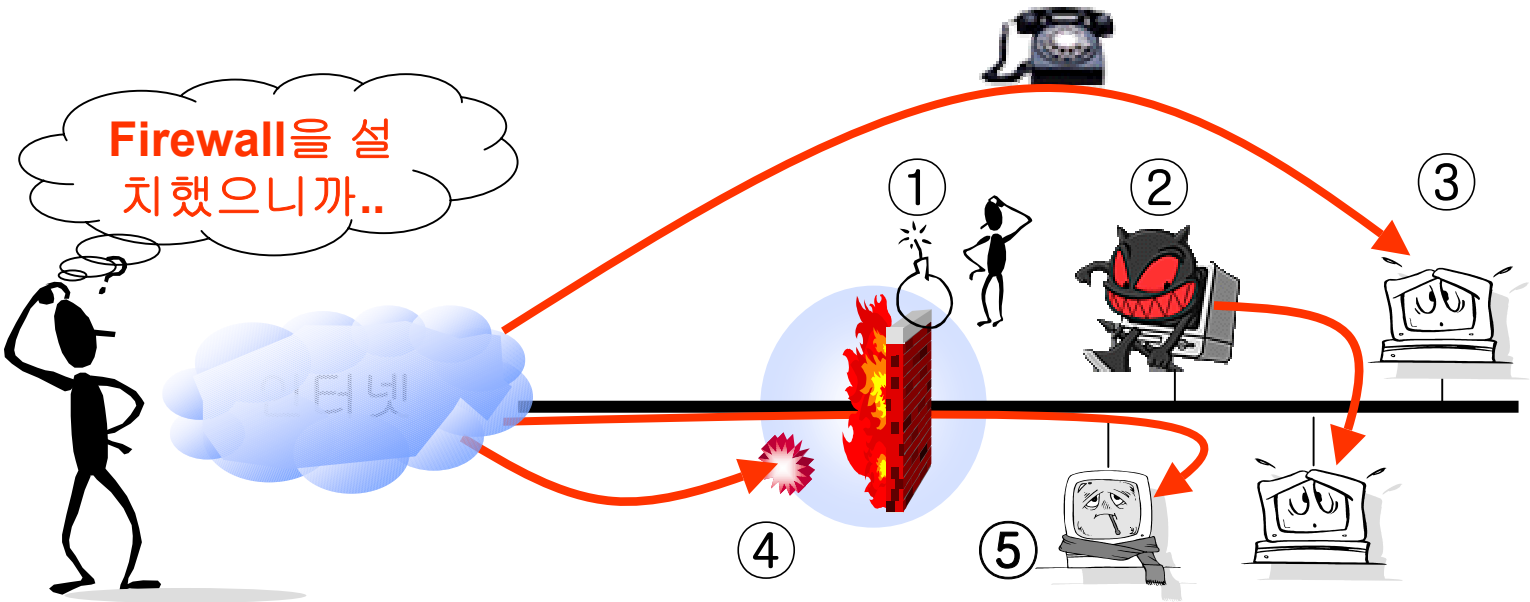
- 자산의 IT 의존도 심화
- 정보자산에 대한 침입 가능성 및 피해 증가
- 침입차단시스템의 한계 극복을 위한 대처수단
  - 상호 보완 시스템 구축
- 개별적/대규모 시스템 보안관리의 어려움
- 시스템/네트워크 침입에 대한 즉각적인 탐지 및 대처 수단의 필요성

S/W 복잡도에 따른 침입기술의 발전

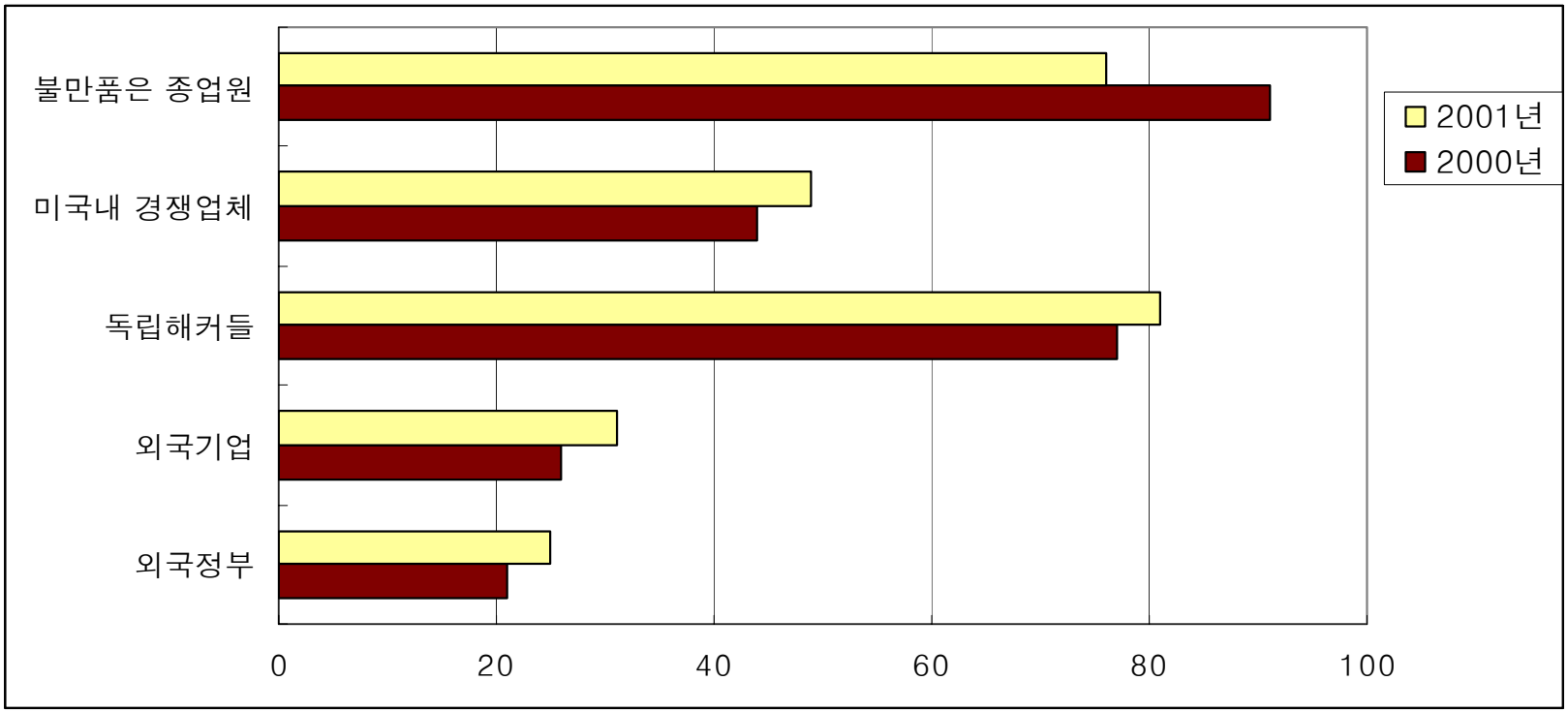


침입차단시스템의 한계

① 관리자의 실수로 인한 Firewall의 관리 상의 문제점
② 내부자에 의한 위협이 가장 위험함(전체 침입의 약 70%)
③ 모든 트래픽이 Firewall을 통과하지 않음(우회 공격)
  * 터미널 서버/Dial-up 서버(모뎀)
④ Firewall 자체에 대한 공격
  Firewall을 공격하는 50가지 방법(http://all.net/journal/50/firewall.html)
⑤ 내부 서버의 취약성으로 인한 공격



내부자의 네트워크 불법 사용 증대



CSI/FBI Computer Crime and Security Survey(2001)

