# 엔터프라이즈 네트워크에서 인터넷 웜의 실시간 탐지 방법

포항공과대학교 정보통신대학원
정보통신학과

분산시스템과 네트워크관리 연구실

2005년 12월21일

조 룡권
rone@postech.ac.kr

POSTECH
DP&NM Lab

# 목차

- 서론
- 연구의 필요성과 목표
- 관련연구
- 인터넷 웜 탐지 알고리즘
- 웜 트래픽 발생 툴
- 알고리즘의 검증
- POSTECH 네트워크에서의 탐지결과 분석
- 결론

# 서론(1)

- 인터넷 웜은 전파속도가 빠르고 네트워크의 마비를 일으킴
  - 1988년 Morris 웜의 탄생
  - 2001년 CodeRed 웜의 대량 전파
  - 2003년 Slammer웜의 인터넷 대란

- 인터넷 웜의 정의
  - “네트워크를 통해 사용자의 개입이 없이 스스로 복사 전파하면서 취약점이 있는 서비스를 공격하는 악성코드”

# 서론(2)

- 인터넷 웜의 트래픽 특성
  - 프로토클: TCP/UDP
  - 취약점이용: Destination Port
  - 스캐닝: 순차적/랜덤
  - 타겟 선정: 전역/부분/로컬
  - 스캐닝속도

- 탐지방법의 연구동향
  - 인터넷 전역에서의 탐지
  - Signature를 이용한 IDS 시스템
  - 엔터프라이즈 네트워크에서의 탐지

# 연구의 필요성과 목표

- 연구의 필요성:
  - 글로벌 네트워크가 아닌 엔터프라이즈 네트워크에서 실시간 탐지가 필요하다.
  - Signature에 근거한 방법이 아닌 Traffic Behavior에 근거한 탐지하는 방법이 필요하다.

- 연구의 목표:
  - 엔터프라이즈 네트워크에서 실시간으로 Traffic Behavior에 근거한 인터넷 웜을 탐지하는 방법을 제시한다.

- 연구의 내용:
  - 엔터프라이즈 네트워크에 적합한 traffic behavior에 근거한 실시간 탐지 방법을 제안
  - 탐지방법의 검증을 위하여 인터넷 웜 트래픽 Generator를 개발
  - 탐지 알고리즘을 검증 및 실제 엔터프라이즈 네트워크에 구현하고 탐지결과의 분석

# 관련연구(1)

- Signature에 의한 탐지 방법
  - Misuse IDS (signature based detection)
    - 새로운 웜에 대한 탐지가 불가능하다.
    - Signature 대조 과정이 많은 처리시간을 요한다.
    - Snort, Bro
  - Upgraded misuse IDS
    - 2004, Bharath, “Design of a System for Real-Time Worm Detection”, IEEE symposium of High Performance Interconnections 2004
    - Signature의 Update로 웜의 signature확보가 가능하다.
- 실 시간 탐지 방법
  - 인터넷 웜이 발생한 후 짧은 시간 내에 탐지
  - 짧은 시간 내에 대량의 트래픽을 처리

# 관련연구(2)

- 인터넷 전역을 대상으로 하는 탐지방법
  - 수학적 모델링 방법
    - 2003, C.C.Zou, “Monitoring and Early Warning for Internet Worms,” ACM Conference on Computer and Communications Security (CCS 03)
    - 2003, Chen, “Modeling the Spread of Active Worms” WORM 2003 on Network Security
  - ICMP type 3 메시지를 이용한 탐지방법
    - 2002,George Bakos, “Early Detection of Internet Worm Activity by Metering ICMP Destination Unreachable Messages,” The International Society for Optical Engineering (SPIE)
  - 대형 보안업체의 웜 로그를 수집하는 방법
    - Symantec, CAIDA 같은 보안 관련 연구단체에서 전 세계 웜의 로그를 수집하여 분석하는 방법

# 관련연구(3)

- 엔터프라이 네트워크를 대상으로 하는 탐지방법
  - Destination-Source Correlation 알고리즘
    - 2004, Gu, “Worm Detection, Early Warning and Response Based on Local Victim Information”, Annual Computer Security Applications Conference (ACSAC 2004)
  - Honey-Pot을 이용한 탐지방법
    - 2004, Christian Kreibich, Jon Crowcroft, “Honeycomb-Creating Intrusion Detection Signatures Using Honeypots,” ACM SIGCOMM Computer Communications 2004

