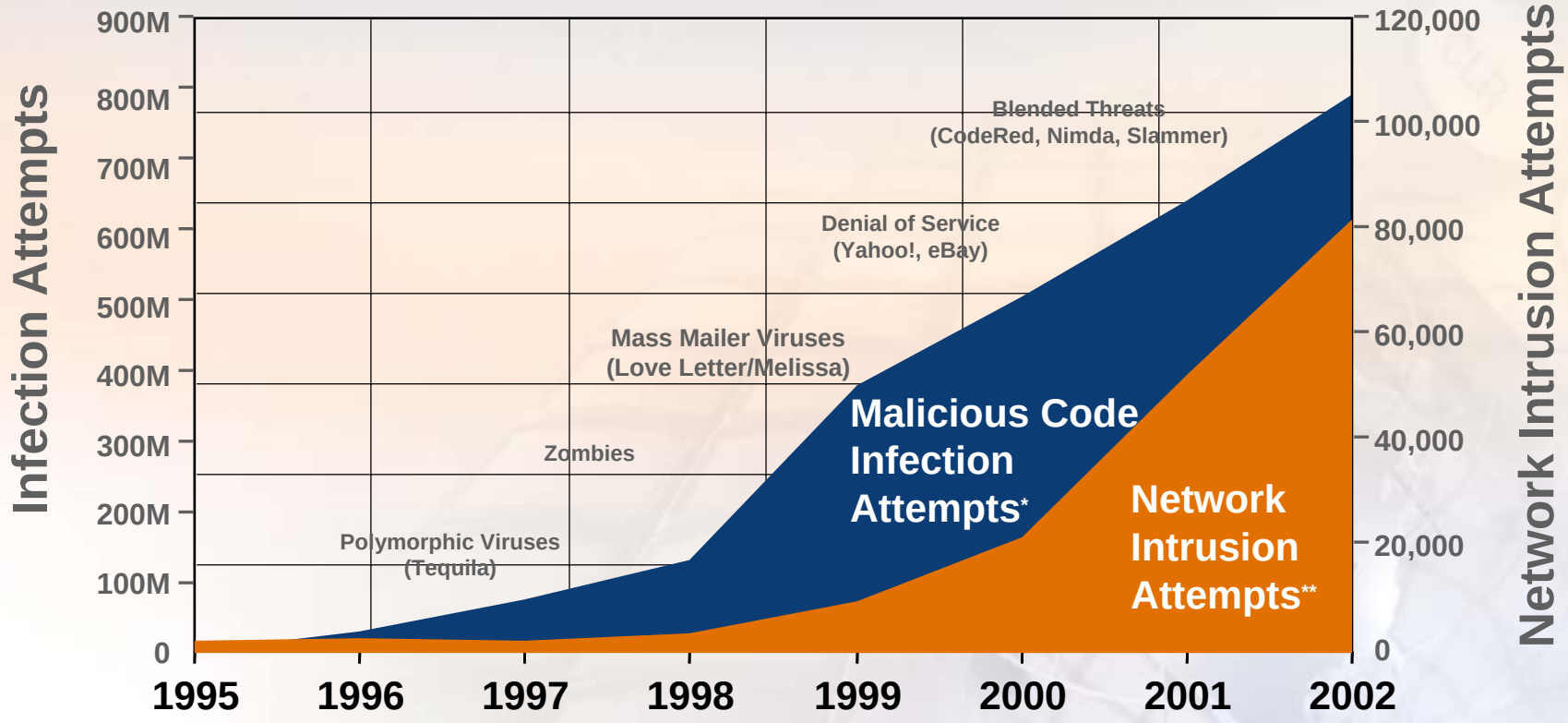
ISP Security Management & Operation

발표자 : ㈜정보보호기술 부사장 이 성 권

차례

1. ISP 보안 위협 현황

Worldwide Attack Trends

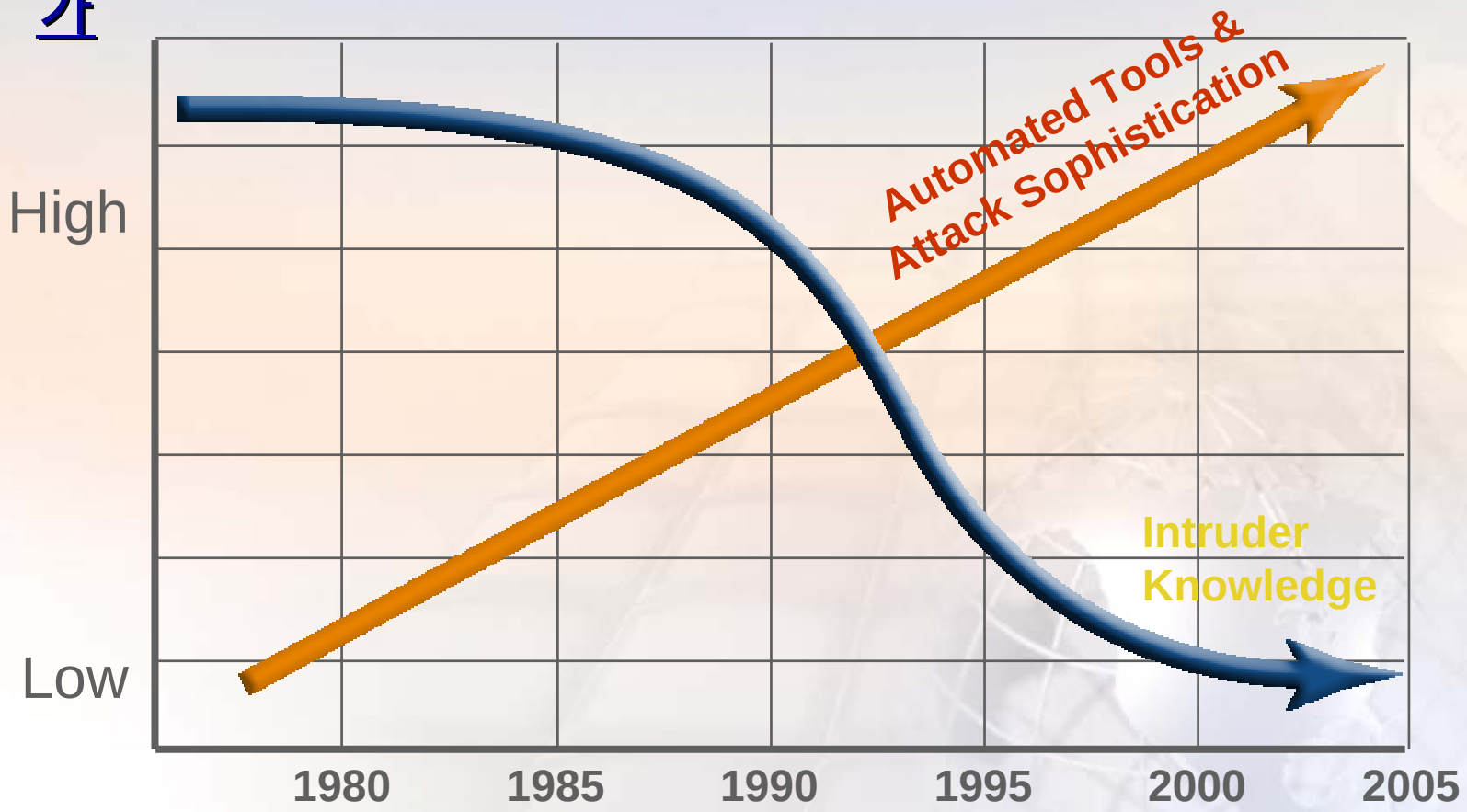


*Analysis by Symantec Security Response using data from Symantec, IDC & ICSA; 2002 estimated

**Source: CERT

1. ISP 보안 위협 현황

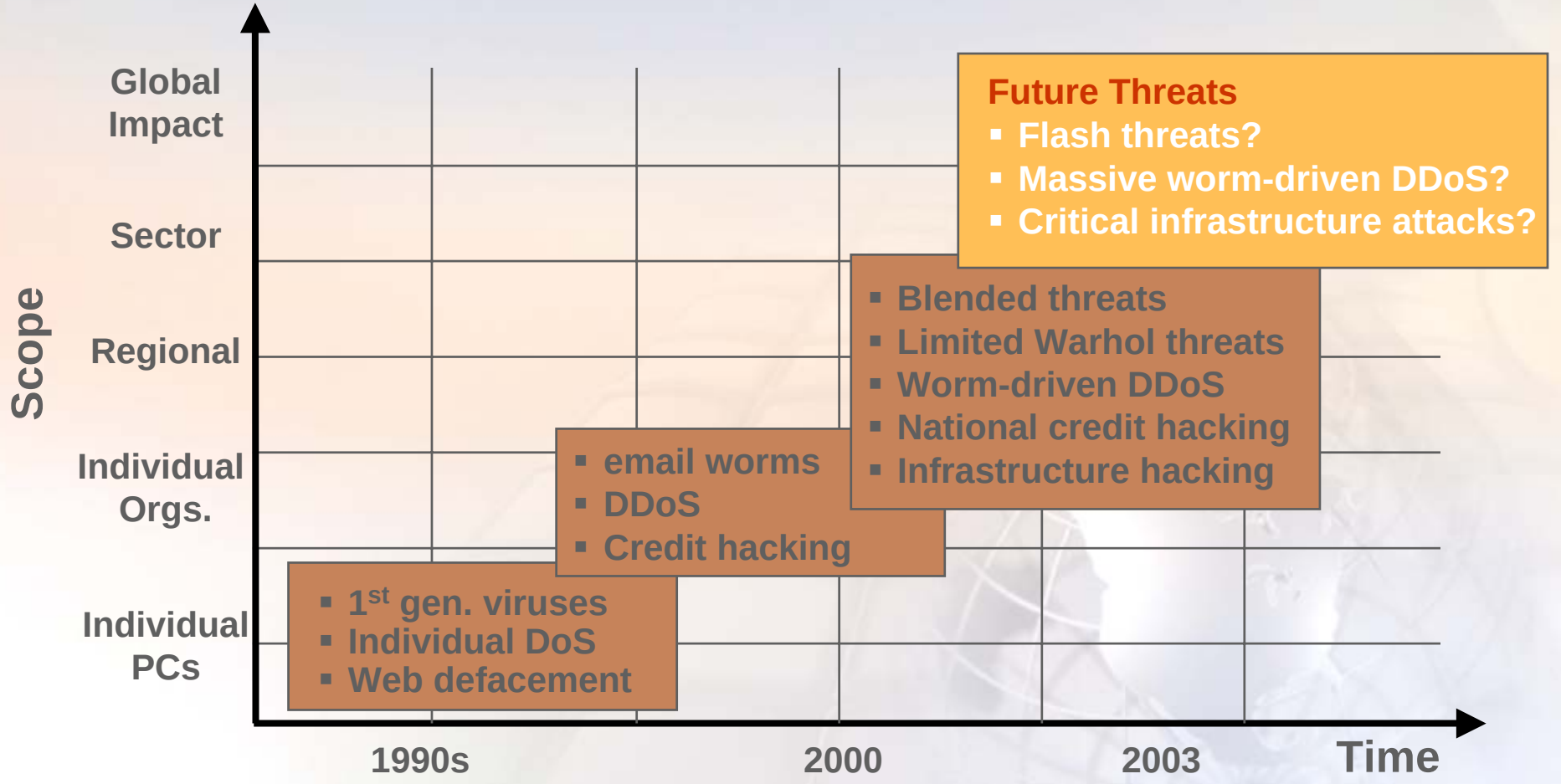
손쉬운 사이버공격의 증가



**Source: Symantec

1. ISP 보안 위협 현황

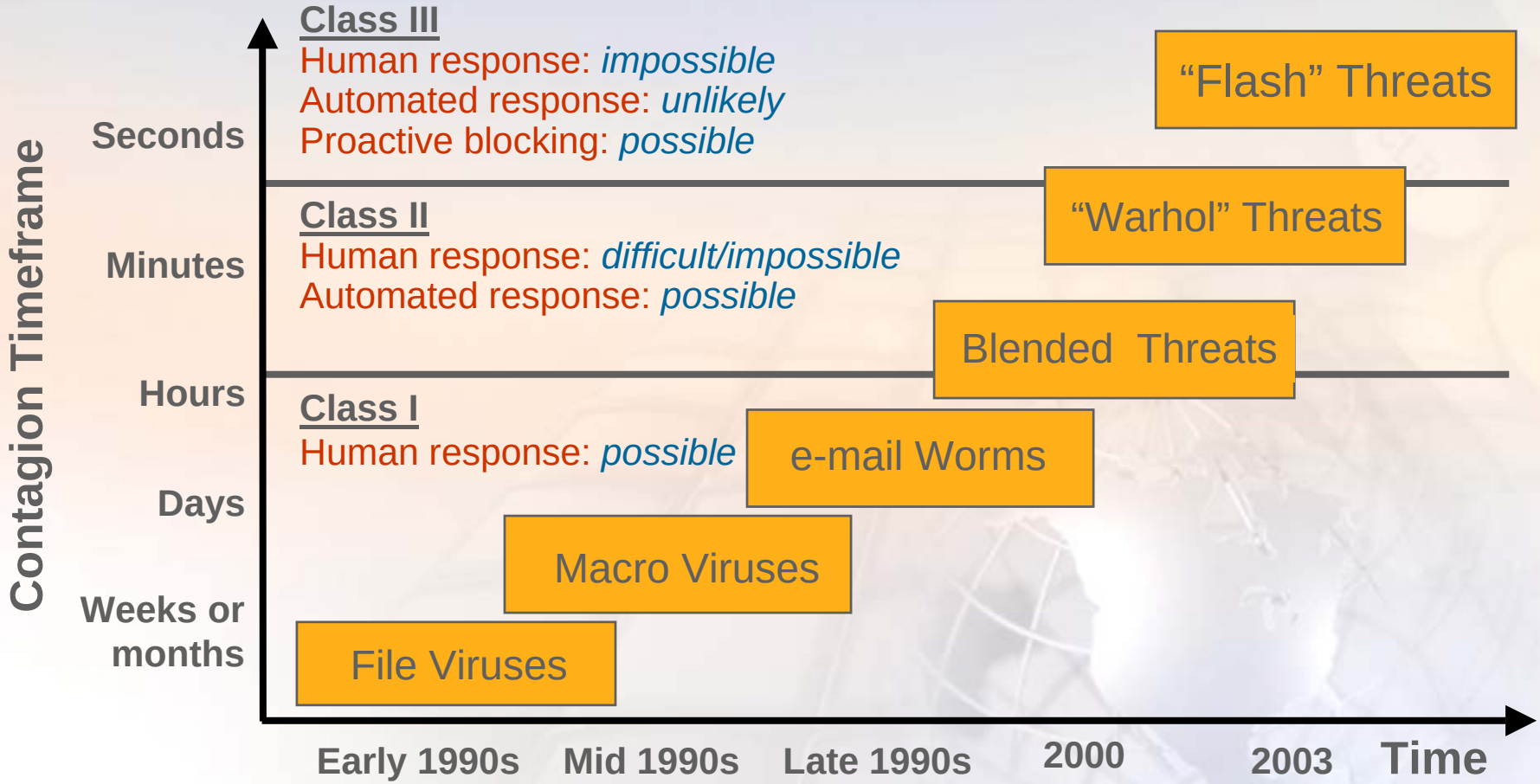
위협 종류별 전파범위



**Source: Symantec

1. ISP 보안 위협 현황

위협 종류별 전파시간

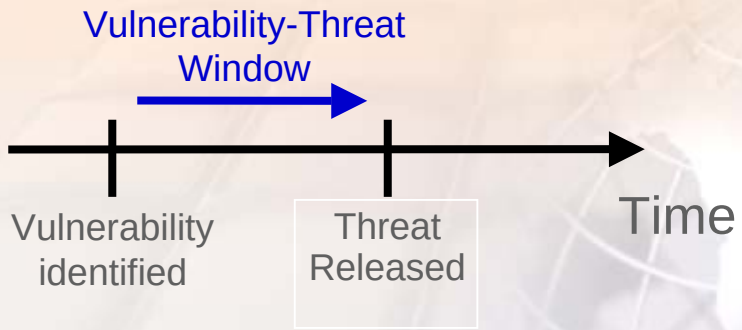


**Source: Symantec

1. ISP 보안 위협 현황

Day-Zero Threat의 정의

- A day-zero threat exploits a previously unknown, and therefore unprotected vulnerability.