개별적/대규모 보안 관리 방식의 문제점

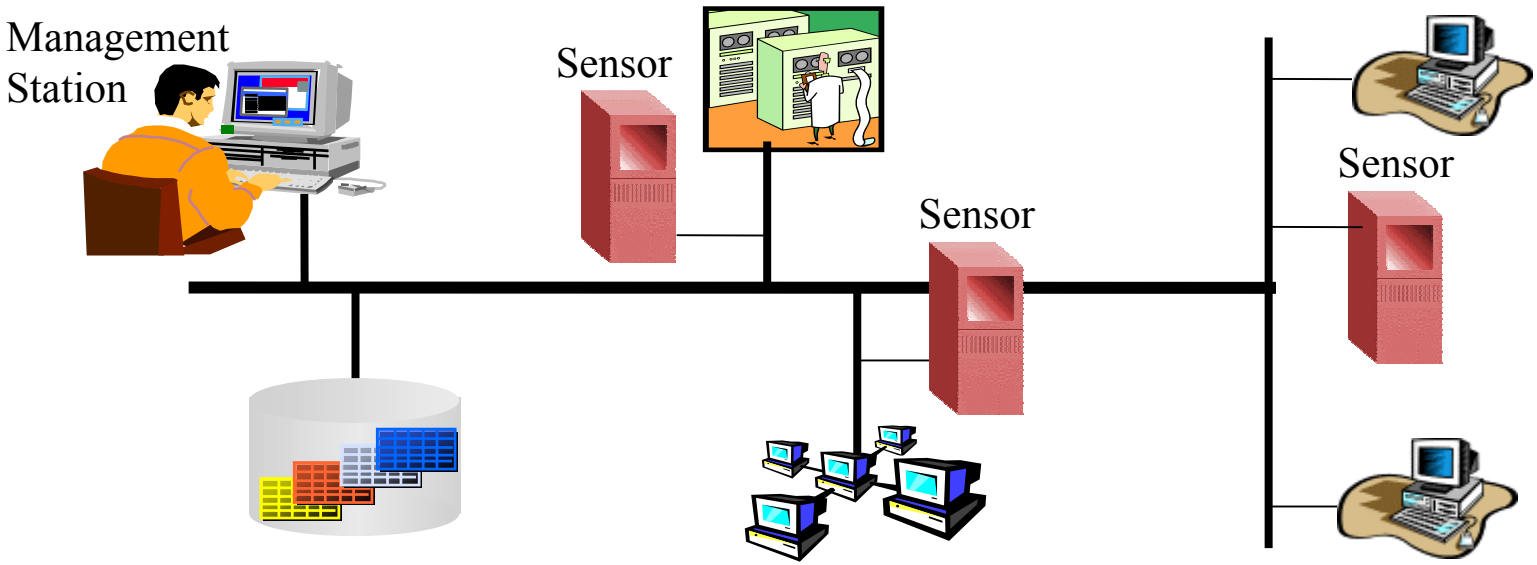
- 관리자의 교육 수준 및 기회 부족
  - 충분하지 않은 관리자 교육 기회 및 투자 비용
- 관리자 및 관리 시간부족
  - 늘어나는 호스트에 비해 관리자의 수 부족
  - 관리자 업무 과중
- 주기적인 시스템 패치 문제
- 새로운 시스템 취약성 발견 및 취약점 잔재

IDS의 효과

- 안전하고 효율적인 보안관리
  - 자동화된 실시간 침입 탐지 및 대응
    - 외부 및 내부 사용자에 의한 보안침해 사고 위협에 대처
    - 비전문가도 효율적인 운용 가능
    - 관리자 부재 시에도 효과적인 대응 가능
  - 침입에 대한 유용한 정보 제공
    - 침해사고 대응 절차 등
  - 공격자에 대한 침입관련 자료 생성
    - Forensics(증거를 수집하는 방법)
- 보안시스템 초기투자 비용감소
- 전문 보안인력 확보의 어려움 극복
- 기술 변화에 따른 위험 부담 감소

일반적인 구조

* 침입탐지
  * 센서, 에이전트, 탐지엔진
* 보안관리
  * 관리콘솔, 매니저

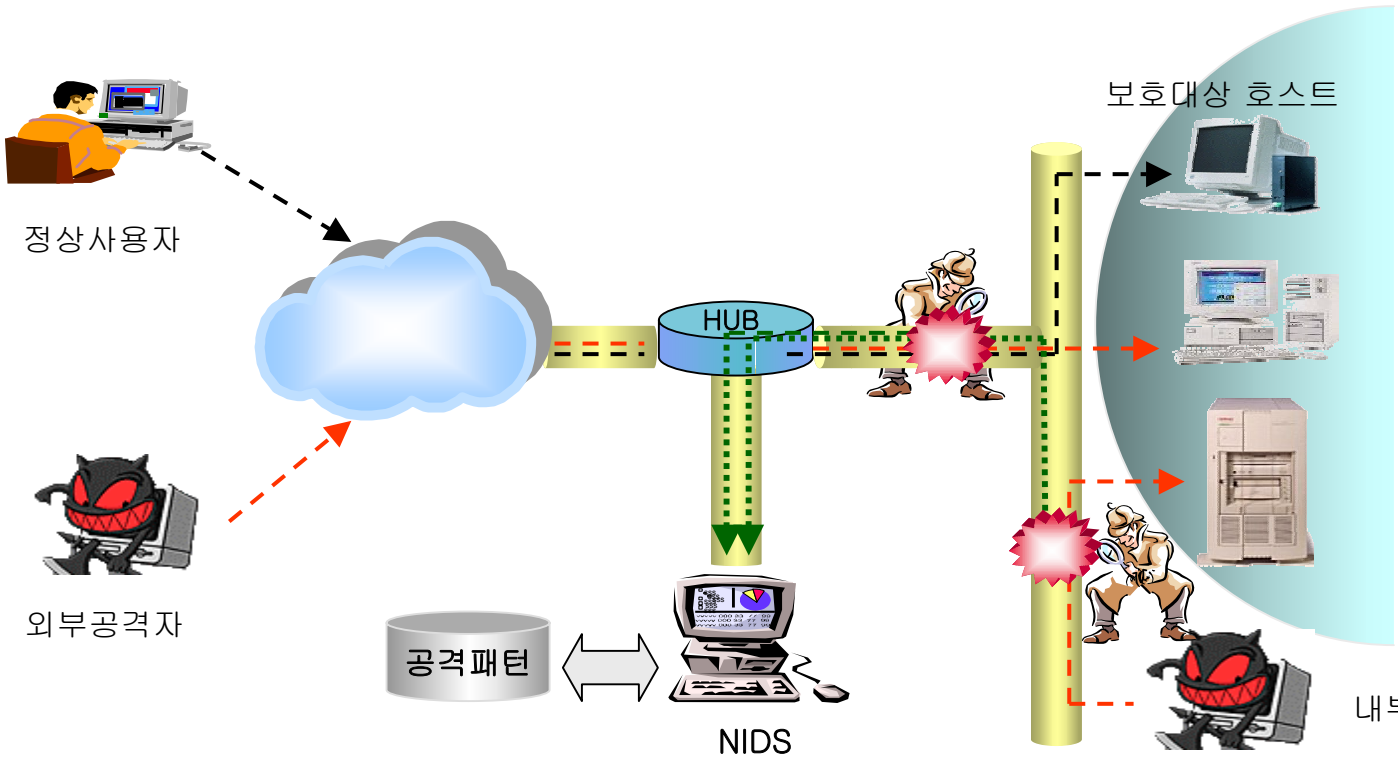


IDS 분류

- 데이터 소스 기준
  - 네트워크 기반
  - 호스트 기반
  - 하이브리드
- 침입탐지 방법 기준
  - 오용 탐지
  - 비정상행위 탐지
- 대응행동 기준
  - 수동적 대응
  - 능동적 대응