# 인터넷 웜 탐지 알고리즘(1)

- 취약점이 존재하는 서비스(목적지 포트)

- 스캐닝 속도(한 호스트에서 대량의 스캐닝 트래픽 발생)

  Suspicious List:

  – **Scanning Rate**이 임계 치 값을 넘는 **3-tuple flow**

  – 3-tuple flow: 같은 Destination Port, Source Host, Protocol을 가지고 있는 패킷의 집합

- 목적지 주소의 분포 (랜덤/순차적)

  Sequential Worm:

  – 순차적: 목적지 주소가 순차적이다

  Random Worm:

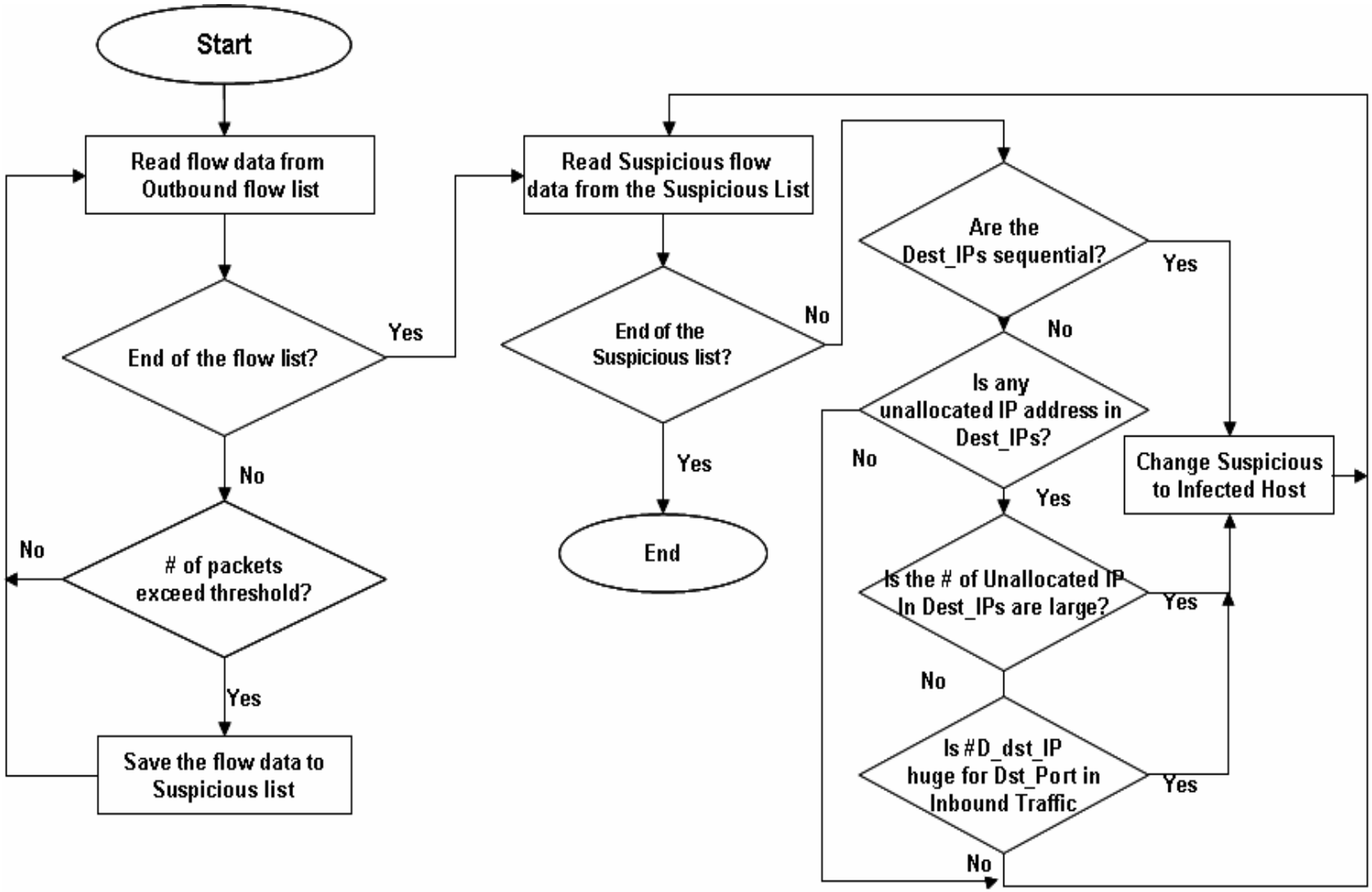
  – 랜덤: 할당되지 않는 **IP** 주소 에 대한 스캐닝(IANA IPv4 Allocation Table 사용)