**Source: Symantec

1. ISP 보안 위협 현황

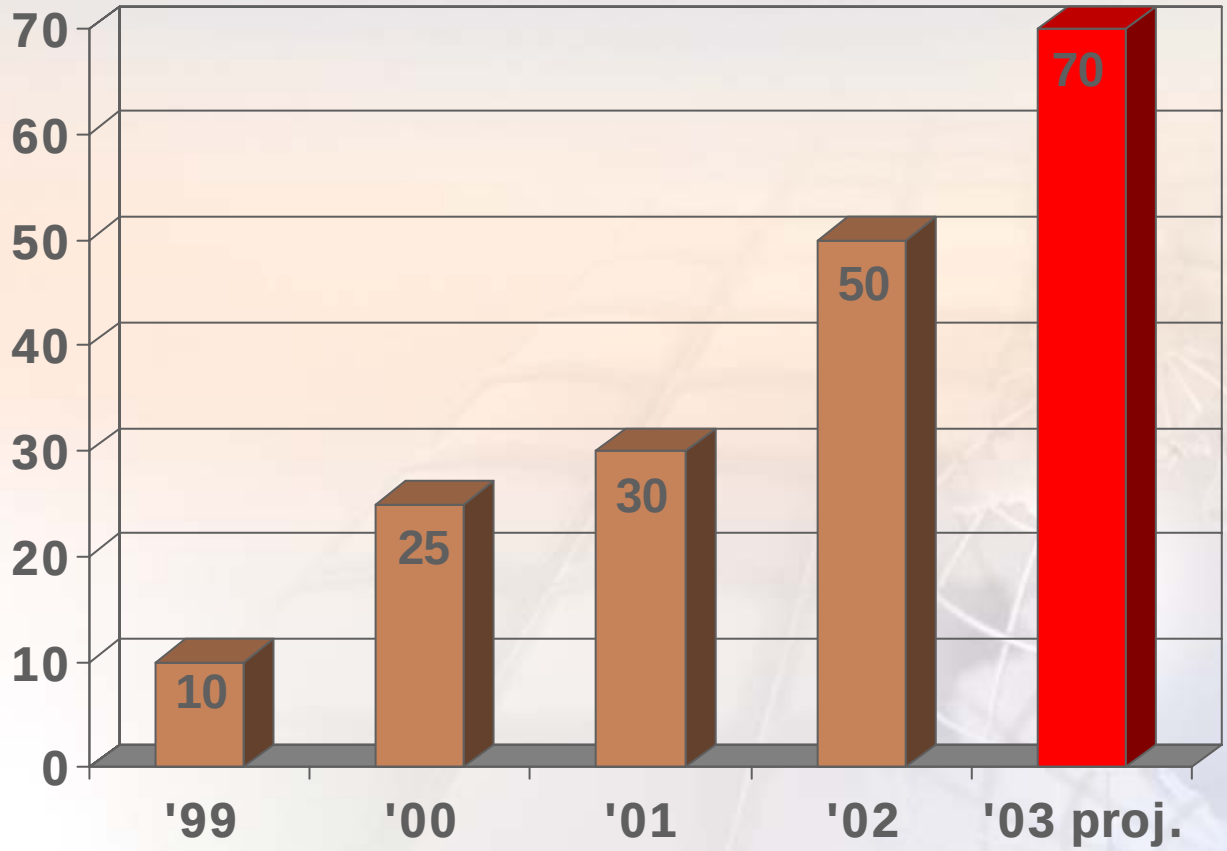
공격대상별 위협에 따른 결과

Threats \ Targets	Wireless Infrastructure	Web Services	Internet Backbone / Broadband	Physical Infrastructure / SCADA
Flash and Day-Zero Threats	Major disruption to multiple networks	Major disruption of B2B services sector-level impact	Global Internet Disruption	Impact to: ▪ Power ▪ Comm ▪ Hydro ▪ Chemical ▪ Other infra.
Warhol and Day-Zero Threats				
Blended Threats	Short-term disruption of individual networks			
DDoS			Short-term/ localized Internet disruption	Disruption of inter-networked SCADA
Targeted Hacking	Account theft/ corruption, DoS	Data theft/ corruption, DoS		Disruption of targeted infrastructures