네트워크 기반 IDS

* 데이터 소스
  * 네트워크 패킷
  * NIC의 Promiscuous mode 이용 패킷 수집

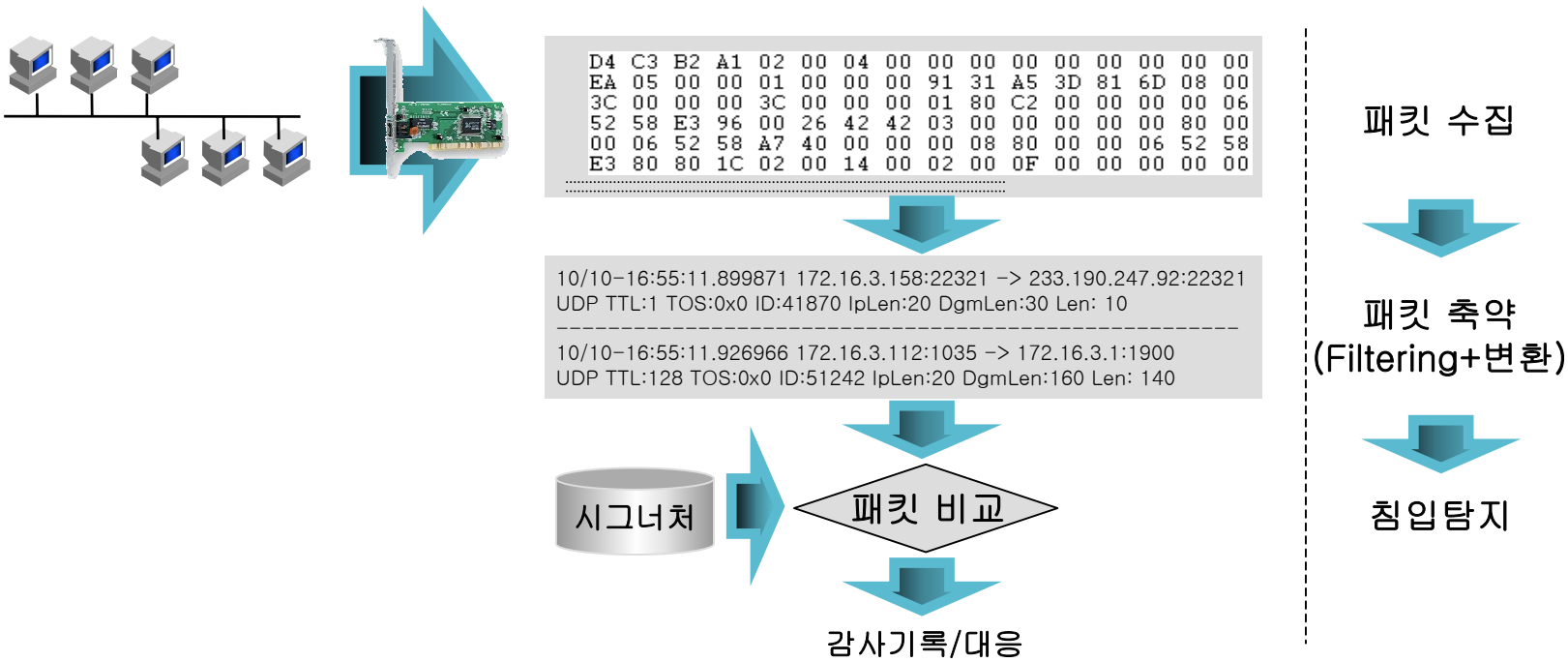


네트워크 기반 IDS(계속)

- 장점
  - 호스트 기반 IDS 에서는 탐지 불가능한 침입 탐지 가능
    - 포트 스캐닝, Land 공격
  - 전체 네트워크에 대한 침입 탐지 가능
  - 기존 네트워크 환경의 변경 필요 없음
- 단점
  - 탐지된 침입의 실제 공격 성공 여부를 알지 못함
  - 고부하(High-volume)/스위치(Switch) 네트워크에 적용문제
  - 다양한 우회 가능성 존재
- 제품
  - 국내
    - Siren 3.0, NeoWatcher@ESM Package V3.0, Netspecter V1.2, TESS/TSN V2.0, Sniper v2.0 등
  - 국외
    - BlackIce(ISS), Cisco Secure IDS, IntruShield, Snort 등

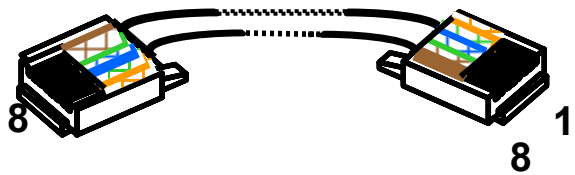
네트워크 기반 IDS(계속)

* 침입 탐지
  * NIC의 Promiscuous mode이용



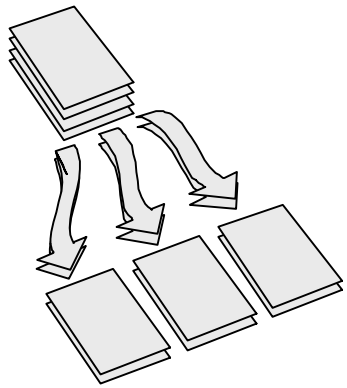
패킷 수집 방법

- Statefull
  - 세션이 연결된 패킷만 수집
    - TCP 세션 : 3 Way Hand Shake
  - False Positive 발생 확률 낮음
  - 메모리 오버헤드
    - 세션이 종료될 때까지 세션 저장
    - Stateless에 비해 많음
- Stateless
  - 보호 네트워크의 모든 패킷 수집
  - False Positive 발생 확률이 높음
    - IP Spoofing
  - 메모리 오버헤드
    - Statefull에 비해 적음



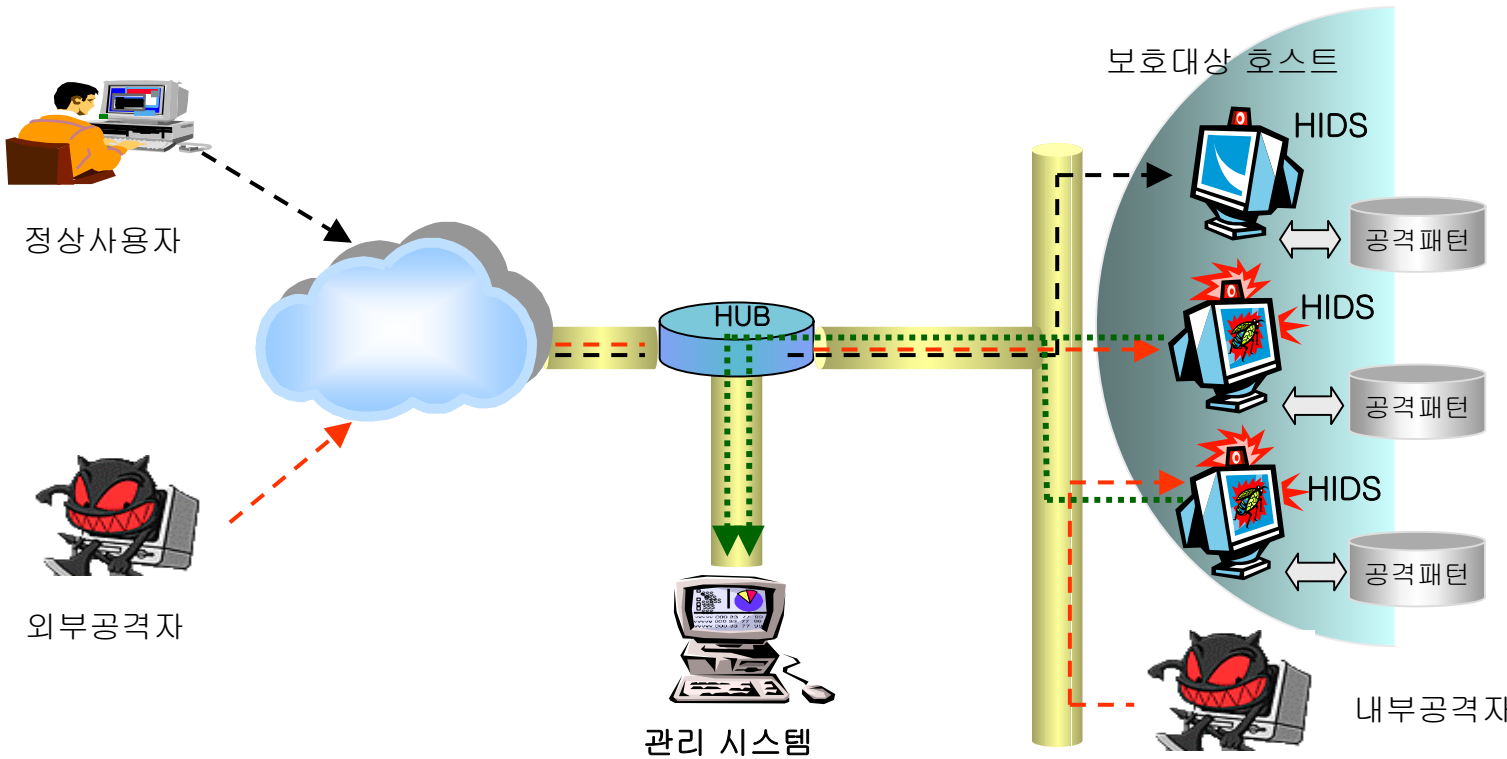
네트워크 기반 IDS(계속)