- 높은 목적지주소의 분산도

  – 해당 포트의 목적지 주소의 분산도가 높다

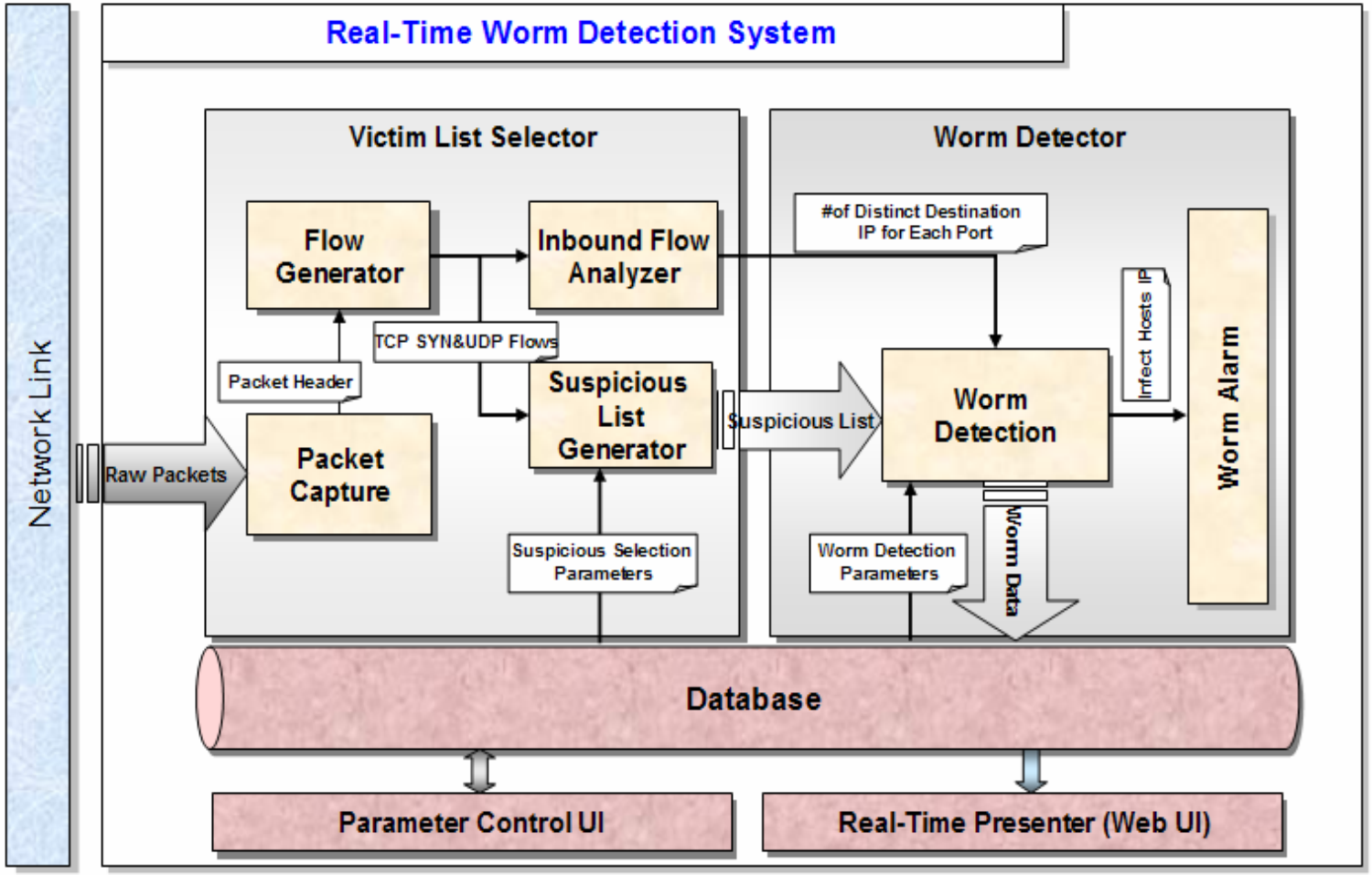
  – Ingress 트래픽에서 해당 목적지 포트의 목적지주소의 분산도 이용