**Source: Symantec

1. ISP 보안 위협 현황

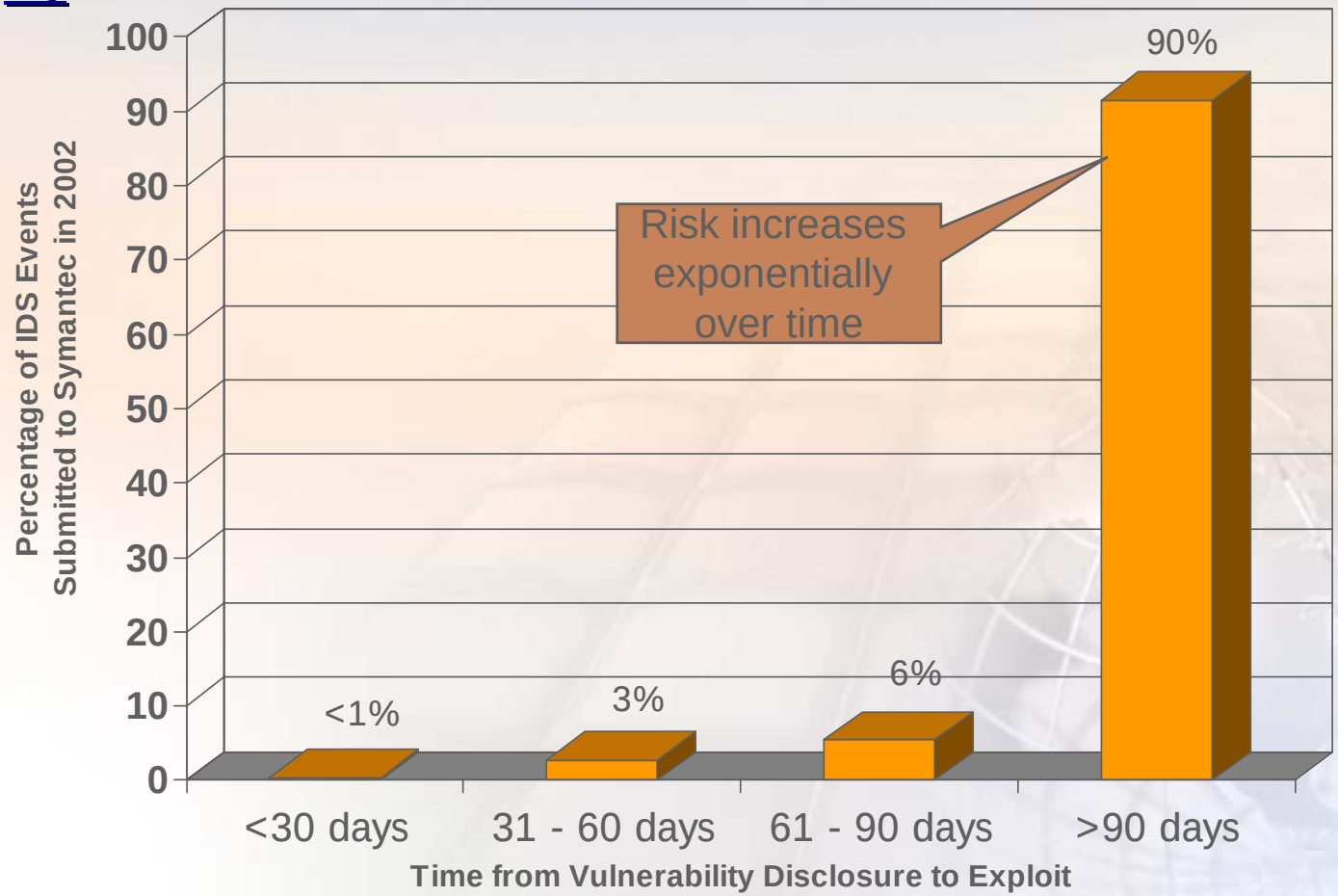
1주당 신규취약점 발생건수



**Source: Symantec

1. ISP 보안 위협 현황

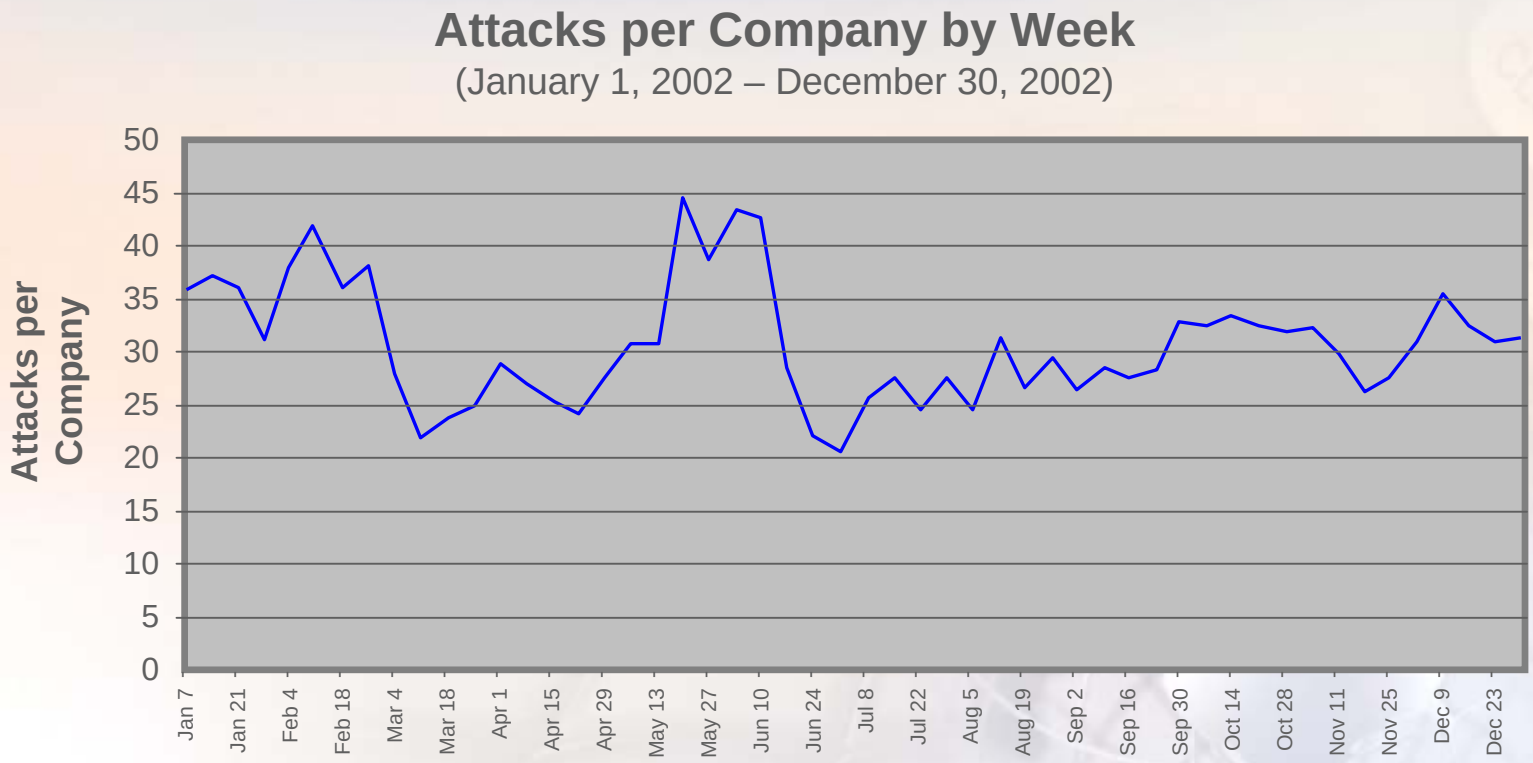
취약점 발표후 시간변화에 따른 위험의 증가



**Source: Symantec

1. ISP 보안 위협 현황

주당 평균 공격 발생 건수

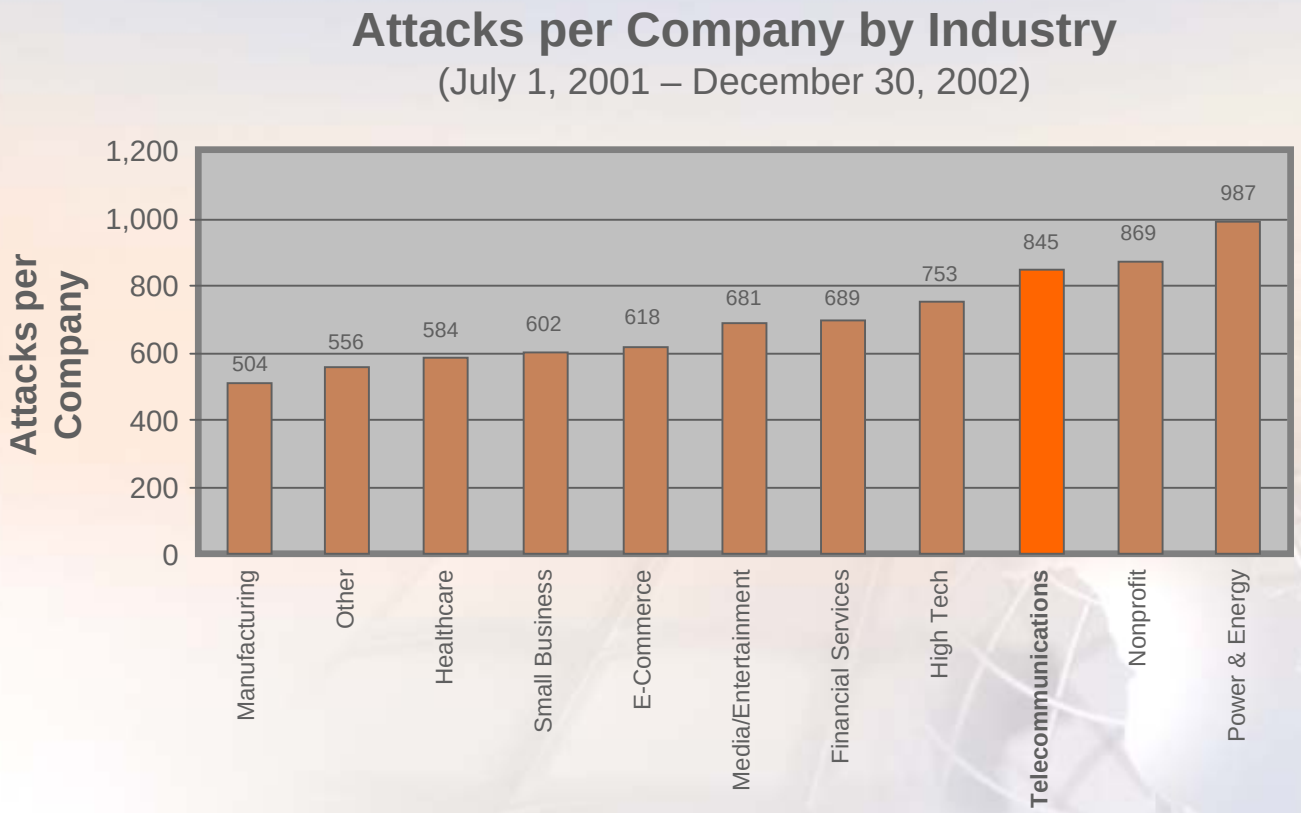


**Source: Symantec

Source: Symantec Internet Security Threat Report

1. ISP 보안 위협 현황

산업별 공격 발생 건수

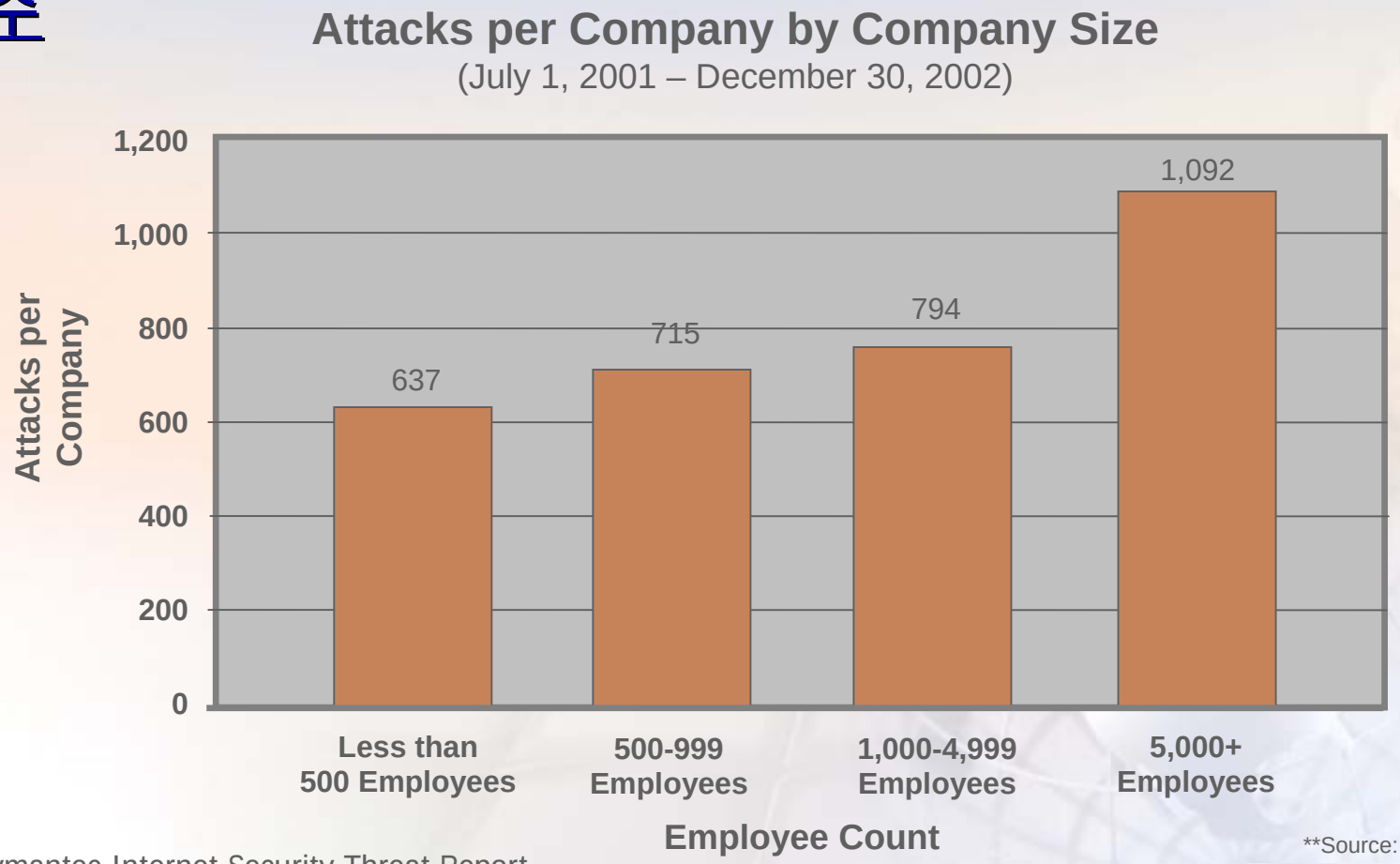


**Source: Symantec

Source: Symantec Internet Security Threat Report

1. ISP 보안 위협 현황

회사 규모별 공격 발생 건수



Source: Symantec Internet Security Threat Report

**Source: Symantec

차례

2. 능동형 보안기술

침입탐지 및 대응을 위한 기반구조

limitation

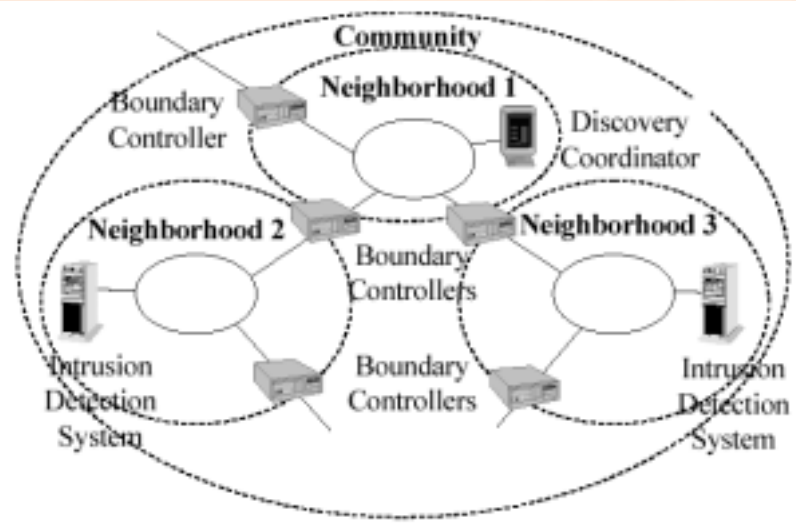
- IDS detect local intrusion symptoms and can only react locally
- No common language for remotely instructing boundary controllers to block selected traffic

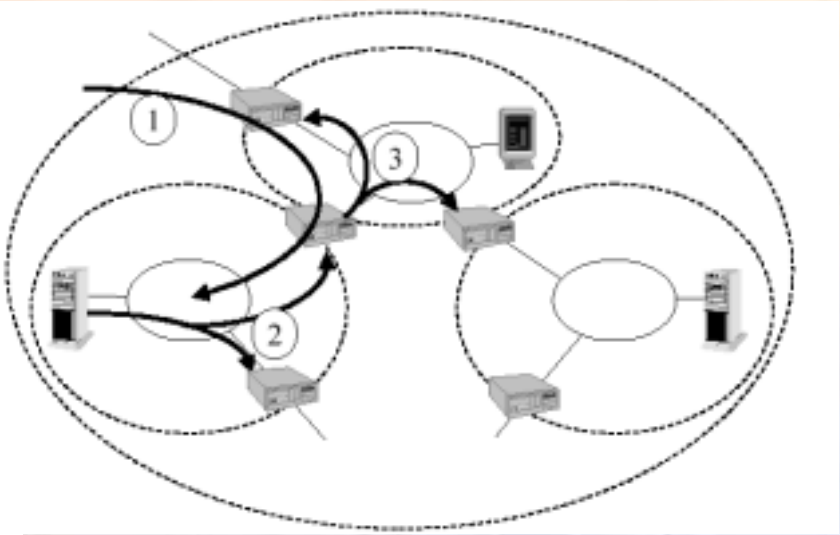
- **IDIP(Intrusion Detection and Isolation Protocol)**
  - Cooperative tracing of intrusions across network boundaries and blocking of intrusion at boundary controllers near attack sources
  - Use of device independent tracing and blocking directives
  - Centralized reporting and coordination of intrusion response

2. 능동형 보안기술

IDIP Concept

- **IDIP Communities**
  - Discovery Coordinator
  - Boundary Controller
  - Intrusion Detection System





2. 능동형 보안기술

IDIP 개요

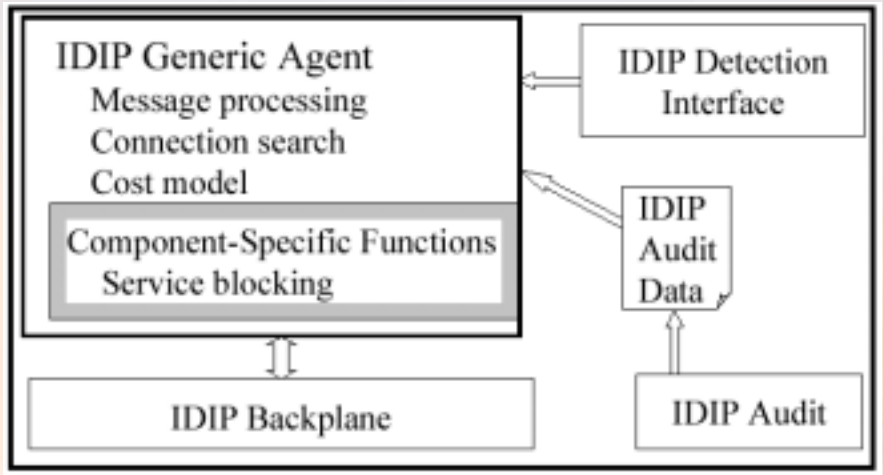
- **IDIP Primary Layers**
  - IDIP Application Layer
  - IDIP Message Layer

- **Message Type**
  - Trace
  - Report
  - Discovery Coordinator Directive

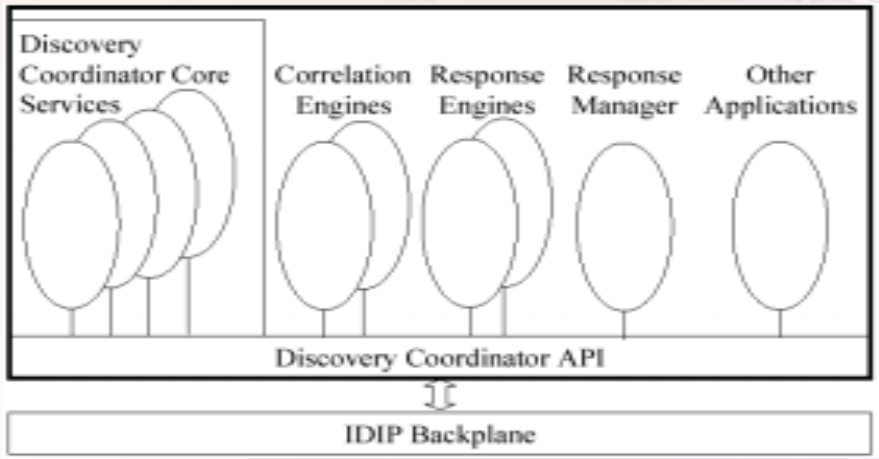
2. 능동형 보안기술

IDIP Application Layer

- Generic Agent

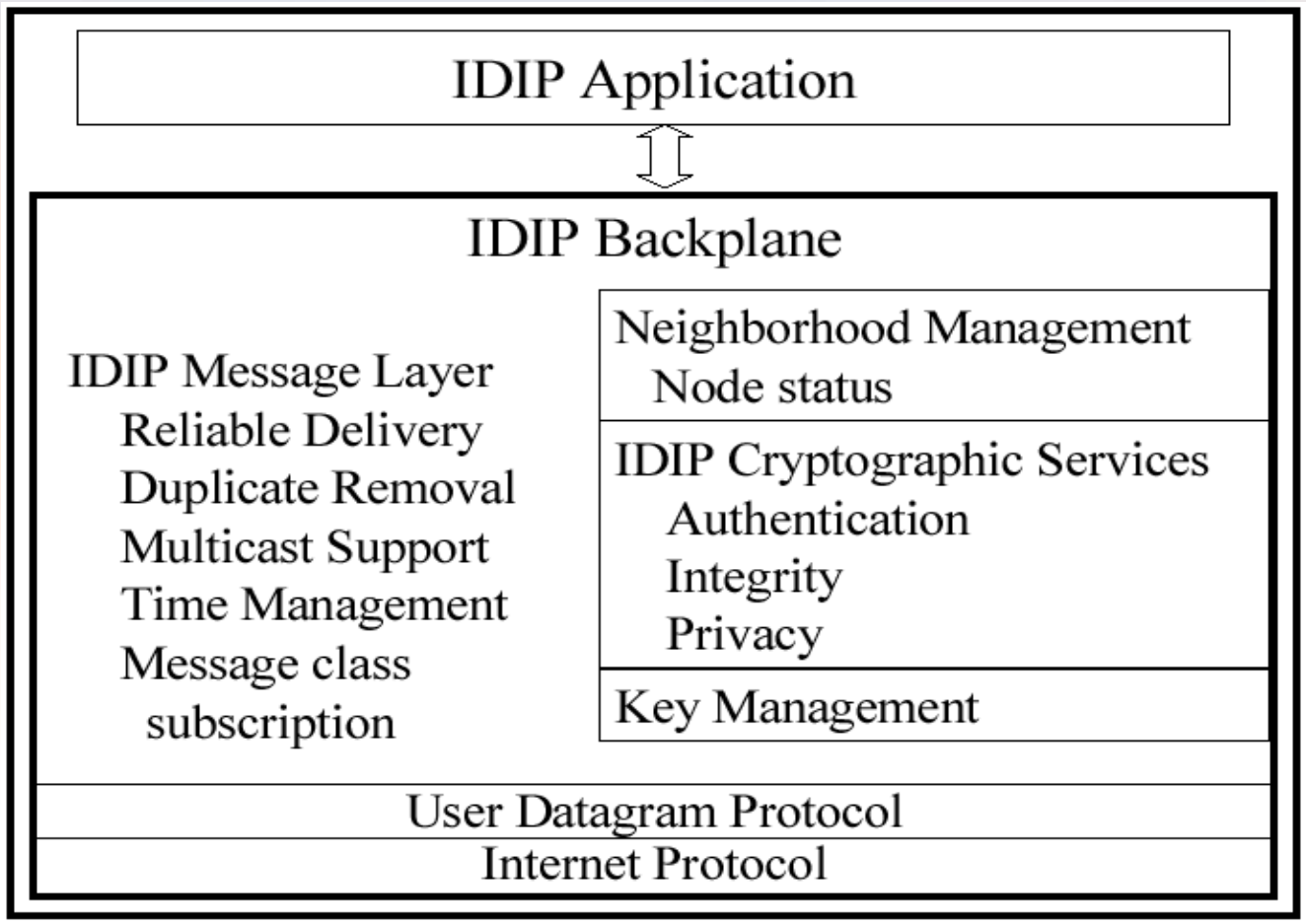


- Discover Coordinator Application



2. 능동형 보안기술

IDIP Backplane



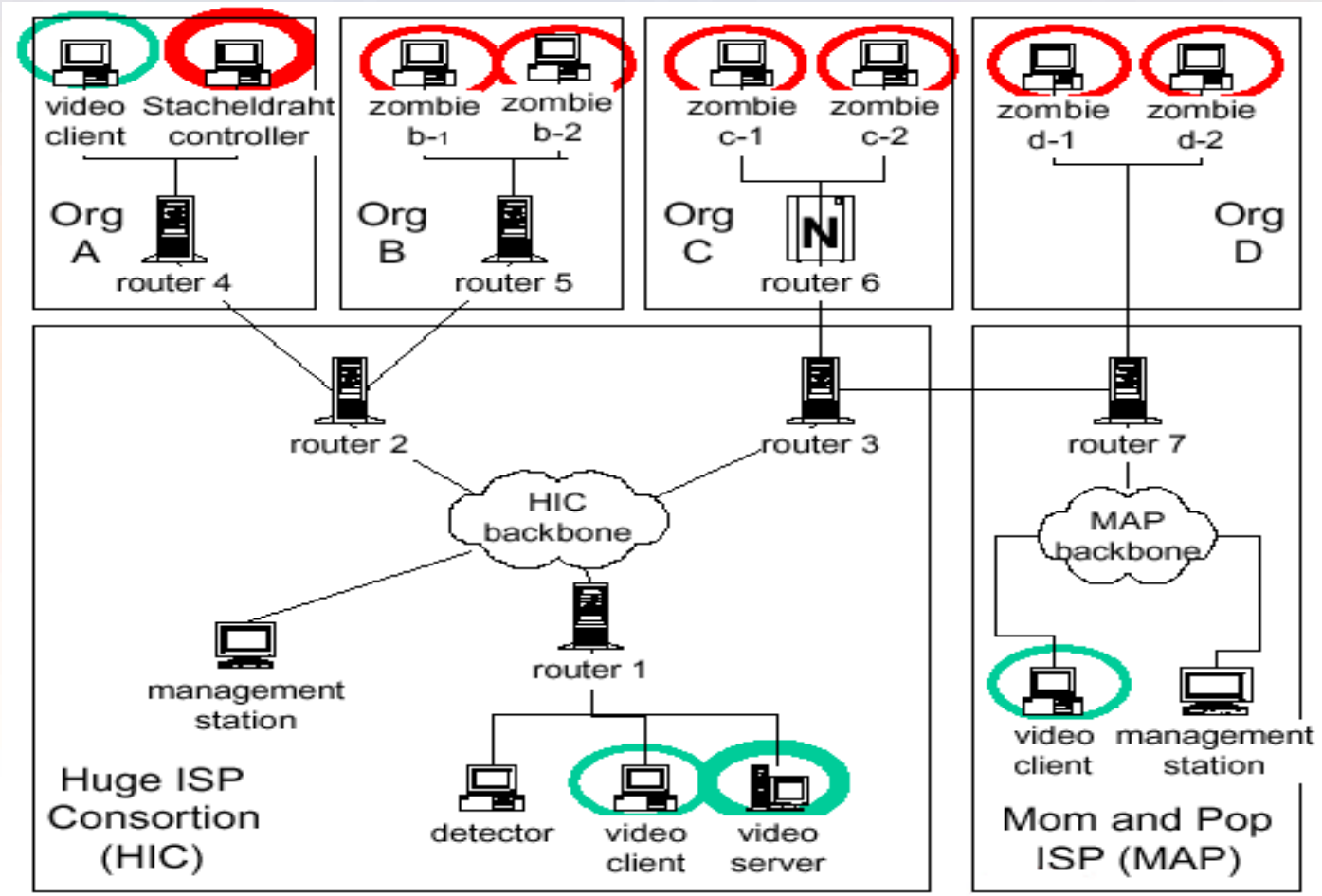
2. 능동형 보안기술

Integrated Components

Boundary Controllers	Intrusion Detection Systems	Host Based Responders
NAI Gauntlet Internet Firewall	Net Squared Network Radar	NAI Labs Generic Software Wrappers Prototype
Secure Computing Corporation Sidewinder™ Firewall	SRI EMERALD BSM and EMERALD FTP Monitors Prototypes	TCP Wrappers
Linux Router	U.C. Davis Graphical Intrusion Detection System Prototype	IP Filter
NAI Labs ARGuE Prototype	Oregon Graduate Institute StackGuard	
NAI Labs Multi-Protocol Object Gateway Prototype	ORA CORBA Immune System Prototype	
	NAI CyberCop Server and CyberCop Monitor	
	Internet Security Systems RealSecure	