- 침입탐지의 효율성
  - 환경적 고려사항
    - 고속 환경에 맞는 NIC 사용
    - 네트워크 트래픽의 로드 밸런싱
      - 스위칭 허브 또는 분산 네트워크
  - 침입탐지시스템 자체 성능향상
    - 투자대비 적절한 시스템 환경 지원
      - 메모리, CPU 성능
    - 패킷 수집 및 탐지 방법, 모델 개선
    - 빠른 패턴비교 알고리즘 사용/개발
      - Snort : 개선된 Boyer-Moore 알고리즘
    - 네트워크에 맞는 시그너처 튜닝
      - False Positive, 시그너처 패치



호스트 기반 IDS

- 데이터 소스
  - OS 감사자료(audit trail)
    - 시스템 사용자 활동
    - 응용프로그램 로그

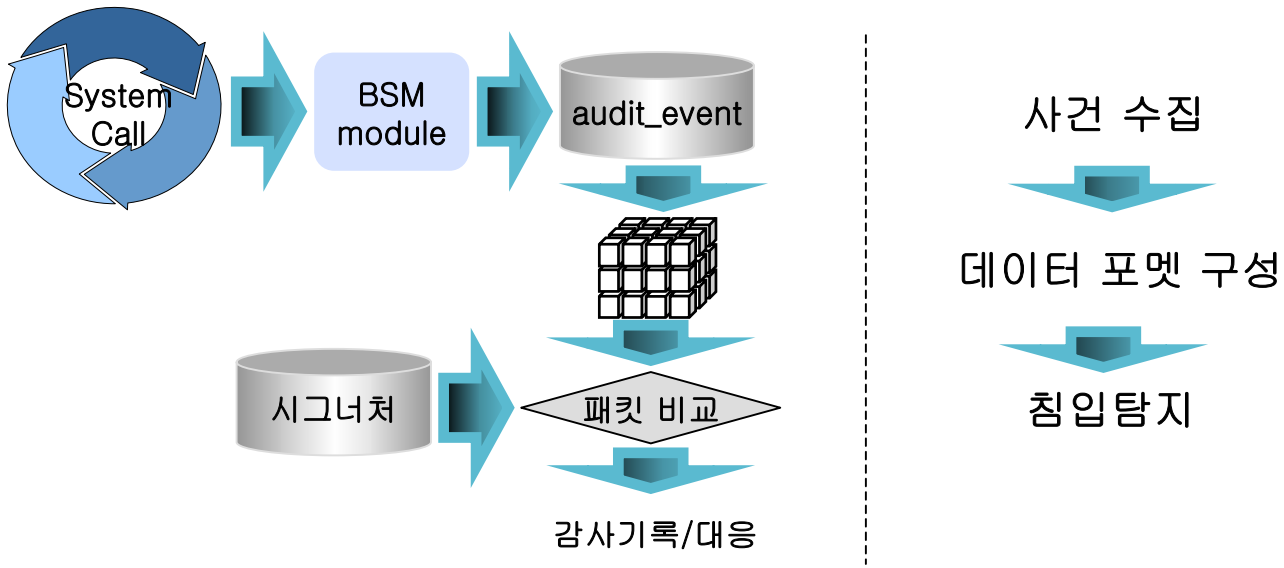


호스트 기반 IDS(계속)

* 장점
  * 네트워크 기반 IDS 에서는 탐지 불가능한 침입 탐지 가능
    * 트로이 목마, Race condition 등
  * 고부하/스위치 네트워크에도 적용 가능
* 단점
  * 모든 개별 호스트에 대한 설치/관리가 어려움
  * IDS가 설치된 플랫폼의 성능 저하
  * IDS가 설치된 플랫폼 자체가 침입에 노출됨
* 제품
  * 국내
    * Siren 3.0, NeoGuard@ESM Package V3.0, SafezoneHost V1.0
  * 국외
    * Appshield, auditGUARD, Centrax, Dragon Squire, NFR HID 등

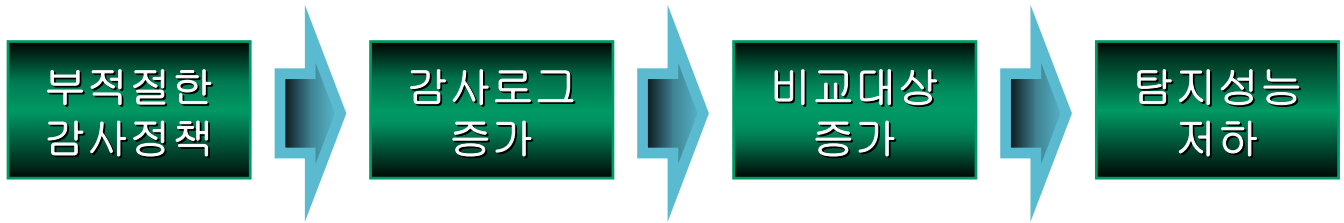
호스트 기반 IDS(계속)

- 침입 탐지
  - Solaris
    - BSM(Basic Security Module)
    - 시스템에서 발생하는 모든 사건 감사
  - Windows 계열
    - 감사 이벤트 로그



호스트 기반 IDS(계속)

* 침입탐지의 효율성
  * 시스템 감사로 processing 오버헤드
    * Solaris 인 경우, 5-10%의 오버헤드 발생
  * 적절한 시스템 감사정책 수립



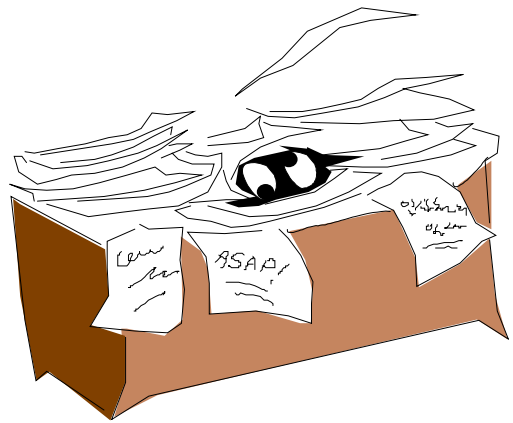
  * 침입탐지시스템 자체 성능향상
    * 투자대비 적절한 시스템 환경 개선(Upgrade)
      * 메모리, CPU 성능
    * 빠른 패턴비교 알고리즘 사용/개발
    * 호스트 시스템에 맞는 시그너처 튜닝
      * False Positive, 시그너처 패치