# 인터넷 웜 탐지 알고리즘(2)



# 인터넷 웜 탐지 알고리즘(3)

- 시스템의 구조

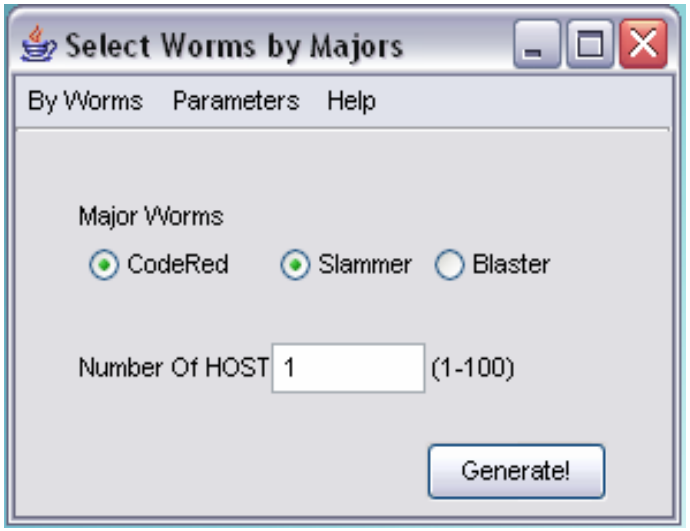


# 웜 트래픽 발생 툴(1)

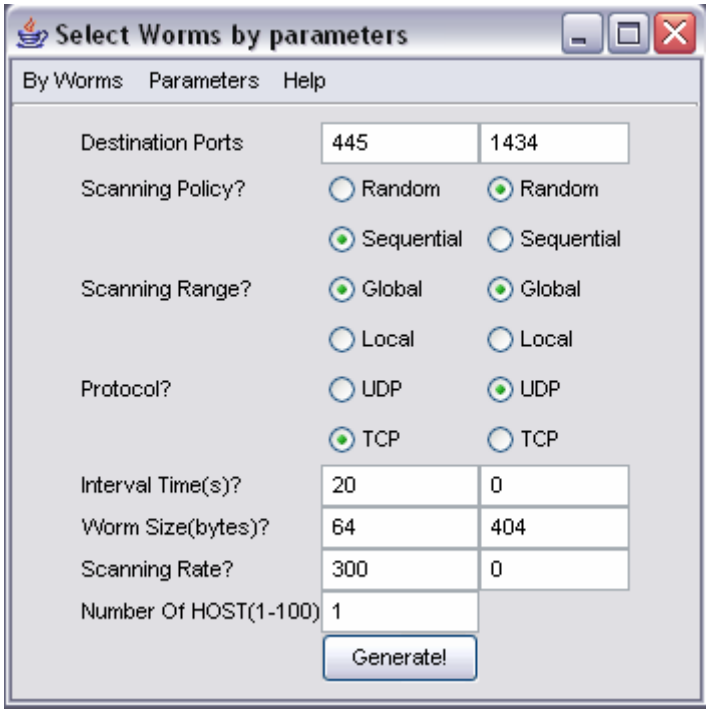
- WTG 개발의 필요성
  - 인터넷 웜의 특성파악을 위해 필요하다.
    - 실제 인터넷 웜 트래픽을 확보하기 어렵다.
    - Simulate을 통한 방법의 한계
  - IDS나 Firewall 의 검증에 필요하다.
    - 제안한 IDS 알고리즘 검증
    - Penetration Testing