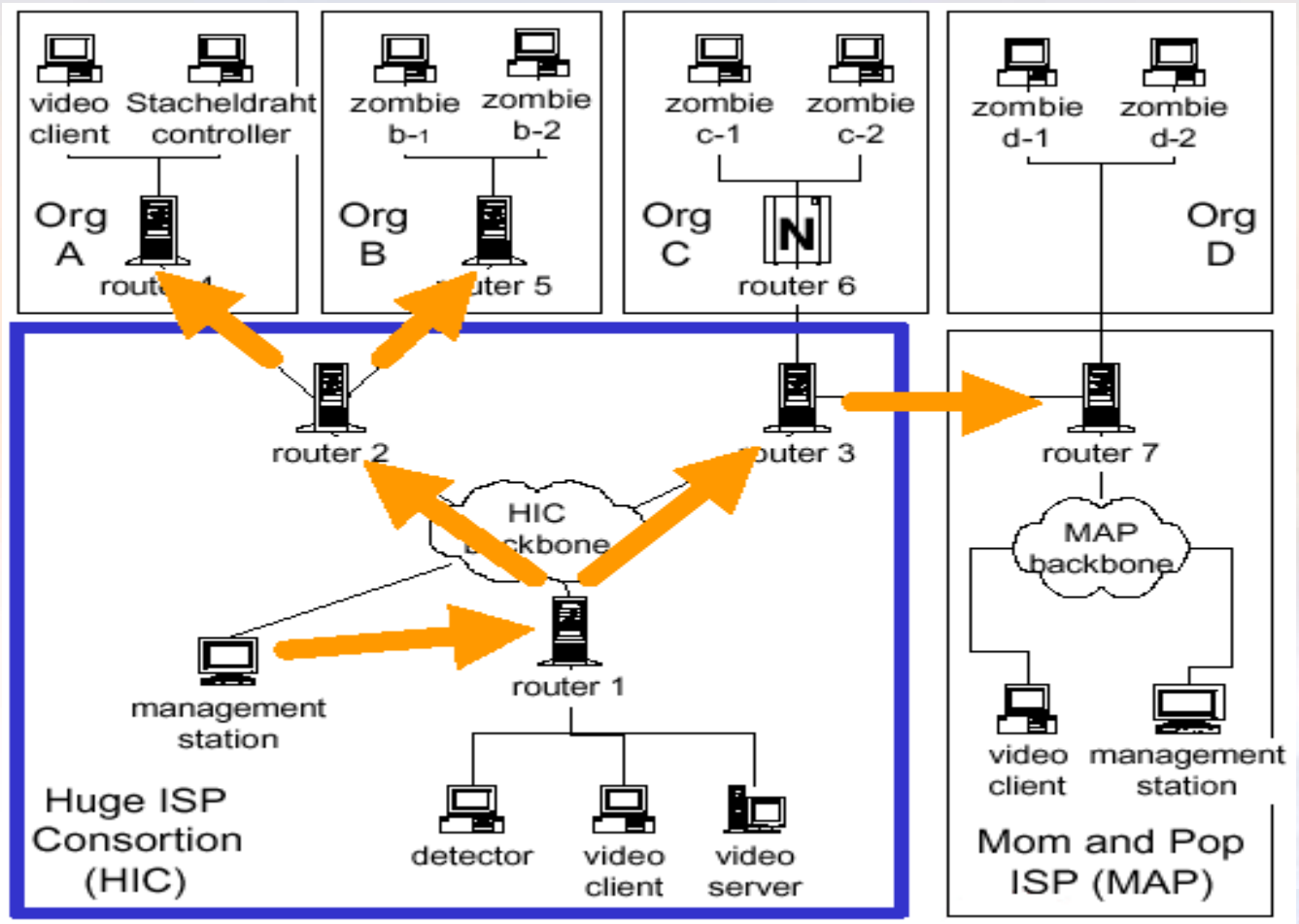
2. 능동형 보안기술

Demonstration Program



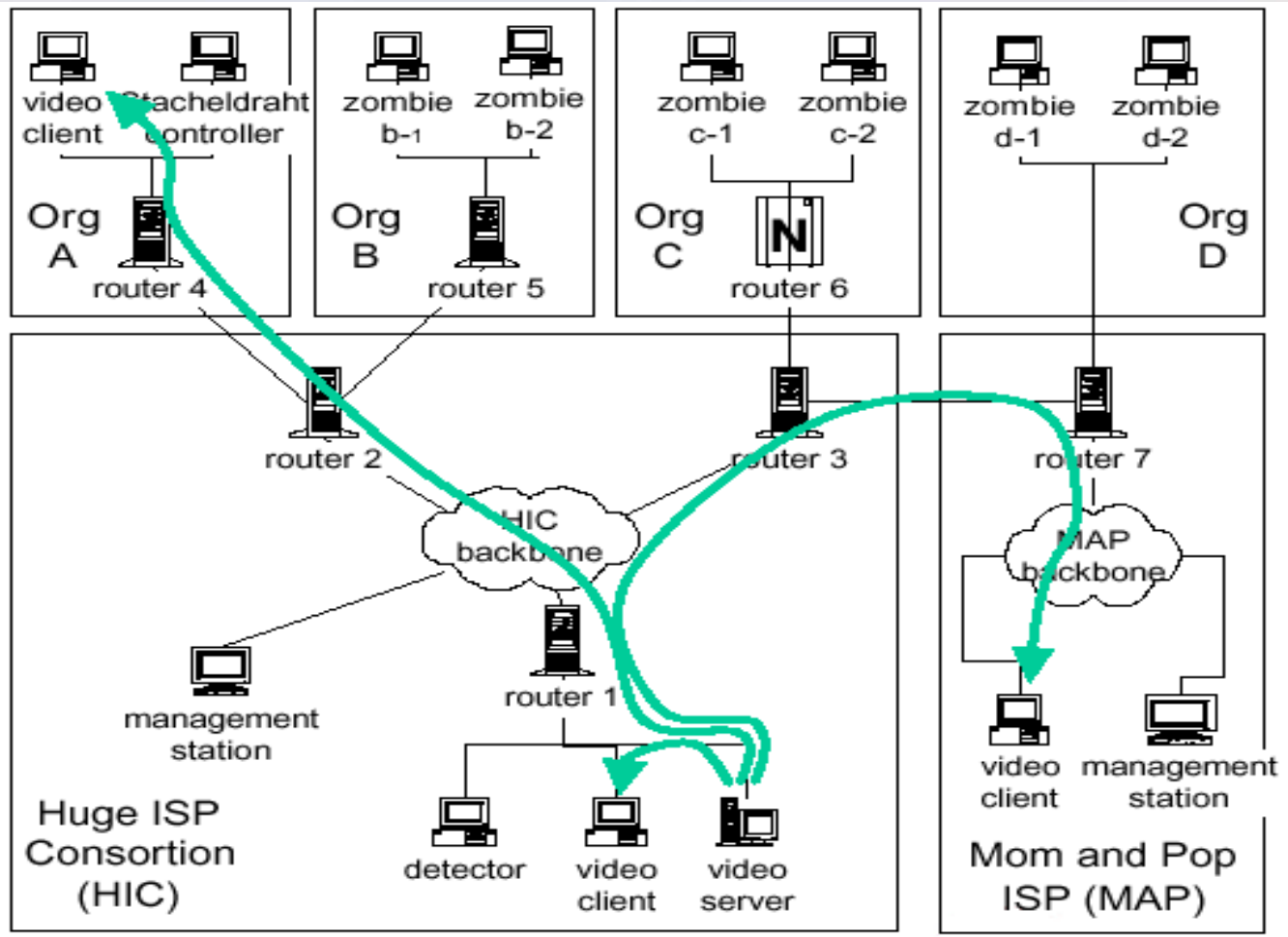
2. 능동형 보안기술

Exploiting Active Networks



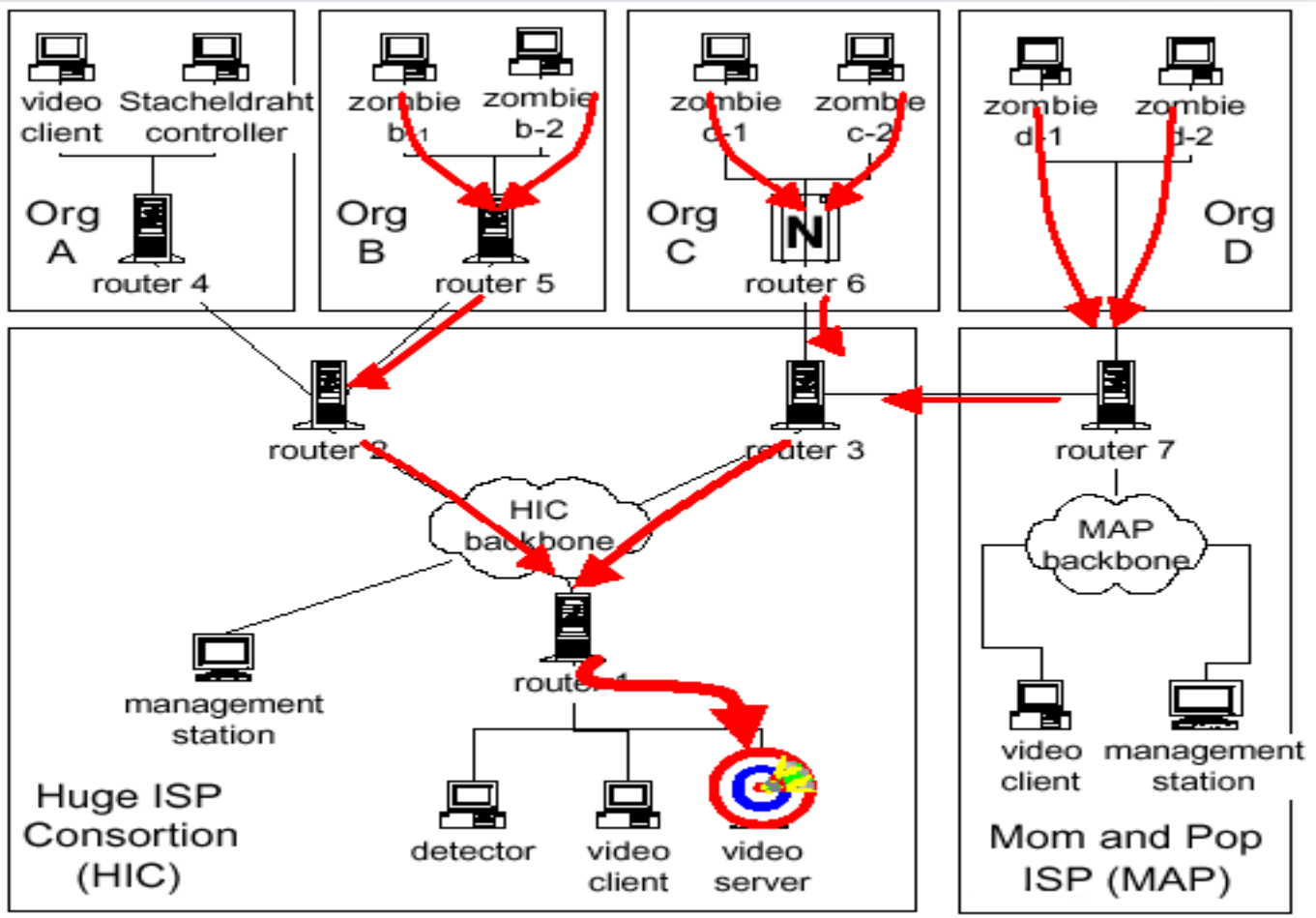
2. 능동형 보안기술

Normal Video Flow



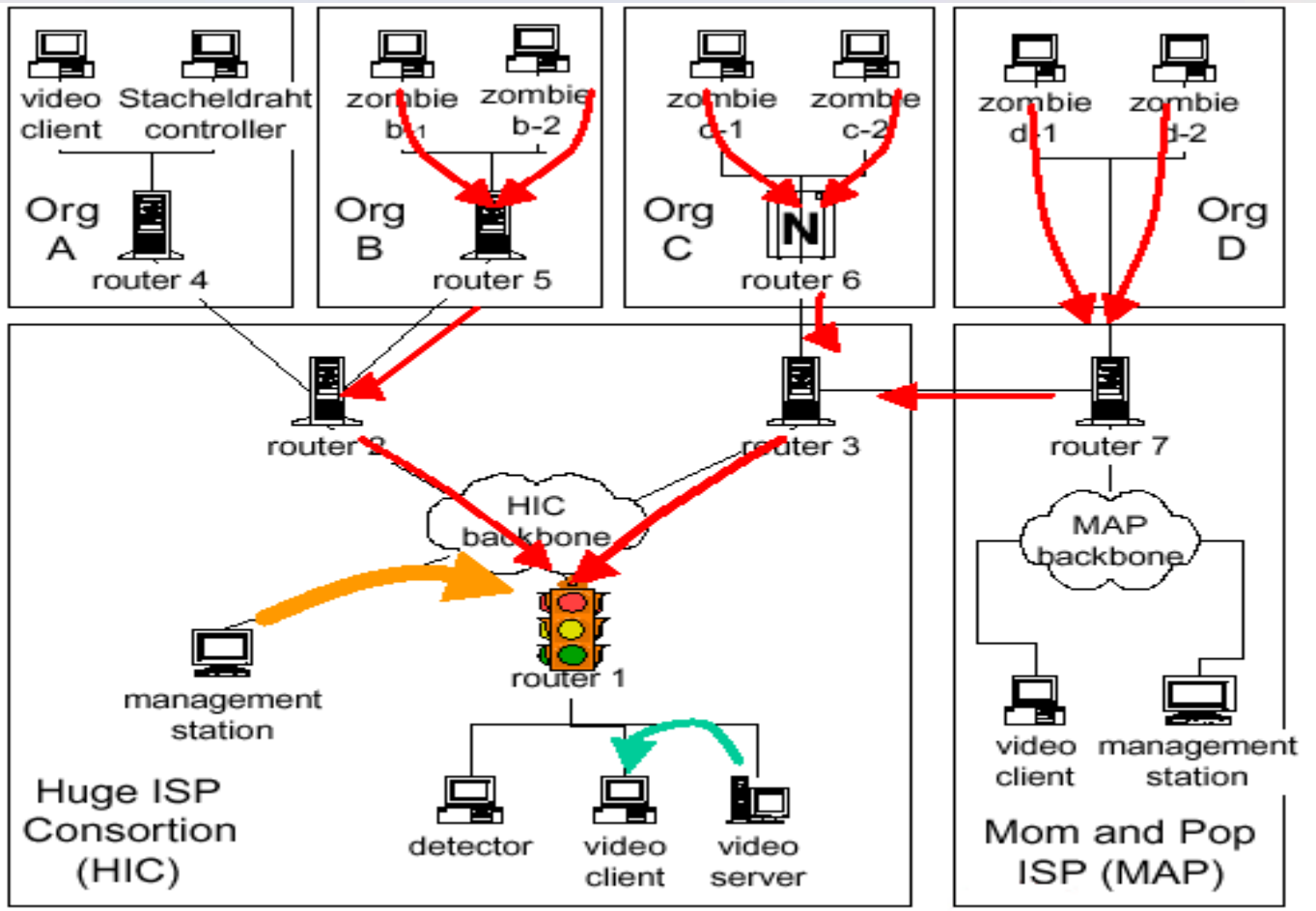
2. 능동형 보안기술

DDoS Attack Begins



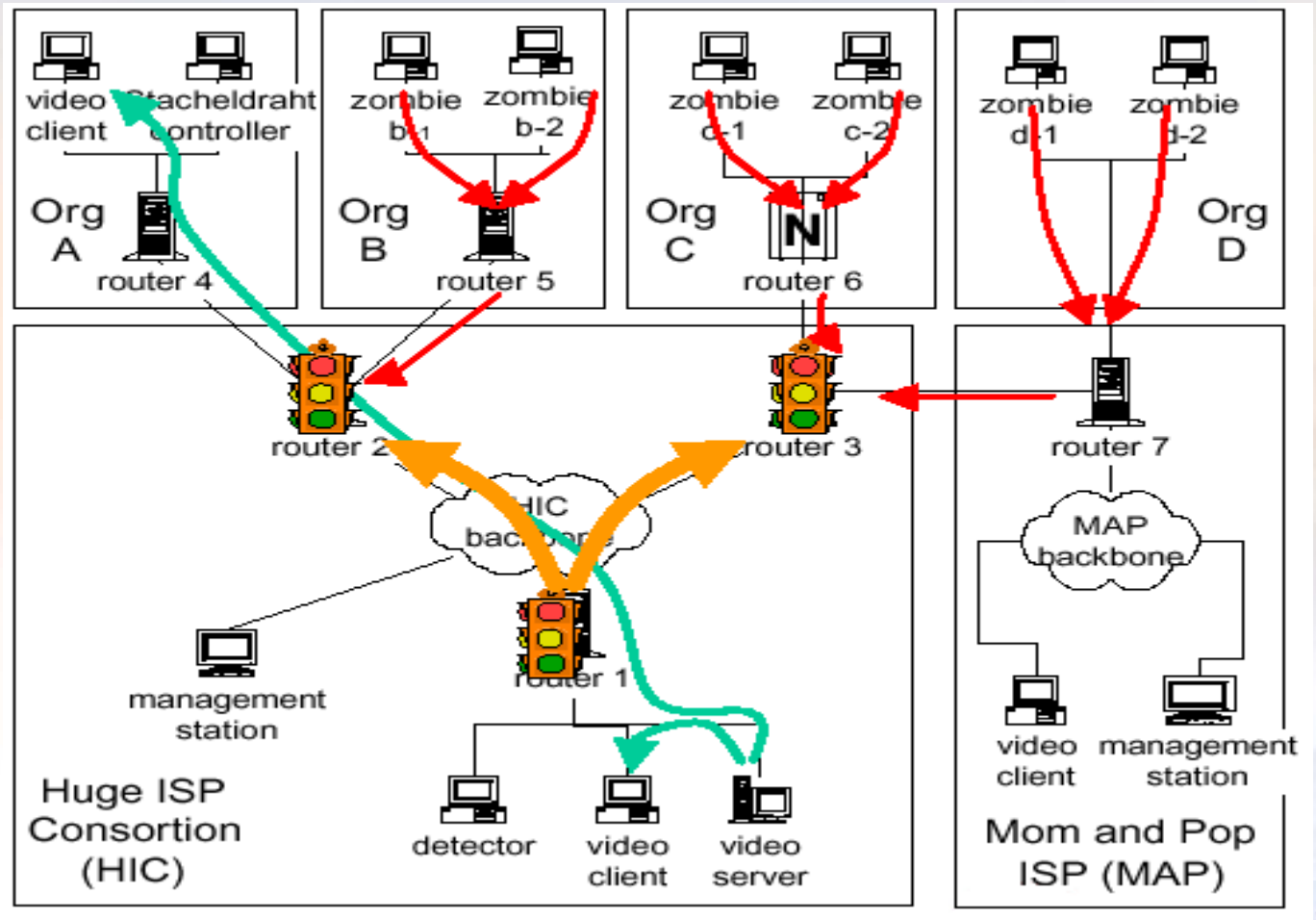
2. 능동형 보안기술

Active Rate Limiter Dispatched



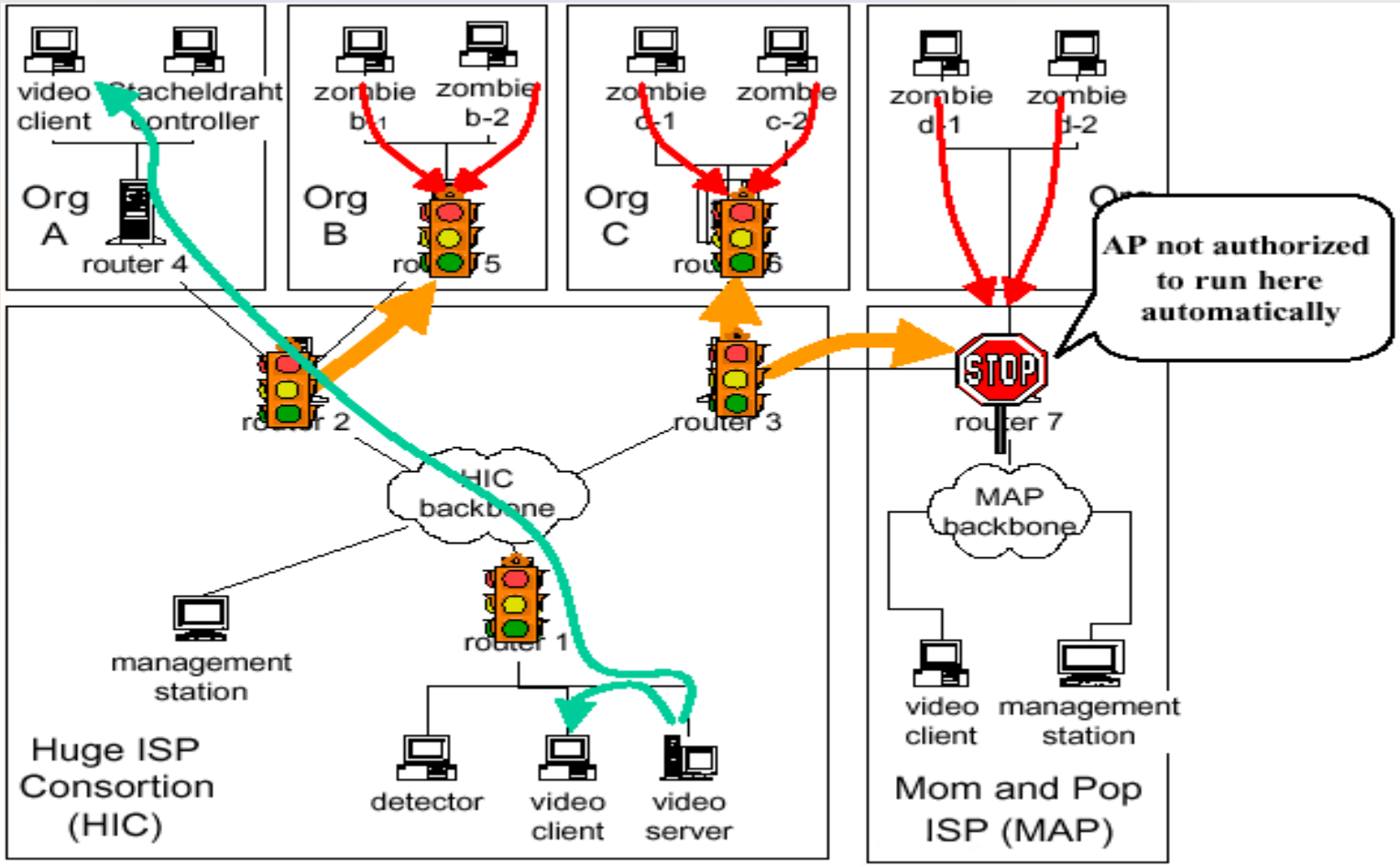
2. 능동형 보안기술

Rate Limiter Mitigates toward Attack Sources



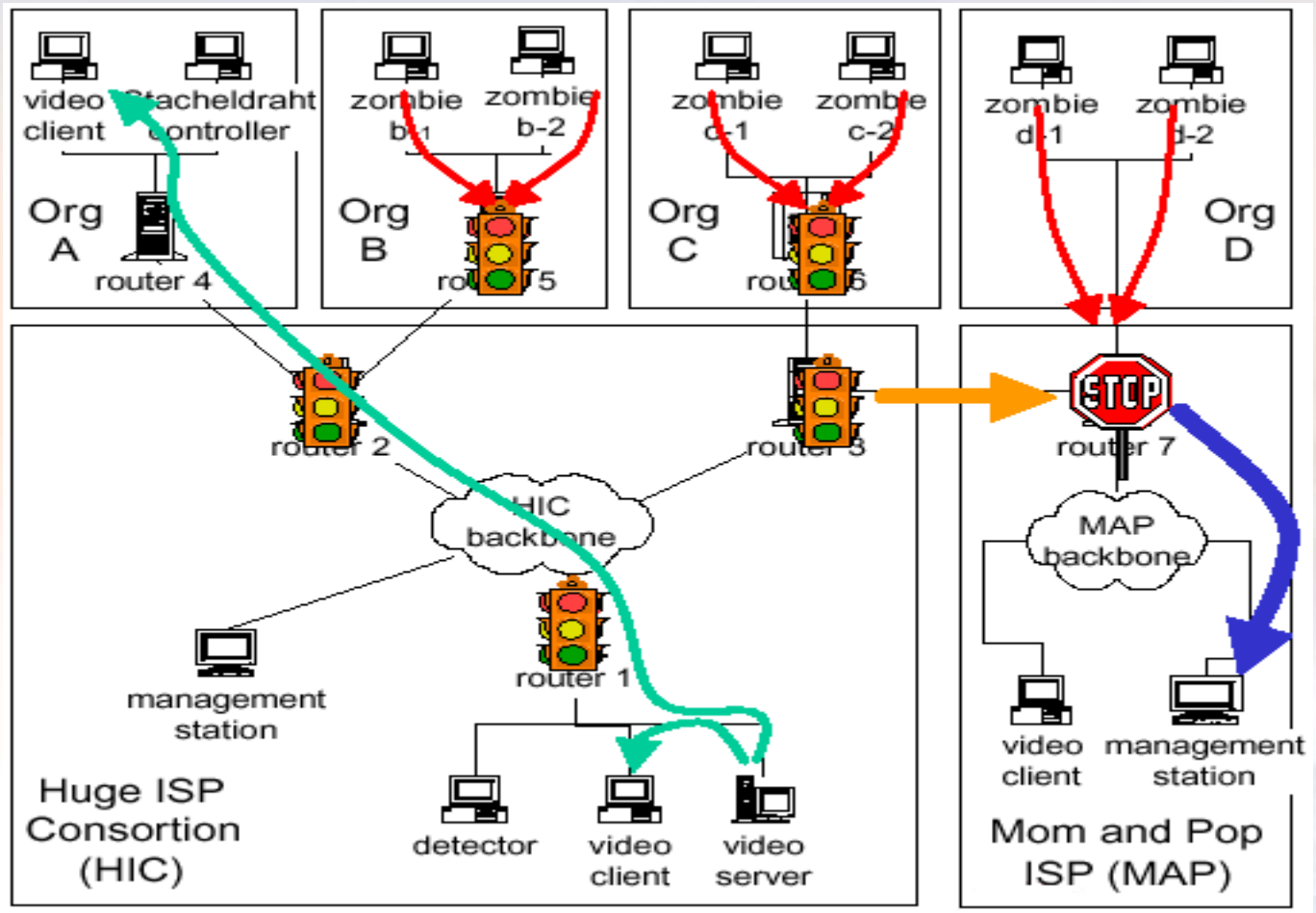
2. 능동형 보안기술

Rate Limiter Attempts to mitigate Beyond HIC