하이브리드 기반 IDS

- 데이터 소스
  - 네트워크 패킷, 시스템/응용프로그램 감사로그
  - No Promiscuous mode
  - Network Node IDS + HIDS
- 장점
  - 네트워크 기반 IDS와 호스트 기반 IDS의 장점 수용
- 단점
  - 모든 네트워크에 설치 어려움
  - IDS가 설치된 플랫폼의 성능 저하
- 제품
  - 국내
    - Siren 3.0
  - 국외
    - NFR HID, Prelude, RealSecure Server Sensor, Stormwatch

탐지방법에 의한 분류

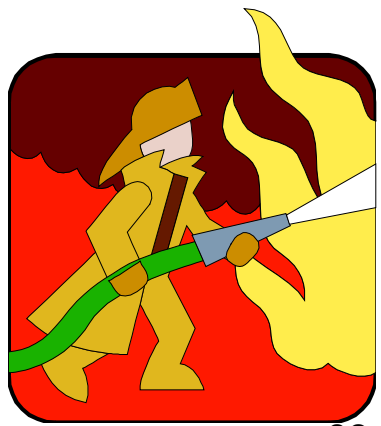
- 오용 탐지(misuse)
  - 침입 시그너쳐(signature) 이용
    - 특정 침입을 나타내는 특징
  - 새로운 침입유형 탐지 불가능
    - 지속적인 침입규칙 업데이트 필요
- 비정상행위 탐지(anomaly)
  - 통계적 기반 등 정상(normal)에서 벗어남(abnormal)을 탐지
  - 탐지방법에 대한 연구가 진행중



대응방법에 의한 분류

* 수동적 대응행동(passive response)
  * IDS는 관리자에게는 침입 정보만 제공
  * 실제 대응행동은 제공된 정보를 기초로 관리자가 수행
  * 종류 : 알림 및 경보 등
  * 예 : E-mail, SMS

* 능동적 대응행동(active response)
  * 실제 대응행동을 IDS가 자동적으로 수행
  * 종류 : 환경 변경, 침입자에 대한 역공격 등
  * 예 : F/W 연동, 세션차단(TCP)

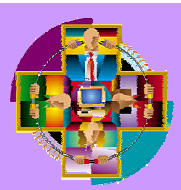


IDS 동향

* 정보보호제품의 변화
* IDS 시장동향
* IDS 세계시장 점유율
* 표준화 동향

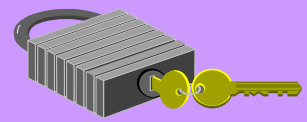
정보호호제품의 변화

제1세대: 침입 방지

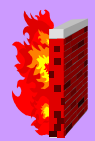

Trust Computing Base

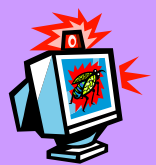

Access Control
&Physical Security

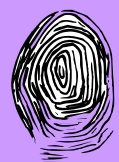
Multiple Levels
of Security


Cryptography

제2세대: 프로그램


Firewall


IDS


Biometric


VPN

PKI

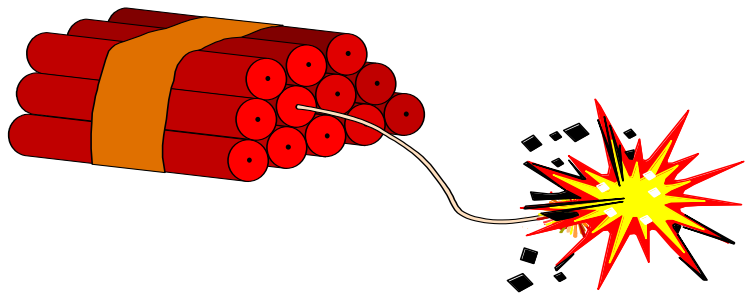
제2세대 + : 통합 시스템

Firewall + IDS + Biometric + VPN + PKI + ...

제3세대: ?

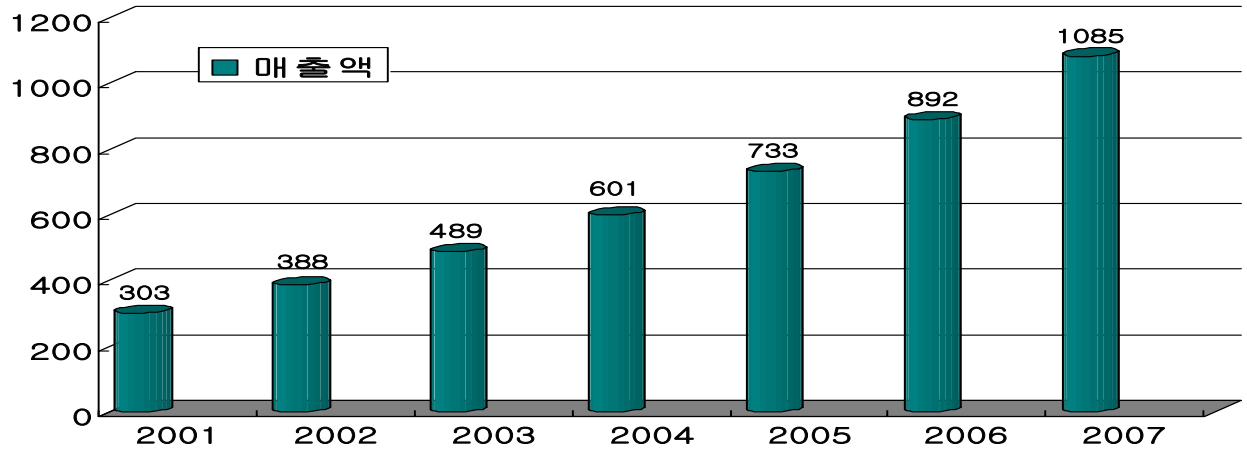
IDS 시장동향

- 급팽창하는 시장
  - Cisco, ISS, NAI, Axent, NetworkICE...
  - 시장 예상(자료 : IDC 2000)
    - 2003년까지 매년 39%의 고속 성장 예상
    - 2003년 : 9억 7천 8백만 달러



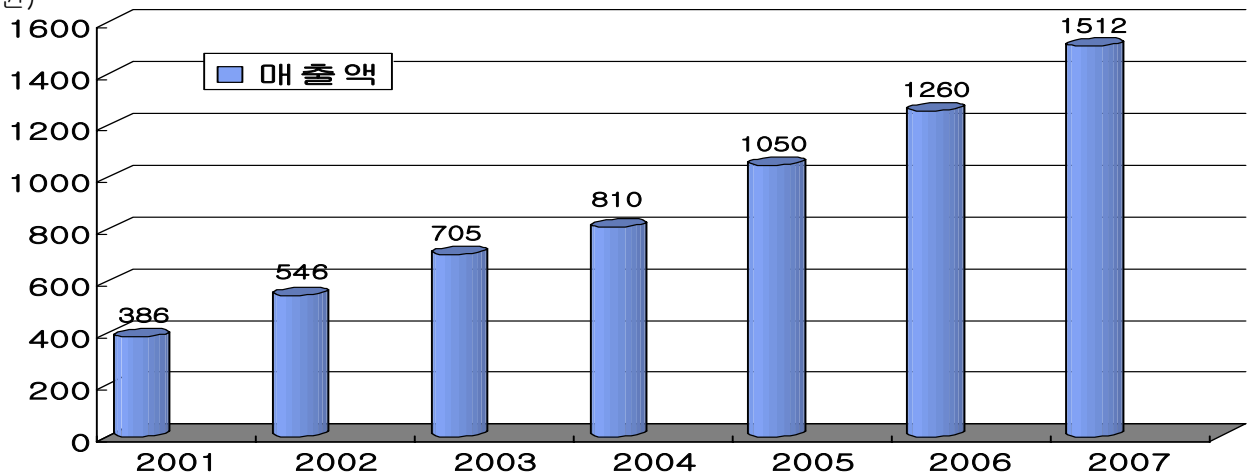
IDS 시장 동향(계속)