# 웜 트래픽 발생 툴(2)

- User Friendly Interface
  - Java Swing based




Major Worm 의 선택




패러미터에 의한 선택

# 웜 트래픽 발생 툴(3)

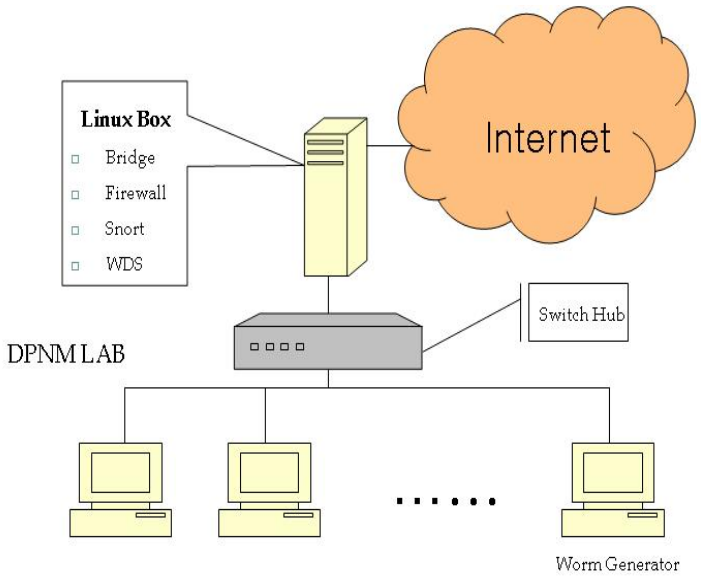
- Parameter Aggregation
  - Major Worms
    - Slammer Worm:
      - {UDP 1434, Global Random, Bandwidth-limited, No interval time}
    - CodeRed:
      - {TCP 80, Global Random, 300 or 600 packets/interval , 21s interval}
    - Blaster:
      - {TCP 135, Local Sequential, Up to 300 packets/interval, 20s interval}
  - Parameters
    - Protocol (TCP/UDP)
    - Destination Ports
    - Scanning Rate
    - Scanning Property (Random/Sequential)
    - Scanning Targets (Global/Local)
    - Number of host infected (Thread)

- Traffic Generation
  - Destination IP Generation
  - Packet manipulation
    - IP header /TCP/ UDP 패킷
  - Send Packets (RAW Socket)

# 알고리즘의 검증(1)

- 실험환경
  - Worm Detection System
  - Worm Traffic Generator
  - Firewall
  - Bridge

- 검증에 사용된 트래픽
  - Global-Random Scanning Traffic
  - Global-Sequential Scanning Traffic
  - Local Random/Sequential Scanning Traffic



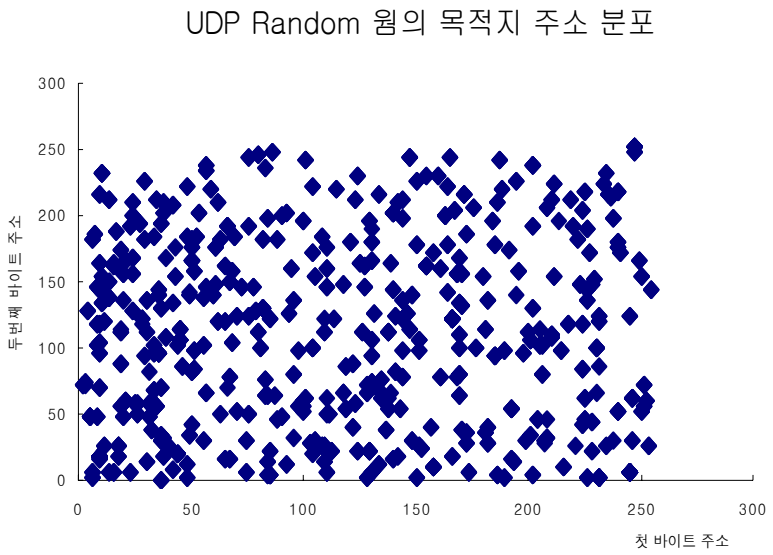

DPNM 연구실에 구축한 실험환경

# 알고리즘의 검증(2)

- Global-Random 웜 트래픽의 탐지
  - UDP-1434-Random-Global-unlimited 웜 트래픽
    - 2005년 12월 17일 12:23분
    - WDS 탐지결과

| Prot | Port | DstIP | SrcIP | SrcPort |
|---|---|---|---|---|
| 17 | 1434 | 212.160.186.4 | 141.223.82.32 | 56815 |
| 17 | 1434 | 221.232.158.10 | 141.223.82.32 | 55152 |
| 17 | 1434 | 218.247.37.130 | 141.223.82.32 | 35420 |
| 17 | 1434 | 220.192.67.78 | 141.223.82.32 | 31036 |
| 17 | 1434 | 130.89.160.231 | 141.223.82.32 | 36701 |
| 17 | 1434 | 67.173.215.99 | 141.223.82.32 | 45208 |
| 17 | 1434 | 222.225.28.123 | 141.223.82.32 | 22423 |
| 17 | 1434 | 85.228.71.53 | 141.223.82.32 | 56451 |
| 17 | 1434 | 220.129.65.121 | 141.223.82.32 | 53726 |
| 17 | 1434 | 85.235.228.44 | 141.223.82.32 | 35297 |
| 17 | 1434 | 80.51.234.224 | 141.223.82.32 | 52446 |
| 17 | 1434 | 218.247.37.194 | 141.223.82.32 | 60362 |
| 17 | 1434 | 82.148.37.30 | 141.223.82.32 | 34198 |
| 17 | 1434 | 196.203.63.182 | 141.223.82.32 | 1214 |
| 17 | 1434 | 218.166.176.207 | 141.223.82.32 | 9374 |
| 17 | 1434 | 85.166.153.24 | 141.223.82.32 | 41198 |