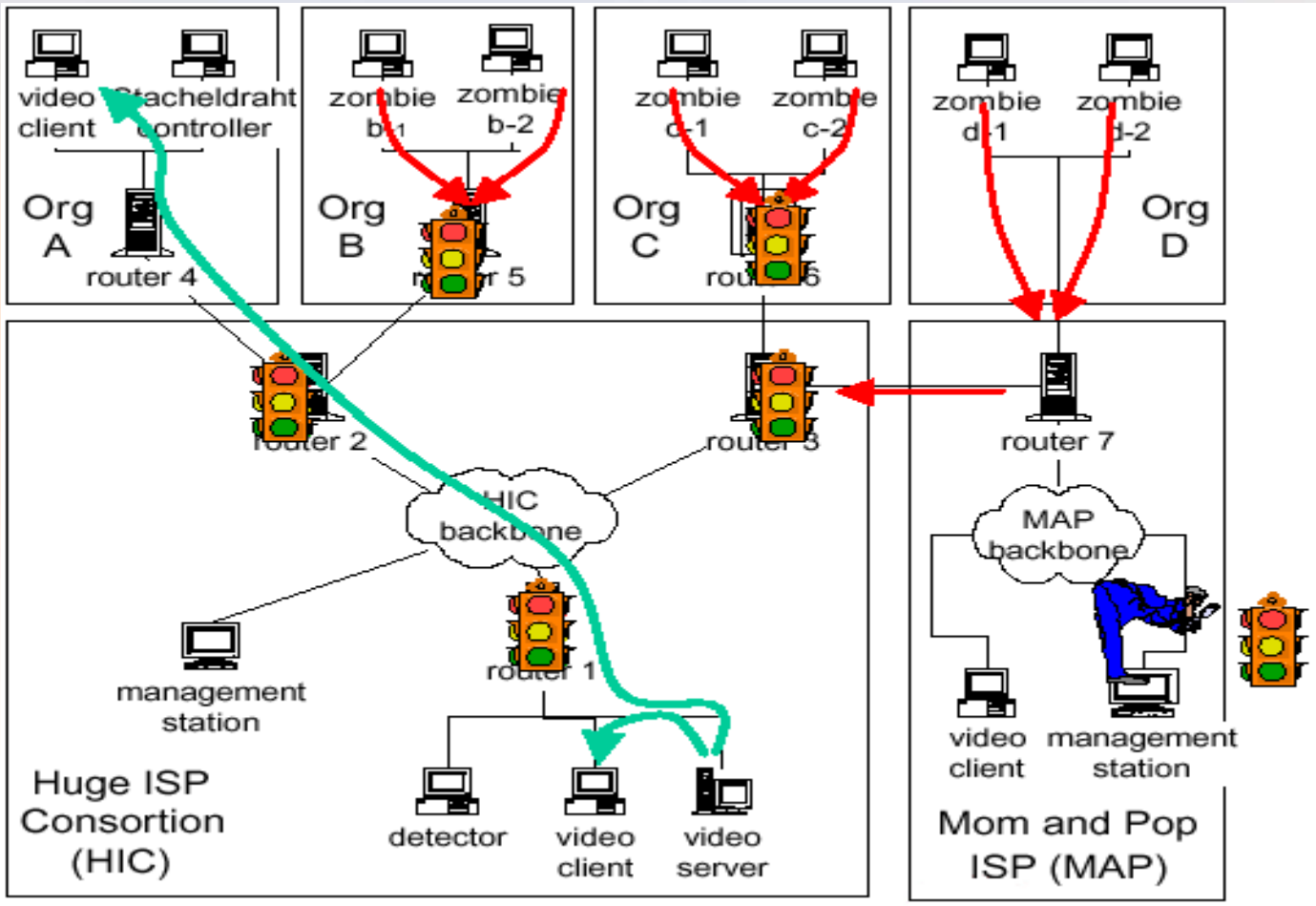


2. 능동형 보안기술

Authorization Failure Reported to MAP

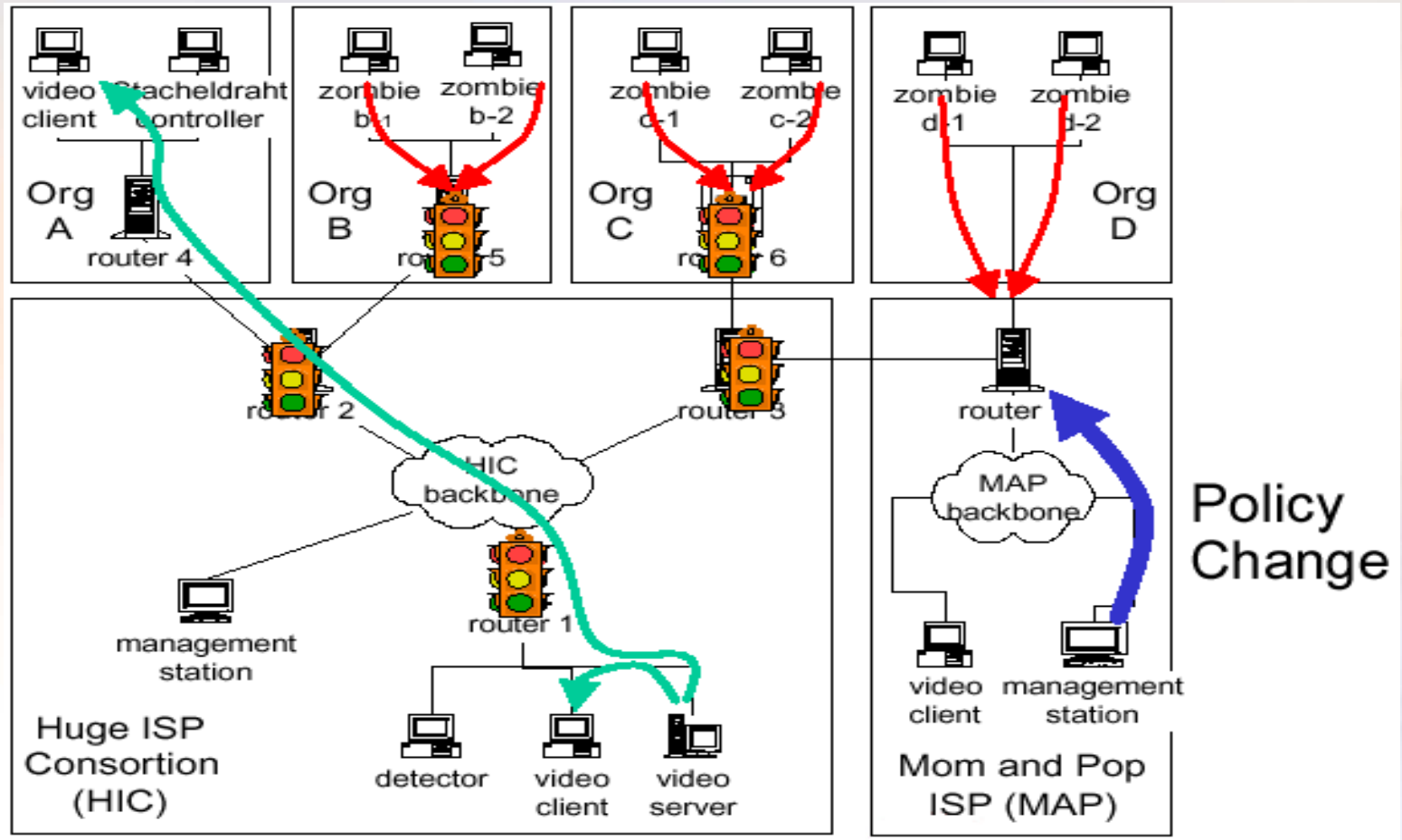


MAP Administrator Reviews Failure



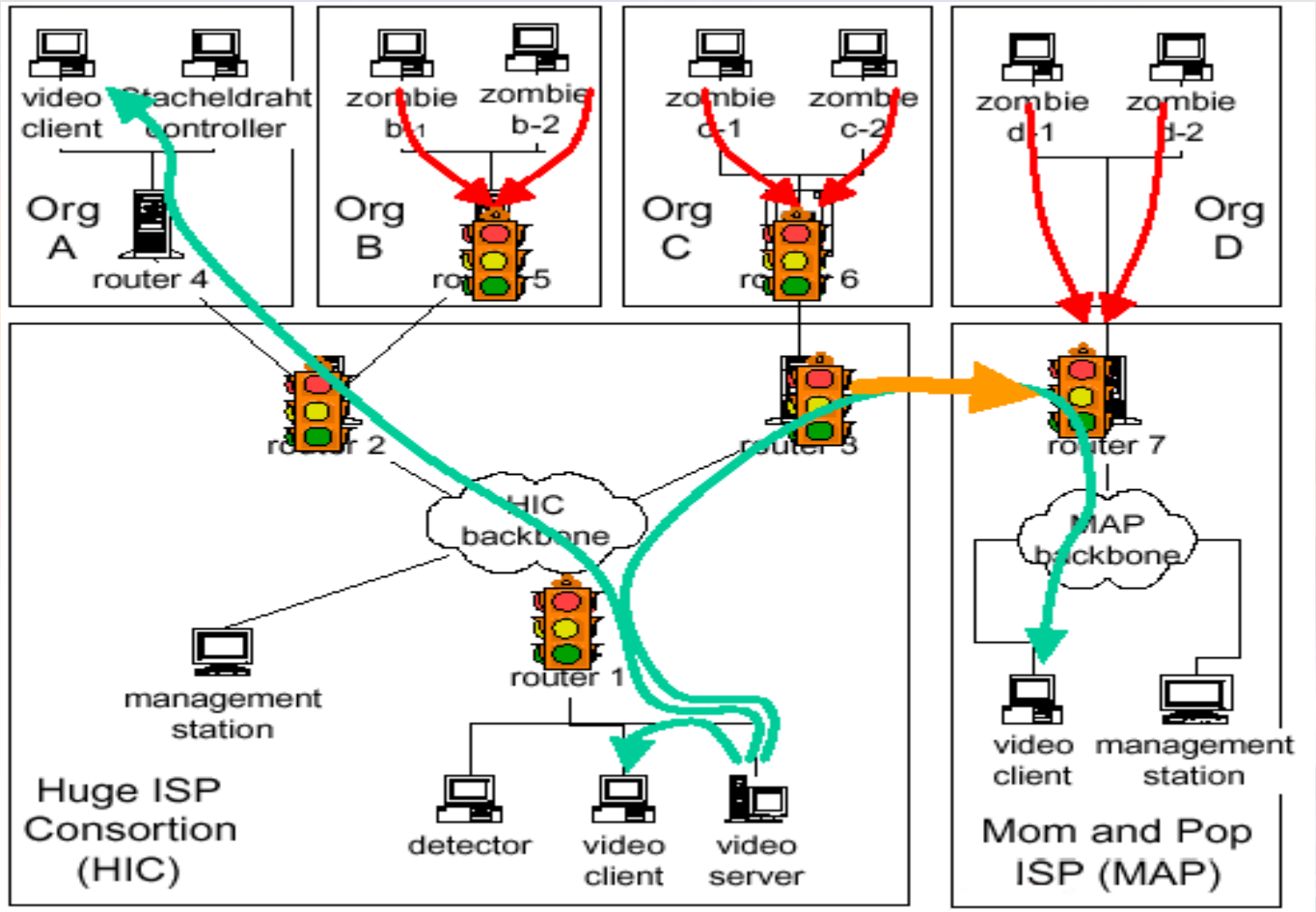
2. 능동형 보안기술

MAP Admin Authorizes HIC Management Control



2. 능동형 보안기술

Active Rate Limiter Permitted to Run

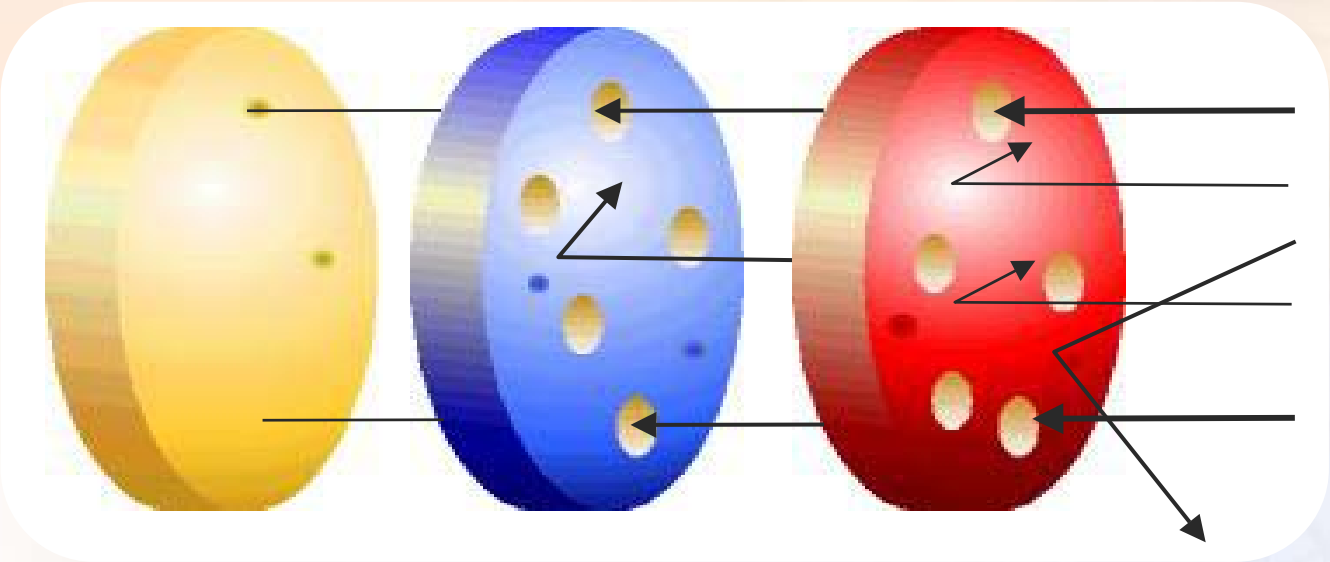


차례

3. DARPA ITO/ISO 보안기술

Layered Defense

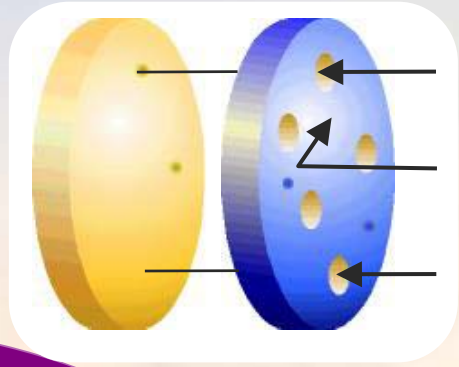
Tolerate Detect Prevent



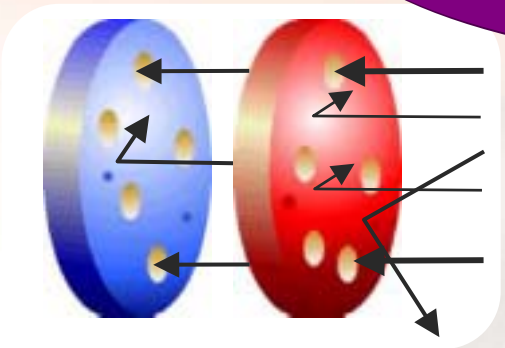
3. DARPA ITO/ISO 보안기술

Roadmap

Inherent Survivability
1999-2003



ISO Info Assurance
1997-2000