(단위:백만달러)



세계 시장

(단위:억원)

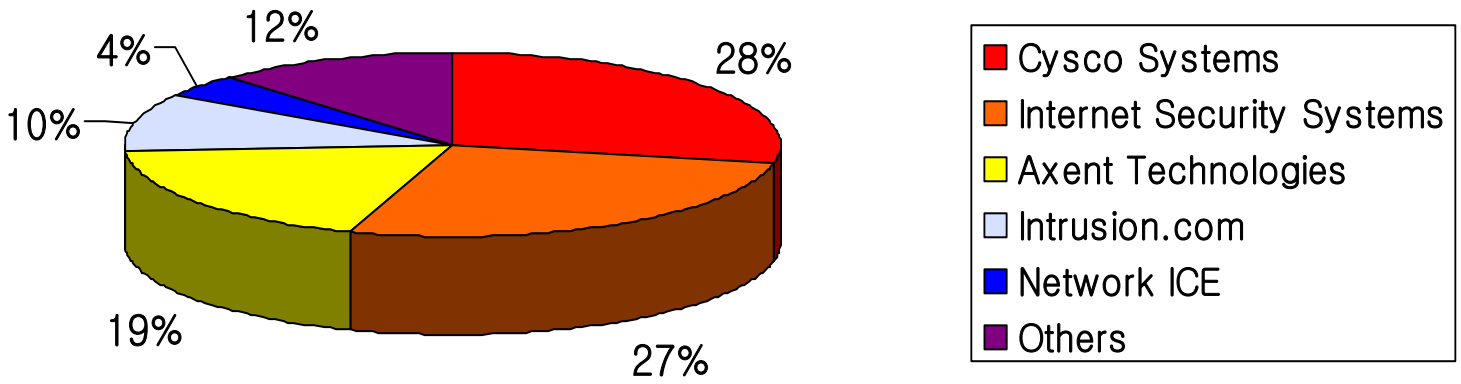


국내 시장

<자료>: ETRI 정보화기술연구소, 2002 정보보호산업실태조사 한국정보보호산업협회, 2002.8

IDS 시장동향(계속)

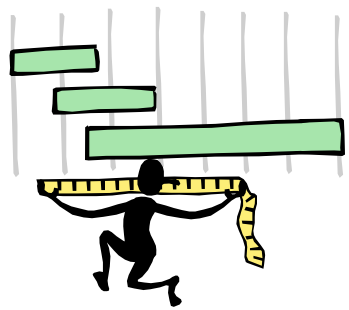
* IDS 세계시장 점유율



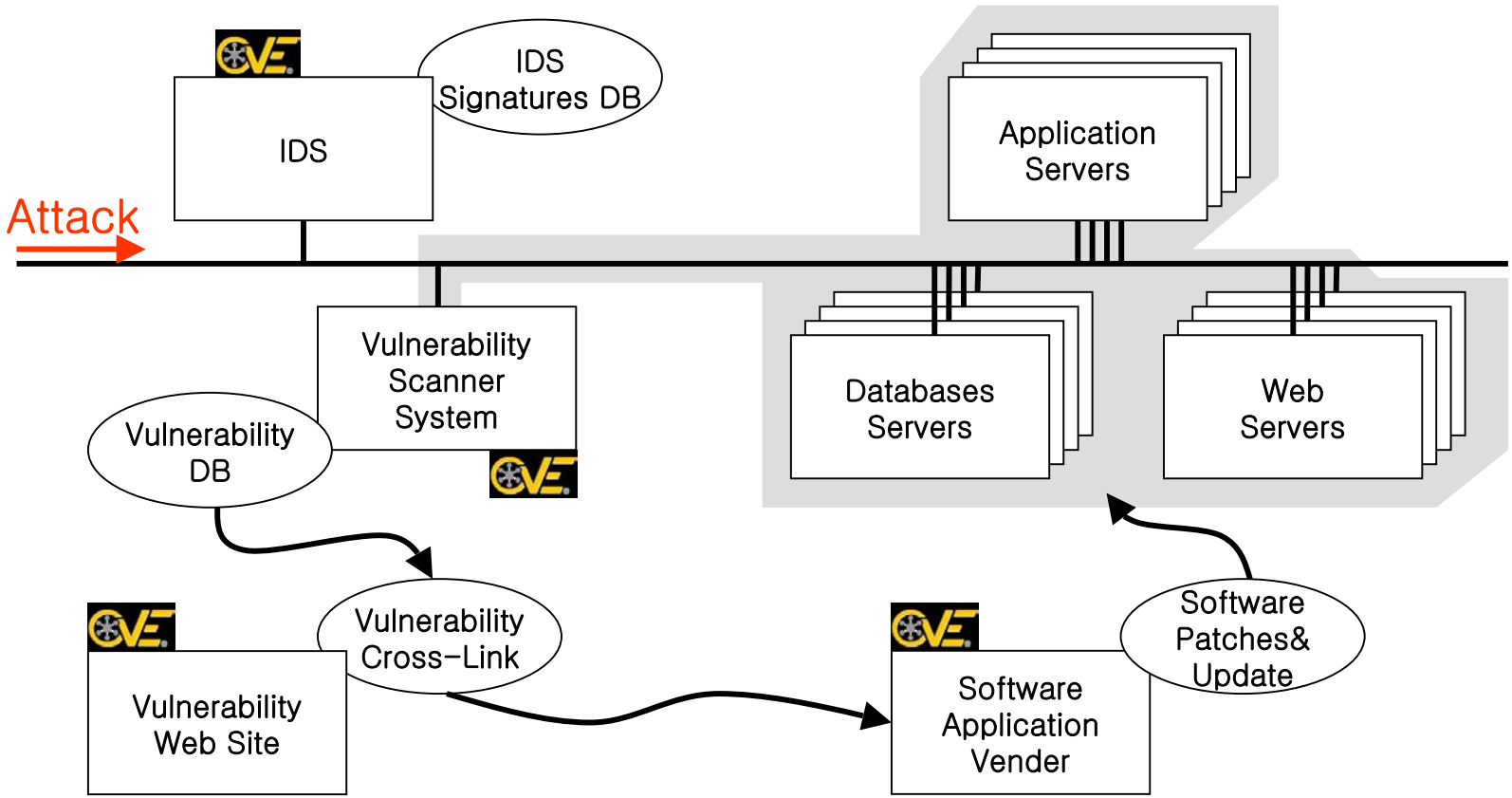
Greg Shipley,"Watching the Watchers: Intrusion Detection ", November 13 2000

표준화 동향

- 취약성 목록에 대한 표준화
  - CVE(Common Vulnerabilities and Exposures)
    - http://www.cve.mitre.org/
  - CERTCC(Computer Emergency Response Team Coordination Center)
    - http://www.cert.org/
  - BUGTRAG(Securityfocus)
    - http://www.securityfocus.com/
- IDWG(Intrusion Detection Working Group)
  - IETF에서 IDS 관련 표준화 작업
    - http://www.ietf.org/

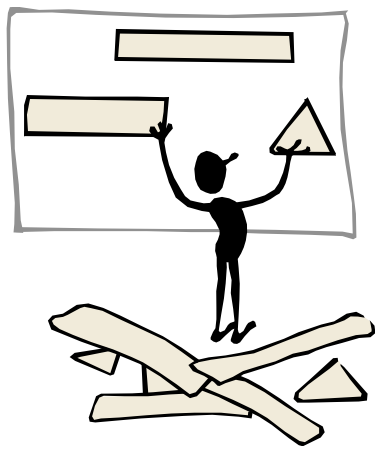


DVE-enabled Process



IDS 설치시 문제점

* 개인정보(privacy) 침해 가능성
* 고부하(high-volume) 네트워크 문제
* 스위치(switch) 네트워크 문제
* 과다한 대응행동 설정 문제
* 암호화 패킷 분석 문제



개인정보 침해 가능성

- 개인정보 침해 가능성
  - 침입탐지를 위해 사용자 활동 모니터
    - 외부 공격자/내부 사용자에 한 모니터링
    - Web 접속, E-mail 송신/발송, telnet, ftp 작업 등
- 대처방법
  - 변호사와 상의(미국)
    - 개인정보 침해 가능성이 있는 정보보호제품
    - Firewall 설치와 관련된 법적문제
      - *http://www.all.net/books/audit/Firewall/manal/index.html*
  - 일반적인 방법
    - 사용자들에게 모니터링 함을 사전에 공지하고 허락 받음
    - IDS 기능 악용금물

고부하 네트워크에서 문제

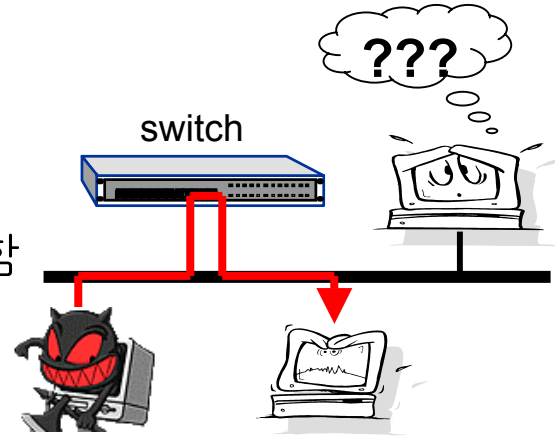
* 고부하 네트워크 환경에서의 “Packet drop” 현상
* 대처방법
  * 탐지 대상 네트워크 분리
  * 탐지 대상에 따른 침입 분리
  * 패턴 수집 및 침입 분석 방법 개선
  * IDS 시스템 성능 향상

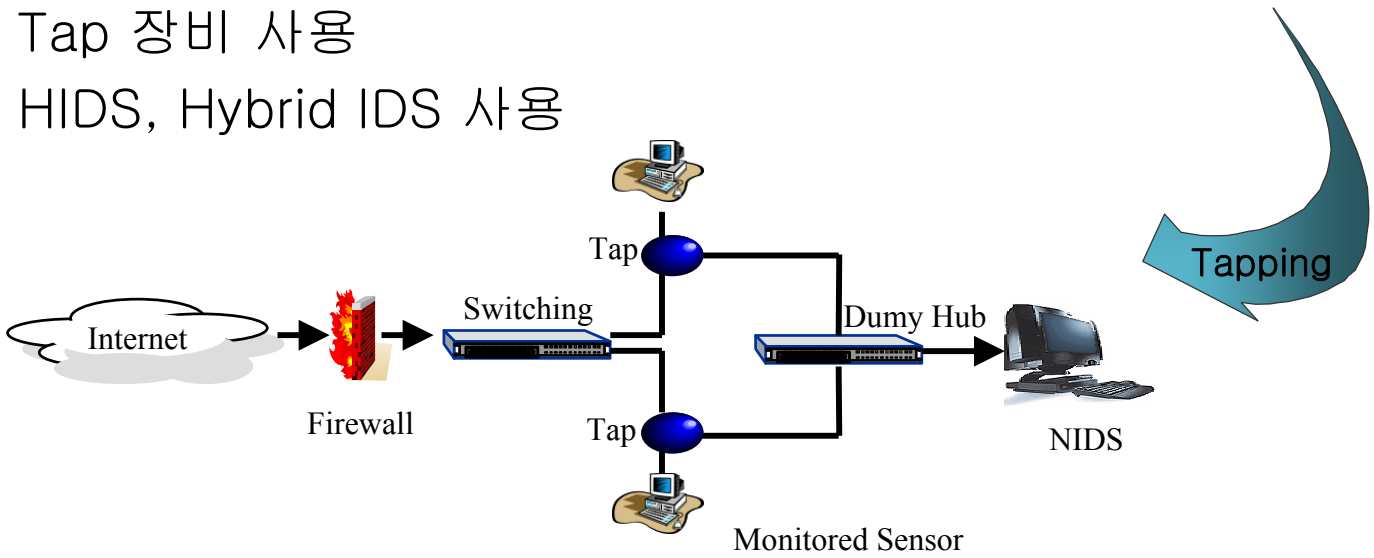
네트워크 부하	탐지율(%)
~ 2 Mb/s	66
~ 5 Mb/s	67
~ 13 Mb/s	75
~ 25 Mb/s	33
~ 49 Mb/s	10

(자료 : 1998년 Compaq 사의 ISS RealSecure 제품 테스트 결과)

스위치 네트워크 환경 문제

- 스위칭 네트워크
  - Promiscuous mode로 동작 불가
    - NIDS는 전체 네트워크를 감시 못함
- 대처방법
  - Span/Monitor 포트 사용
  - Tap 장비 사용
  - HIDS, Hybrid IDS 사용





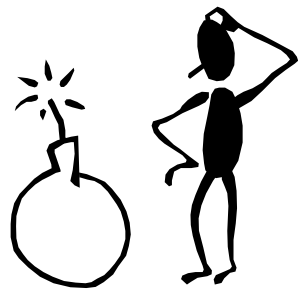
(자료 : http://www.sans.org/newlook/resources/IDFAQ/switched.htm)

암호화 패킷 분석 문제

- 암호화 패킷 분석 불가
  - VPN 설치로 인한 암호화된 패킷
  - 암호화 통신에 따른 암호화된 패킷
    - PGP, SSH
- 대처방법
  - 호스트 기반 IDS 이용
  - VPN 내부에 IDS 설치

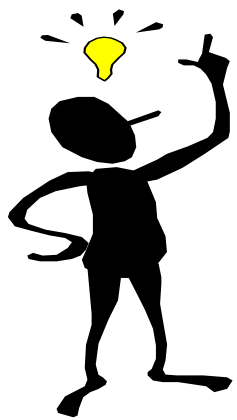
과다한 대응행동 설정 문제

- 대응기능
  - Firewall 연동, TCP 세션 종료, SMS, E-mail
- 과다한 대응행동 설정의 문제점
  - 저장공간 손실
    - E-mail 서버, 핸드폰 문자 수신 한계
  - 네트워크 트래픽 증가
    - E-mail 서버 부하 증가
  - 가용성 문제
    - 공격자의 출발지 주소를 위장, 정상적인 사용자의 접근 차단
    - 접근통제 기능의 경우 매우 위험함
      - Firewall 연동, TCP 세션 종료



과다한 대응행동 설정 문제(계속)

- 대처 방법
  - 적절한 대응행동 설정
  - 일정기간만 접근통제 실시
  - 차단 되어서는 안되는 IP 지정
    - 예 : 비즈니스 파트너 네트워크



IDS 관리 문제

- 하드웨어 유지관리
- False positive 문제
- 즉각적인 응답
- OS 업데이트
- IDS 업데이트와 시그너처 업데이트
- 중앙집중적인 경고 관리
- 시그너처 생성 및 업데이트
- 즉각적인 프로그램 변경/패치
- 사용자 관리