Information Survivability
1995-1999

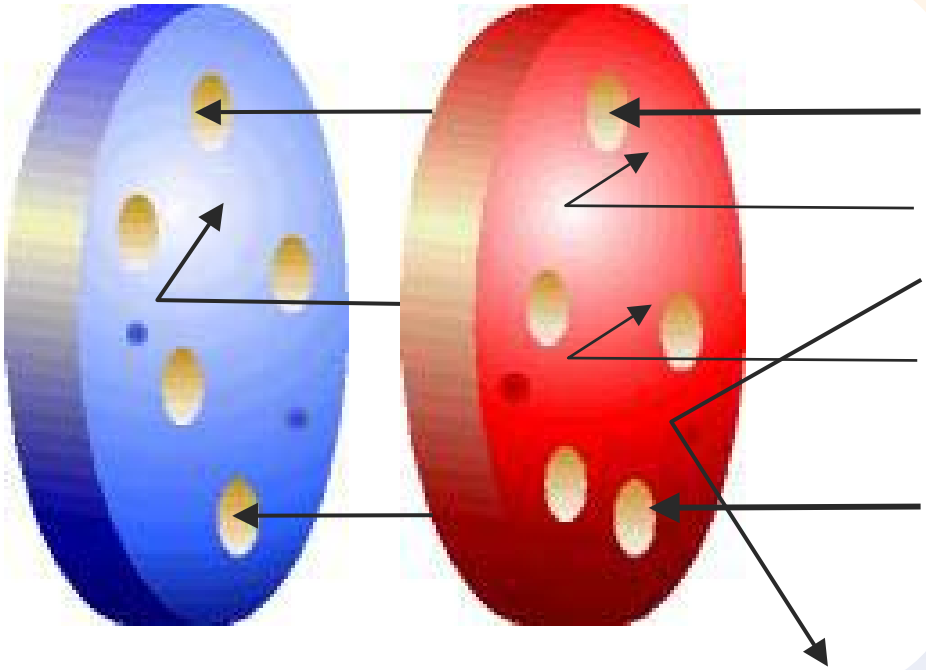
3. DARPA ITO/ISO 보안기술

Accomplishments

Local Detection ***Strong Barriers***

Information Survivability Program

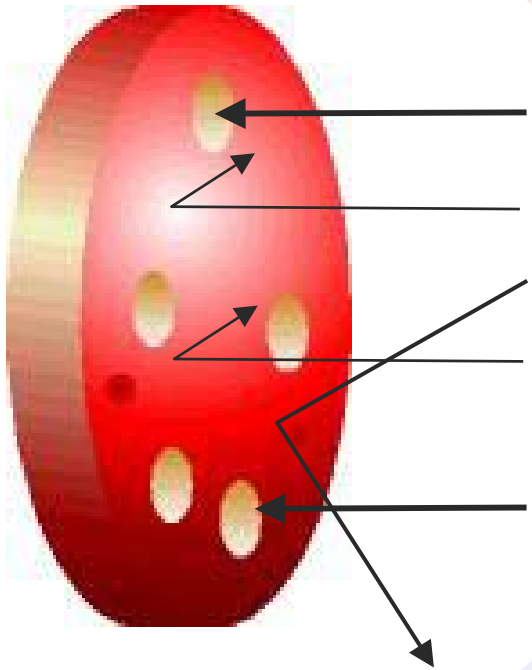
1995-1999



3. DARPA ITO/ISO 보안기술

Strong Barriers

Develop strong barriers to penetration at all system levels



3. DARPA ITO/ISO 보안기술

Network: DNS Security

www.darpa.mil?

Authenticated Name-Address Mappings

(root) says:

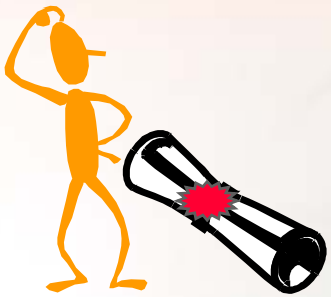
mil is 164.117.176.1

.mil says:

darpa is 192.5.18.99

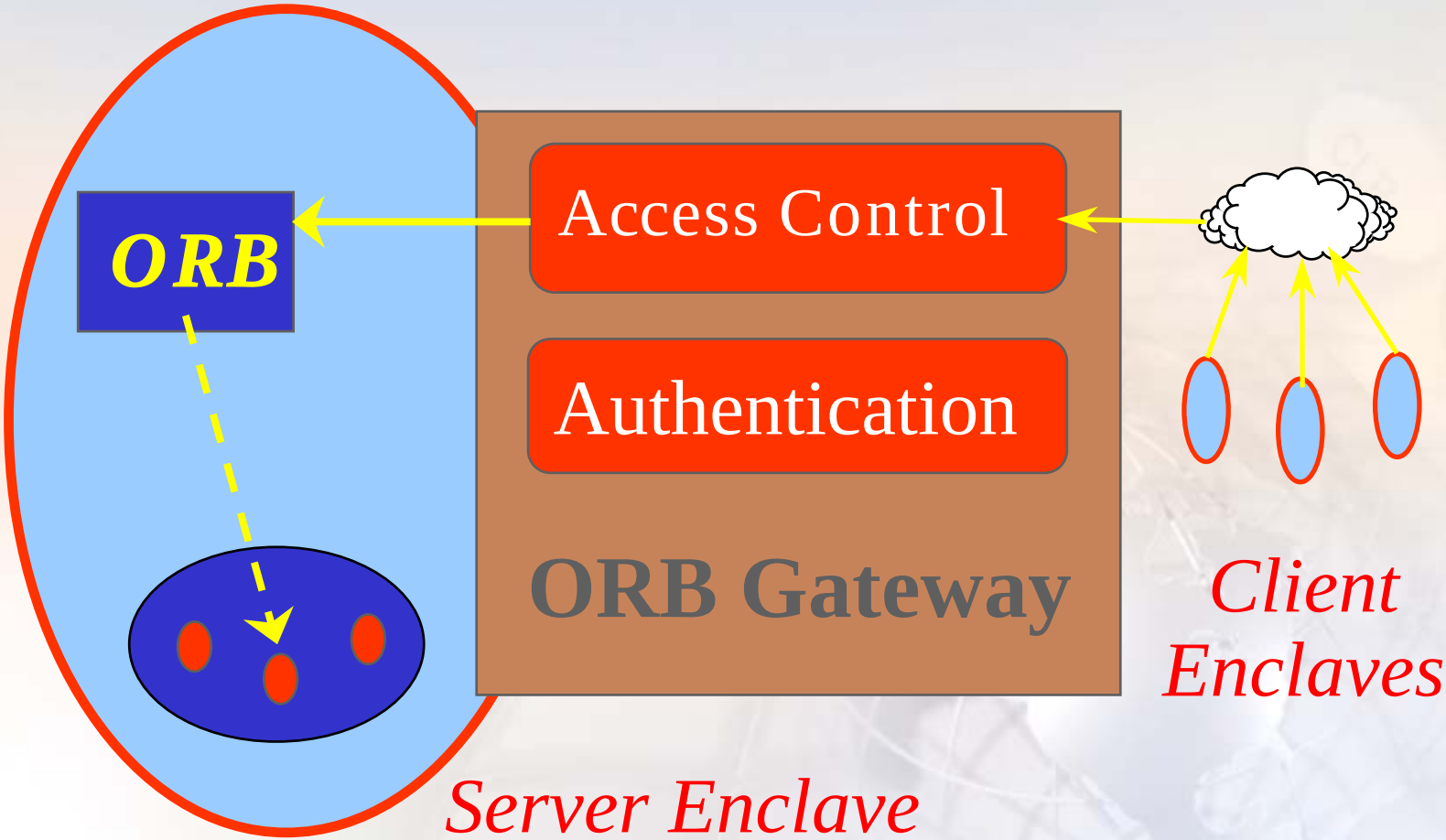
darpa says:

www is 192.5.18.70



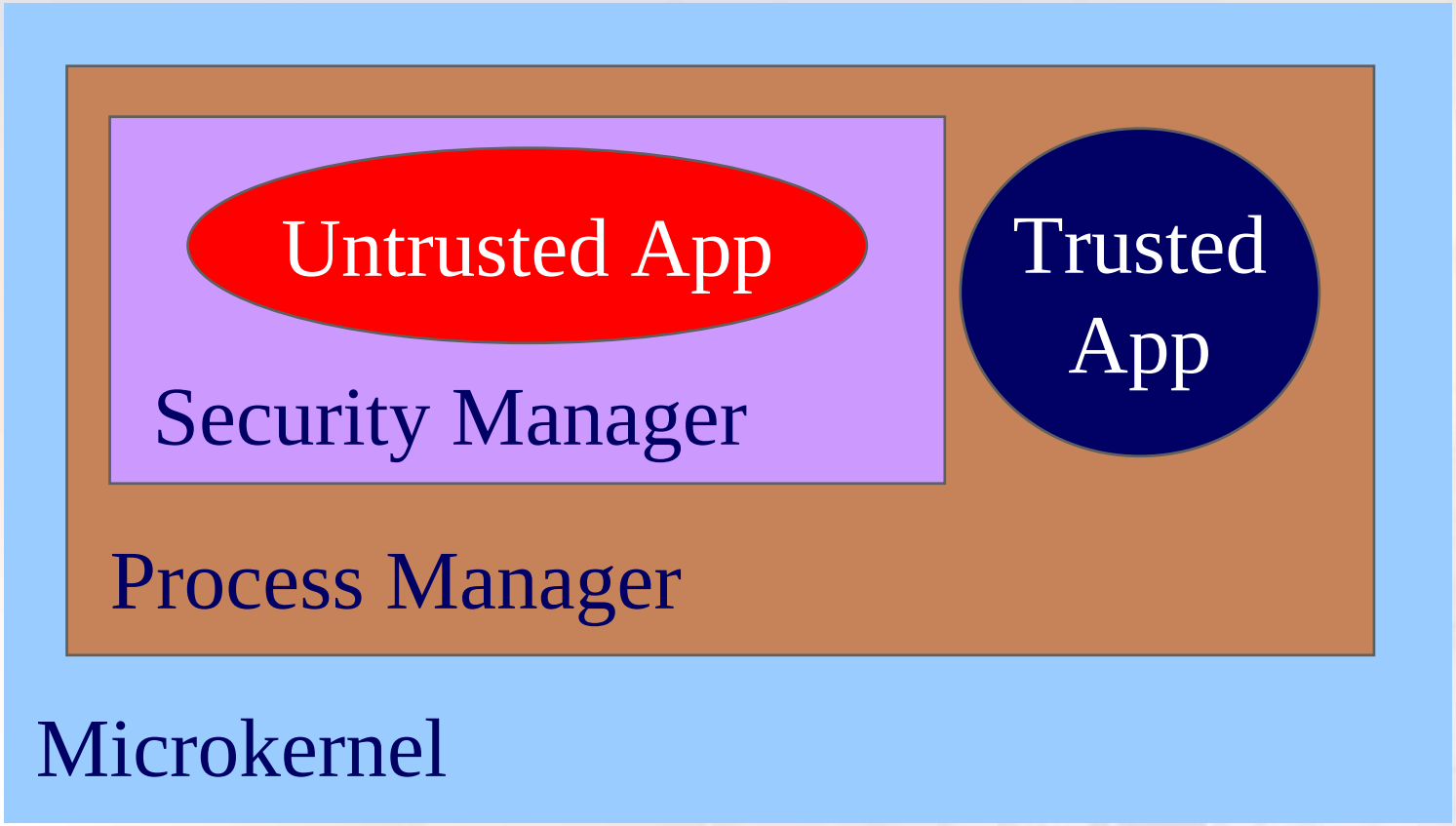
3. DARPA ITO/ISO 보안기술

Middleware: CORBA



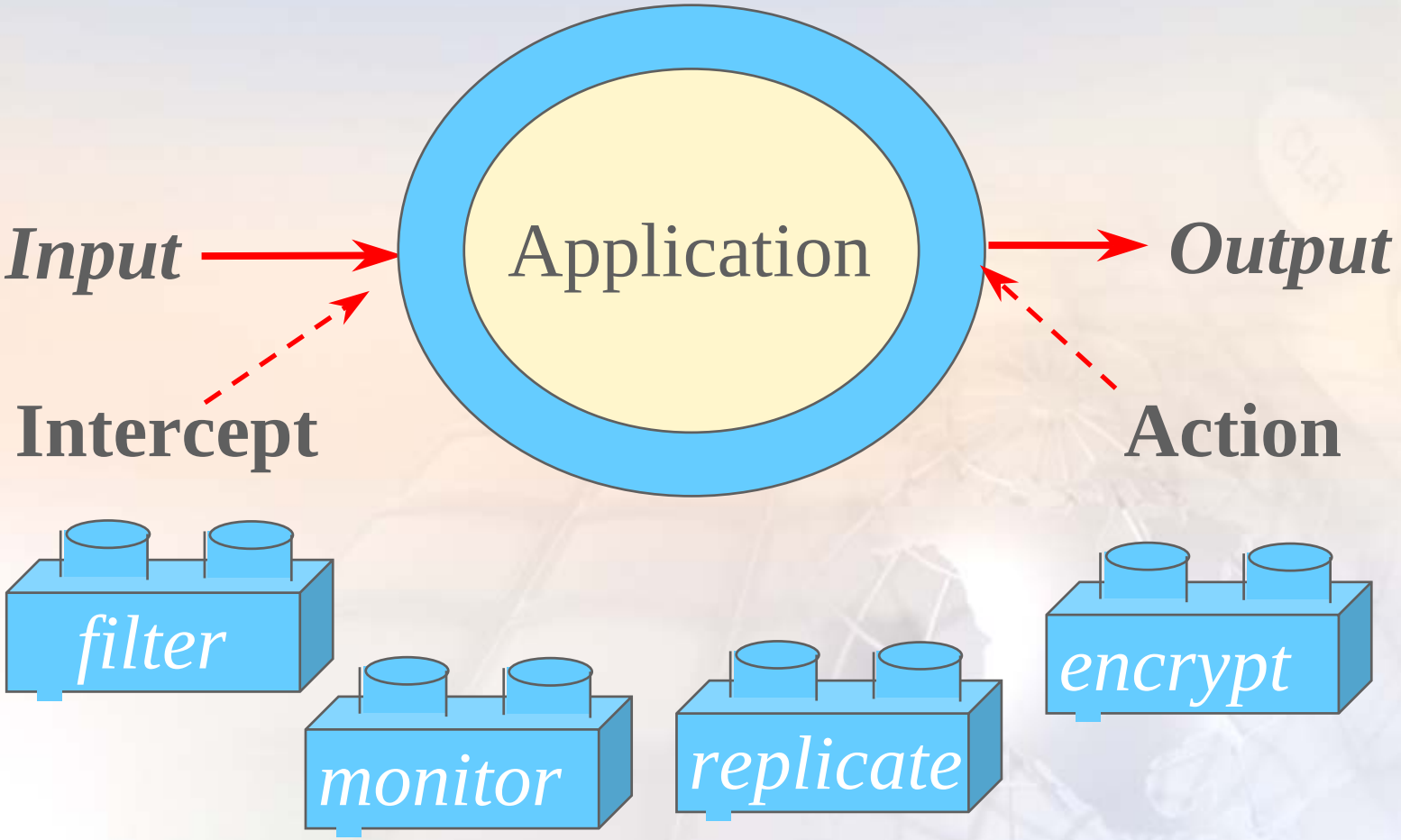
3. DARPA ITO/ISO 보안기술

OS: Nested Processes



3. DARPA ITO/ISO 보안기술

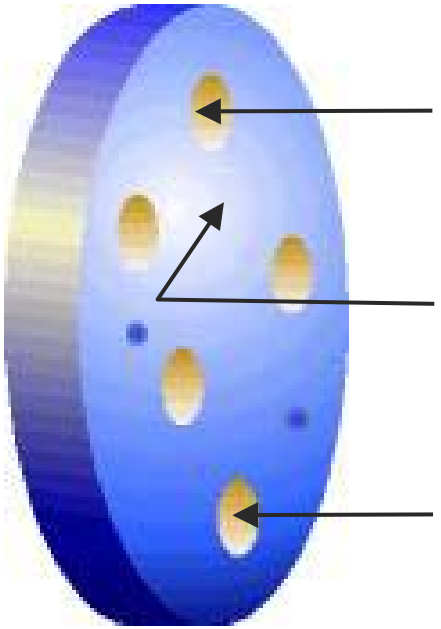
Application: Wrappers



3. DARPA ITO/ISO 보안기술

Local Intrusion Detection

Detect attacks locally with high confidence and low false alarm rate



3. DARPA ITO/ISO 보안기술

Intrusion Detection

State-of-the-Practice

- Pattern matching on known attacks

Program focus

- Statistical Anomaly Detection
- Model-Based Profiles

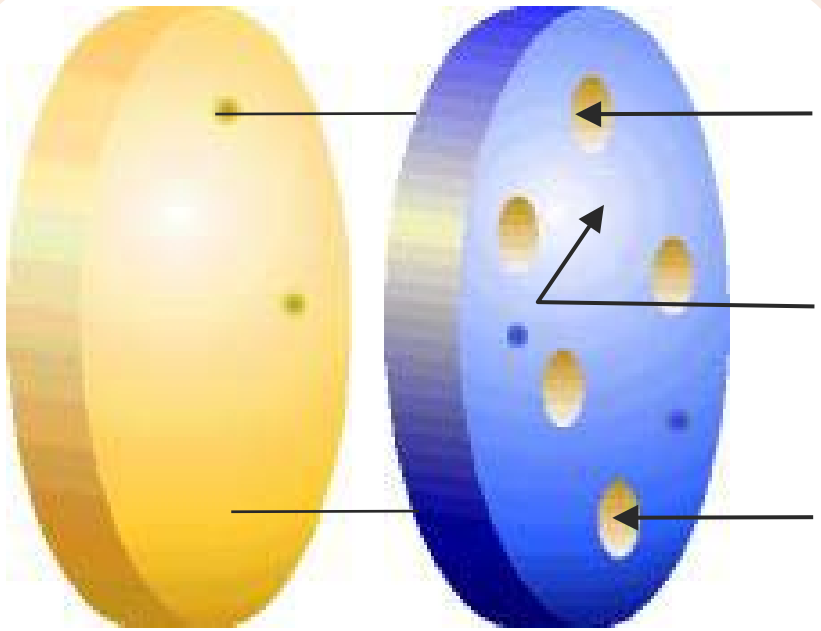
Detect Previously Unknown Attacks

3. DARPA ITO/ISO 보안기술

New Directions

Intrusion Tolerance

Global Detection

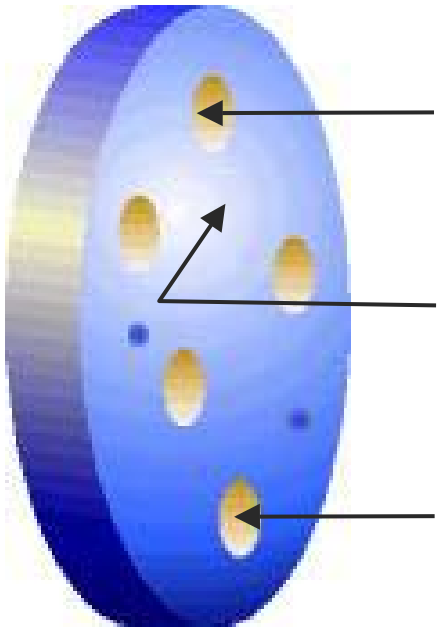


Inherent Survivability Program

1999-2003

3. DARPA ITO/ISO 보안기술

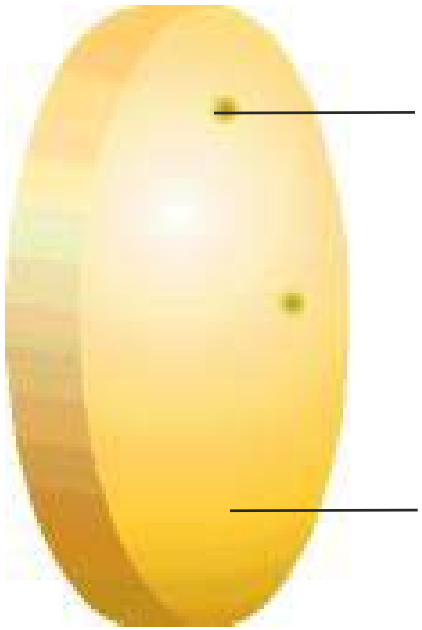
Global Detection



Distinguish events of elevated significance from those of only local interest

3. DARPA ITO/ISO 보안기술

Intrusion Tolerant



Intrusion Tolerant Systems :
Maximize ability to continue critical operations following partial compromise

Intrusion Tolerant Networks :
Maximize residual capacity of network infrastructure following partial compromise

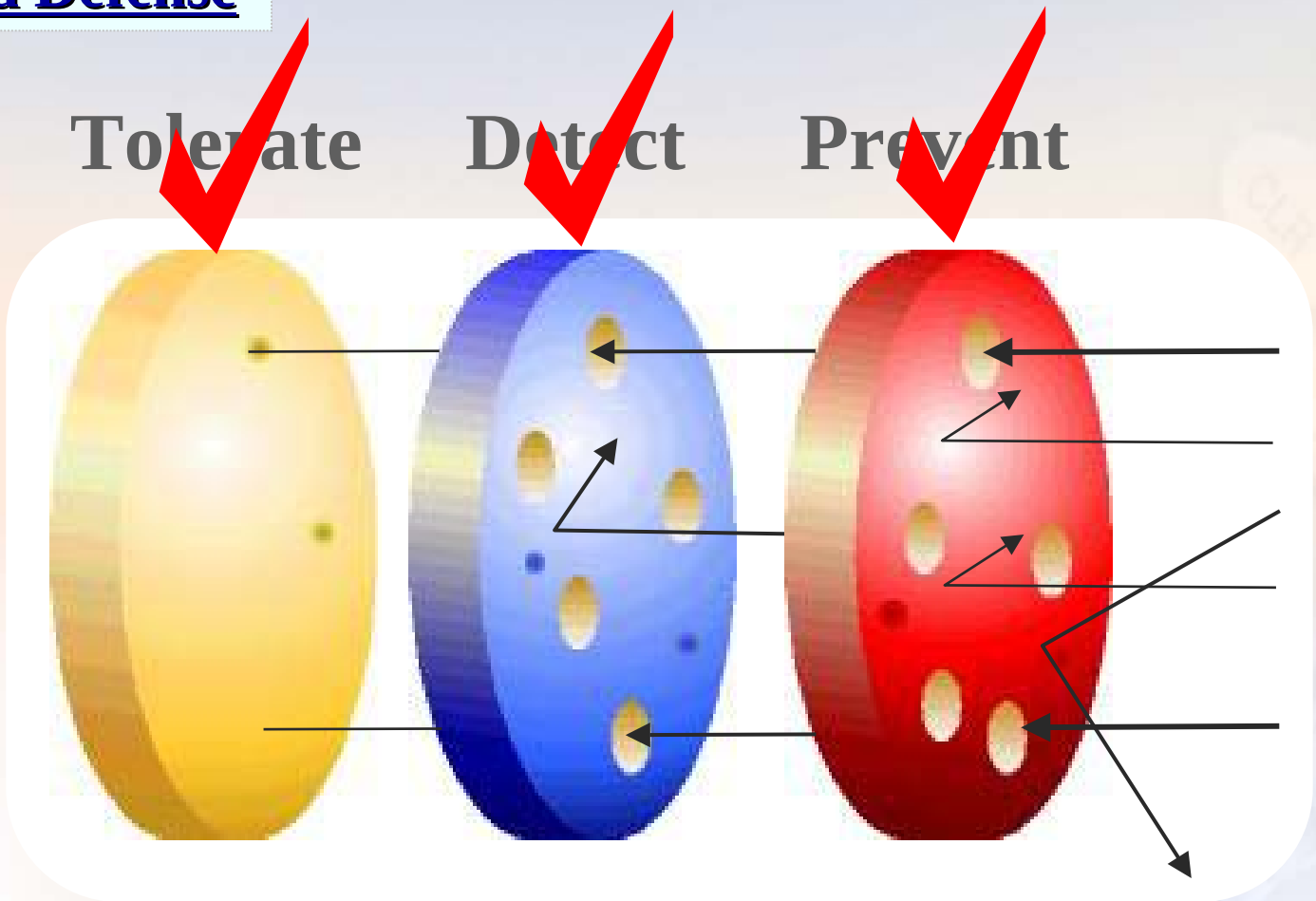
3. DARPA ITO/ISO 보안기술

Tolerance Techniques

- Data Redundancy
- Programs Redundancy
- Hardware Redundancy
- Communication Codes Redundancy
- Information (Analytic) / Design Redundancy
- Temporal Redundancy