IDS 한계

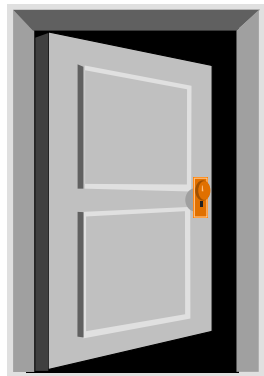
- 완벽한 솔루션이 아님
  - 제품을 설치해도 여전히 침입 발생가능성 있음
- 조직 내의 근본적인 문제점 해결 불가능
  - 보안전략, 보안정책의 부재 등
- 다른 보안 메커니즘의 기능을 대체할 수 없음
  - Firewall, VPN, PKI, I&A, Anti-Virus 등
- 관리자의 개입 없이는 효과적인 운용불가
  - 침입탐지 결과 대응 및 분석 등
- 오판율(False Positive)
  - 관리자에게 추가적인 시간과 자원 소비 유발
- IDS 직접 공격
- IDS 우회 공격

IDS 직접 공격

- 공격방법
  - 저장공간 및 메모리 소진
    - DOS, DDOS, IP Fragmentation
  - 동일한 IDS를 구입하여 kill 할 수 있는 방법 찾기
- 대처방법
  - 저장공간 관리
    - 백업, 충분한 저장공간 확보
  - 메모리 관리
    - 분산 네트워크 환경 구성
    - 탐지 센서 분리
  - 과도한 트래픽 제어
  - 안전한 프로그램 관리

IDS 우회 공격

- 우회 공격방법
  - IDS에는 탐지되지 않으면서 실제로 공격에는 성공하는 방법 (false negative)
  - 공격방법
    - 패턴 변조
      - 대부분의 NIDS들이 “pattern matching”에 의존
    - 주소위장(IP Spoofing)
    - IP Fragmentation
    - Slow scans
    - 공동으로 여러 IP 주소를 이용해 slow scan
- 대처방법
  - 패턴 조합(Reassemble) 기능
  - Statefull 패턴 수집
  - 주기적인 Scan 탐지

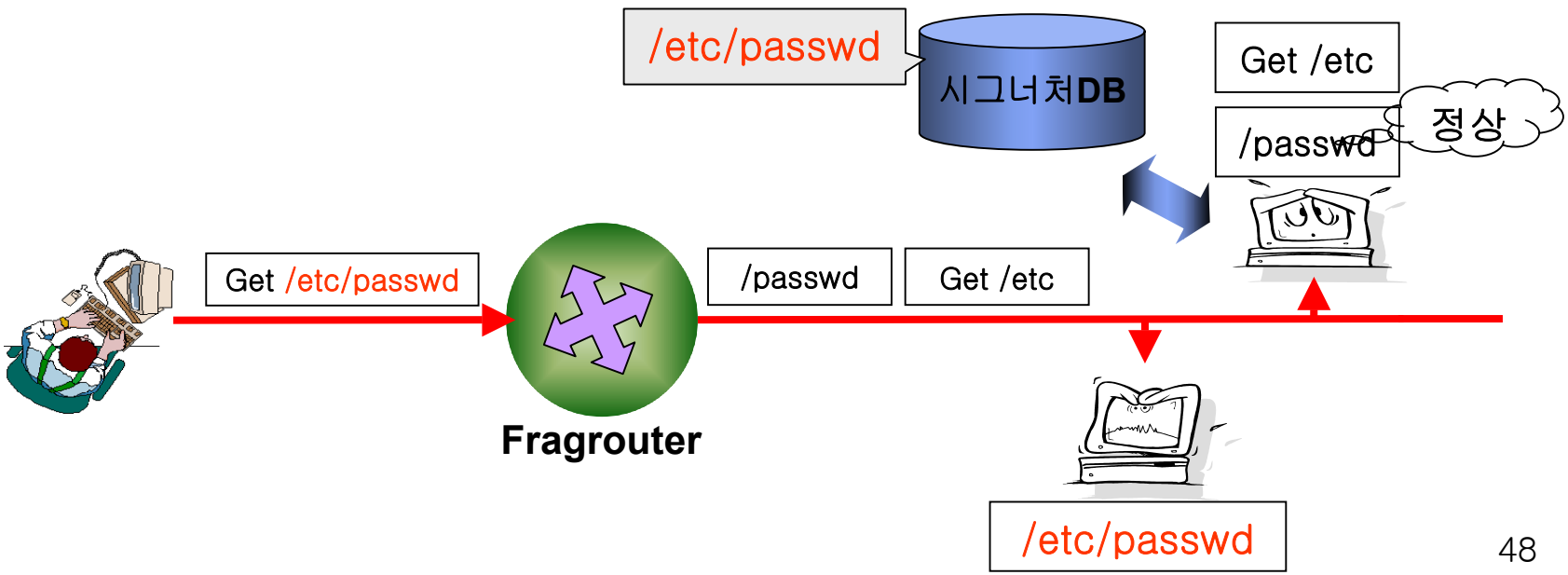


IDS 우회공격(계속)

- 다양한 우회방법 존재
  - Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection
    - http://www.robertgraham.com/mirror/Ptacek-Newsham- Evasion-98.html
  - 50 Ways to Defeat Your Intrusion Detection System
    - http://www.all.net/journal/netsec/9712.html
    - 실제 발생 가능한 다양한 아이디어 제시
  - 공격 도구
    - Fragrouter, Whisker, SideStep, IDSWakup, ISIC, AMDMutate, Stick 등

IDS 우회공격(계속)

* IDS 우회 공격 도구 – Fragrouter
  * http://www.anzen.com/research/nidsbench/
  * 단편화(fragmentation) 기법 이용
  * 22 가지 우회방법 제공



IDS 선택시 고려사항

* 폭넓은 고객지원이 가능한가?
* 목적과 환경에 적합한가?
* 다양한 침입탐지가 가능한가?
* 오탐률이 낮은가?
* 침입탐지 룰의 업데이트가 신속한가?
* 환경에 맞는 유연한 설정이 가능한가?
* 다양한 침입대응 기능을 제공하는가?
* 침입 재현 기능이 제공되는가?
* 타 시스템과 유기적인 연동이 가능한가?
* 자기보호 기능을 가지고 있는가?

'전문가가 권하는 'IDS(침입탐지시스템) 선택 10계명, 전자신문 2002. 5. 28 일자

결 론

- 침입탐지시스템
  - 조직의 보안확립에 기여
  - 보안을 위한 완벽한 해결방법은 아님
  - 탐지오류 최소화를 위한 지속적인 연구필요
- 지속적인 제품 관리
  - 보안위반사건 목록 업데이트
  - 지속적인 관리 및 운용이 매우 중요
- 침입발생 시 체계적인 보안대응 정책 수립이 요구됨
- 충분한 관리자 교육
  - 침입정보 분석 및 대처 능력 배양

참고자료

- NSA Glossary of Terms Used in Security and Intrusion Detection
- http://www.networkintrusion.co.uk
- http://www.networkcomputing.com
- http://www.exodus.net
- NIST- Special publication on IDS
- SANS 연구소 IDS FAQ
  - http://www.sans.org/newlook/resources/IDFAQ/ID_FAQ.htm
- Robert Graham Network IDS FAQ
  - http://www.robertgraham.com/pubs/network-intrusion-detection.html
- SecurityFocus IDS
  - http://www.securityfocus.com/frames/index.html?focus=ids

보안 투자로 인한 가치 산정

* (R-E) + T = ALE
  * T = 침입탐지 도구 가격
  * E = $ 도구를 이용해서 얻은 이익
  * R = 침입피해 복구 비용(매년)
  * ALE = 소비 예상액(Annual Loss Expectancy)

* R – (ALE) = ROSI
  * 보안 투자 공제에 따른 대가(return)
    * 침입으로 인한 피해액 – 매년 소비예상 액

CIO Magazine (February 15, 2002)
HuaQiang Wei, Researcher – University of Idaho