3. DARPA ITO/ISO 보안기술

Layered Defense



3. DARPA ITO/ISO 보안기술

Constant Feedback

Change Firewall Rules

Disable Accounts

Retask Sensors

Vulnerability Assessment

Intrusion Detection

HUMINT

Automated Response

Tactical Decisions

Strategic Decisions

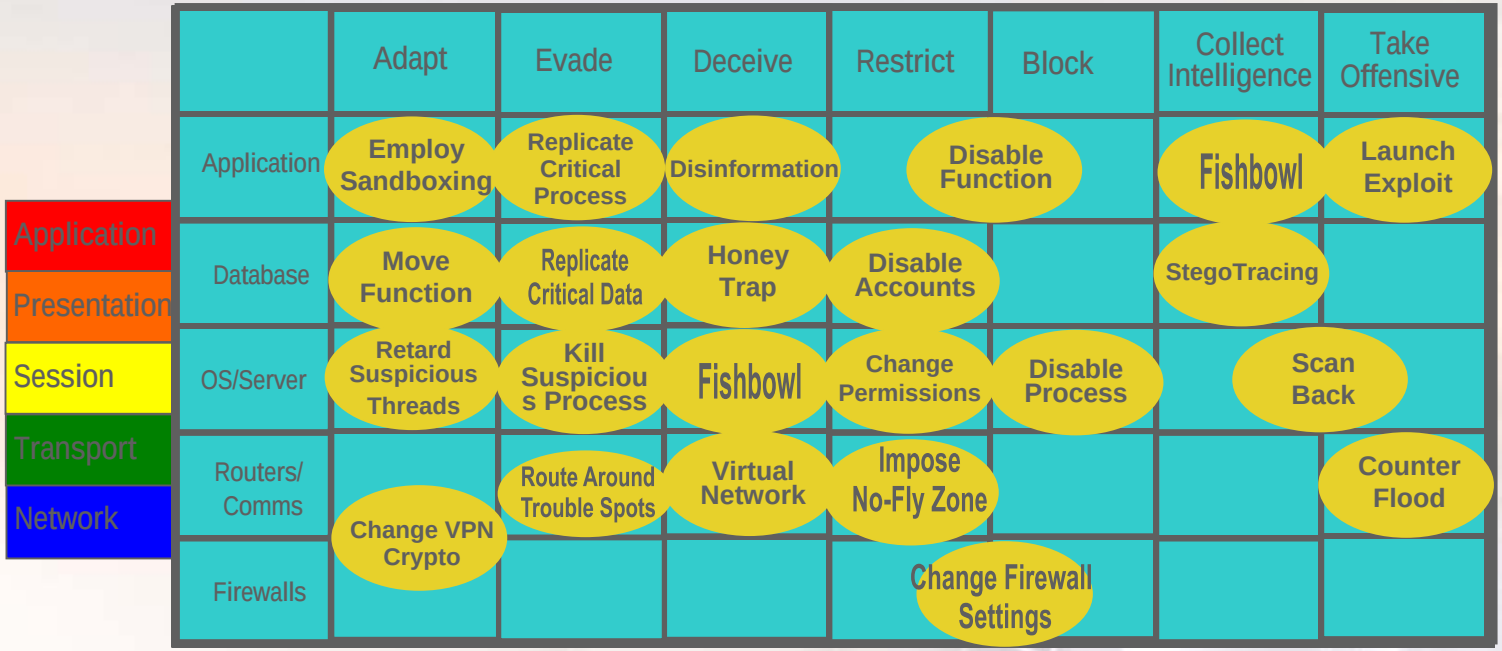
Visualization

Cognitive Science

Correlation and Fusion

3. DARPA ITO/ISO 보안기술

Response & Correction Function



차례

4. 위협 관리 체계 구축

위협 관리 체계의 등장 배경 및 필요성

등장 배경

- 대량 메일의 전송 웜과 백도어 프로그램 등의 전통적인 바이러스와 웜은 보안상 취약한 서비스나 사회공학 등의 보안 정책의 결함을 통해 확산되고 있다.(대표적 사례 BugBear.B)
- 감염된 시스템뿐만 아니라 네트워크 또는 네트워크 서비스에 미치는 파급효과가 엄청난 파괴력을 갖는다.(대표적 사례 SQL Slammer)
- 비정상적인 네트워크 트래픽들이 꾸준히 증가하고 있다.(대표적 사례 TCP window 크기가 55808인 트래픽)
- 새롭고 다양한 기법을 통해 인터넷에서 시스템을 공격하고 제어하는 새로운 방법이 제시되고 있다.

필요성

- 상승하는 위협, 새롭게 활성화된 위협 및 네트워크 이상징후를 조기 탐지 및 대응 수단 필요하다.
- 1.25 대란이 재연되지 않도록, 이상징후 등 위협 발생에 대비한 체계적인 사이버 대응 체계 구축이 요구된다.

4. 위협 관리 체계 구축

위협 관리 체계의 구성 요소

TESS NSS(Network Surveillance System)

이벤트 및 트래픽 분석을 통하여 네트워크 이상징후를 조기 감지하고, 상황변화에 대한 원인과 현상을 직관적으로 파악하고 의사결정수단을 제공하는 Global Detection System 이다.

TESS NTMS(Network Threat Management System)

Global Detection System인 NSS를 중심으로, 조기 예·경보시스템, 침해사고대응시스템, 취약점 DB, Global 조기경보서비스(시만텍 DeepSight) 등으로 구성된 체계적인 사이버 공격 대응 시스템이다.

TESS NSS – 주요 특징 설명

TESS NSS(Network Surveillance System)

특징 1 – TESS NSS는 Global Detection System이다.

- TESS NSS는 **Local Detection과 Global Detection 기능을 동시에 수행한다.**
- 이벤트 통계 및 상관관계 분석을 통해 새롭게 상승하는 중요 이벤트들 식별하고, 발생된 이벤트들의 추이 변화 분석을 통한 상황 변화 및 이상징후를 탐지한다.
- 트래픽 기반의 비정상행위를 탐지한다 (프로파일, 모델에 기초)

Local Detection System	Global Detection System
높은 신뢰성과 낮은 오탐율로 로컬의 공격을 탐지한다.	단순한 지역적인 관심 이벤트들로부터 새롭게 증가하는 중요 이벤트들을 구분한다.
알려진 공격에 대한 패턴 매칭	통계적 또는 모델에 기반, 비정상 행위 탐지

TESS NSS – 주요 특징 설명

TESS NSS(Network Surveillance System)

특징 2 – TESS NSS는 효과적인 네트워크 유해 트래픽 분석 시스템이다.

- TESS NSS는 **Intrusion Detection 과 Network Traffic Monitoring 기능을 동시에 수행한다.**
- 뿐만 아니라, **발생이벤트와 트래픽간의 연관분석을 통해 효과적인 유해 트래픽 제어가 용이하다.**
- 바이러스, 웜 등의 유해 트래픽으로 인한 네트워크 상태변화에 대한 원인과 그 영향을 정확히 판단하고, 대응 방안을 수립할 수 있는 의사결정수단을 제공하다.

Intrusion Detection System	Network Monitoring System
패턴 기반의 침입 탐지를 통해, 사건 발생의 정확한 원인 파악이 용이하다.	바이러스, 웜 등 유해 트래픽으로 인한 네트워크 상태 변화에 대한 정확한 원인 파악이 어렵다.
발생 이벤트로 인한 네트워크 영향 및 현상 파악이 어렵다.	네트워크의 이상징후 및 상태 파악이 용이하다.

TESS NSS – 주요 특징 설명

TESS NSS(Network Surveillance System)

특징 3 – TESS NSS는 강력한 Visualization 기능을 제공한다.

- 이벤트 추이 분석, 네트워크 추이 분석, 이벤트간 상관관계 분석 이벤트와 트래픽간 상관관계 분석을 위한 GUI 제공
- 전반적인 침입 및 네트워크 상황을 직관적으로 파악할 수 있는 GUI 제공
- 네트워크 동향 및 분석을 위한 프리젠테이션 및 맞춤 보고서 제공
  (자동 보고서 생성 및 보고서 생성시 자동 메일 전송 기능 등)

TESS NSS – 주요 기능 설명

- IP기반/IP 이외의 모든 프로토콜 및 서비스에 대한 트래픽 분류 및 통계 정보 유지
- 통계적 기법 및 Drill-down 방식을 이용한 이벤트 상관관계 분석
- 프로파일 기반의 비정상 행위(네트워크 이상징후) 탐지
- 이상징후 탐지 및 분석 - 알려지지 않은 위협으로 인한 네트워크 이상징후 발견 시 트래픽 로깅 및 트래픽 정보 분석
- 세션 통계 분석 및 모니터링 - 스팸 메일 릴레이 또는 부당한 서비스 사용 시스템 검출에 유용함
- 보고서 작성기 - 반 자동 보고서 및 예약을 통한 자동 보고서 생성
- 보고서 - 예약을 통한 자동을 생성 및 메일 전송된 일간 경향 분석 보고서

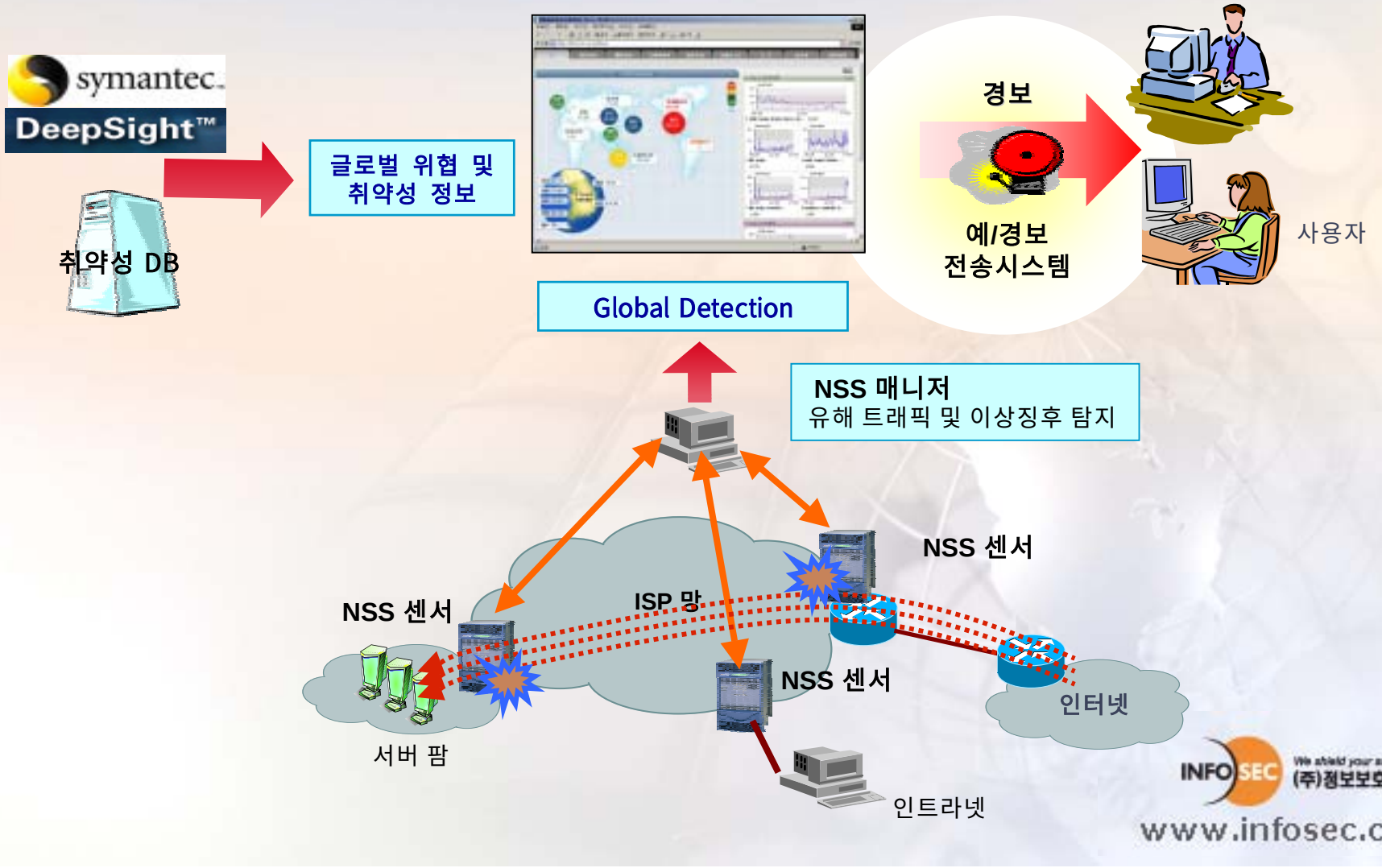
TESS NTMS(Network Threat Management System)

시스템 구성

- NSS(Global Detection & Network Anomaly Detection System)
- 조기 예/경보 시스템(Early Warning & Alert System)
- 사고 대응 시스템(Response System)
- 취약점 DB(VA DBMS)
- Symantec DeepSight TMS(글로벌 조기경보 및 취약성 정보제공 서비스)

TESS NTMS

TESS NTMS 개념도



INFOSEC We shield your success (주)정보보호기술

www.infosec.co.kr

TESS NTMS – 주요 기능 설명

- 종합 상황도 – 현재 네트워크 상태, 발생 이벤트 추이, 이벤트 발생 지역 분포 등 종합적인 요약
- 탐지 분석 – 이벤트 발생 건수, 트래픽 영향 등의 기준에 타른 Top N 이벤트 분석
- 탐지 분석 –Top N 이벤트의 추이 분석
- 트래픽 분석 – 프로토콜 별, 서비스별, 프래임 사이즈 별 통계 및 추이 분석
- 사고 대응 – 특정 이벤트들을 발생시키는 유해호스트를 블랙리스트로 관리 및 적당한 대응 조치
- 예/경보 – 네트워크 프로파일에 기반 한 이상징후 또는 급격한 트래픽 변화 등이 발생시 예/경보 발령

NTMS 구축사례 1

데이콤 국가망 G/W 보안을 위한 NTMS

구성

- Global Detection System – NSS 센서(4) 및 NSS 매니저
- 예/경보 전송 시스템
- 사고 대응 시스템
- 취약성 DB & 시만텍 DeepSight 서비스
- 위협관리 웹 서버 시스템

특징

- 신속한 예/경보 발령을 위해 E-Mail 뿐만 아니라 SMS 문자서비스를 포함한 NTMS 첫 구축사례
- 활성화된 위협에 대해 신속한 대처를 위해, 내부망에서 추출된 정보뿐아니라, 해외에서 발생하는 이벤트 정보수집을 위해 시만텍 DeepSight 서비스와 연동

NTMS 구축사례 1 – Sqlexp worm(Slammer) 대응 사례

Sqlexp worm(Slammer) 대응 사례 요약

Sqlexp worm(Slammer) 란?

- 네트워크 서비스의 영향력을 고려하였을 때 가장 의미 있는 네트워크 관련 이벤트는 1.25 대란을 일으킨 SQL Slammer로 불리는 SQLExp 웜이다.
- SQLExp 웜은 매우 빠르게 전파되어 은행 자동 출납기나 보통 인터넷 기반의 악성코드에 별 영향을 받지 않던 네트워크까지 혼란에 빠지게 하였다.
- 이 웜의 영향은 3일간 지속되었으며, ISP 업체의 강력한 UDP/1434 포트의 필터링으로 인하여 영향력이 줄어들었다.

대응 요약

- 패치되지 않은 서버가 재감염을 통해서 SQLExp 웜을 활성화 시킴 되는 경우가 산발적으로 발생한다.
- 한 두개의 서버에서 SQLExp 웜이 활성화되어도 그 영향력은 상당하다.
- 9월 23일, 11월 4일 두 차례에 걸쳐 다시 활성화된 SQLExp웜을 탐지하고, 근원지에 대해 망접근 차단 및 사용기관 관리자에 대해 경고 메일 전송
- 사건발생 10여 분만에 탐지 및 대응 조치 완료

NCA 국제IX망의 안전한 운영을 위한 NTMS

구성

- Global Detection System – NSS 센서(10) 및 NSS 매니저
- 예/경보 전송 시스템
- 사고 대응 시스템
- 위협관리 웹 서버 시스템

특징

- 전체 10개의 NSS 센서 중 2개의 센서를 스팸 분석 전용 센서로 활용
- 웜, 바이러스 및 침입 이벤트들과 이에 기이한 유해 트래픽을 정확히 산정 가능
- 전체 트래픽 대비 유해 트래픽 측정

스팸 릴레이 탐지 및 스팸 트래픽 산출 사례 요약

스팸 릴레이 란?

- 인터넷에 노출된 무 방비하게 노출된 국내 서버들이 행킹에 의해 스팸 릴레이 악용되는 사례가 많이 발생하고 있다.
- 최근 중국을 비롯한 해외 해커들에 의해 스팸 릴레이로 악용되어 해외 관문국에 전송되는 메일의 상당수가 스팸 메일로로 추정되고 있다.

스팸 릴레이 탐지 및 스팸 트래픽 산출 요약

- 통계적 기법 및 패턴 분석 방법을 이용한 스팸 릴레이 예상 후보 탐지
- 스팸 릴레이 예상 후보들이 전송하는 메일 헤더 분석
- 스팸 릴레이로 확인된 서버 등록 및 이들에서 발생된 메일 트래픽 산출