WDS에서 수집된 웜 트래픽

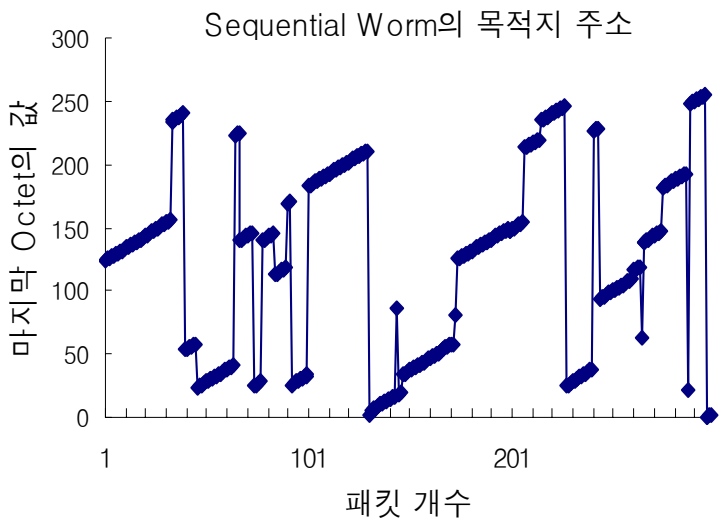


# 알고리즘의 검증(3)

- Global-Sequential 웜의 탐지
  - TCP-SYN-Sequential-Global-20s Interval Scanning
    - 2005년 12월 17일 1시 37분

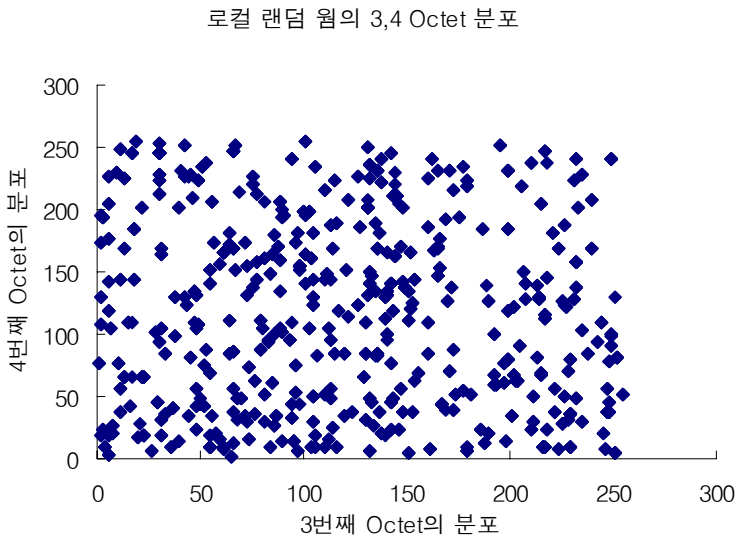
| Prot | Port | DstIP | SrcIP | SrcPort |
|---|---|---|---|---|
| 6 | 445 | 68.91.68.94 | 141.223.82.32 | 24368 |
| 6 | 445 | 68.91.68.95 | 141.223.82.32 | 24624 |
| 6 | 445 | 68.91.68.96 | 141.223.82.32 | 24880 |
| 6 | 445 | 68.91.68.97 | 141.223.82.32 | 25136 |
| 6 | 445 | 68.91.68.98 | 141.223.82.32 | 25392 |
| 6 | 445 | 68.91.68.99 | 141.223.82.32 | 25648 |
| 6 | 445 | 68.91.68.100 | 141.223.82.32 | 25904 |
| 6 | 445 | 68.91.68.101 | 141.223.82.32 | 26160 |
| 6 | 445 | 68.91.68.102 | 141.223.82.32 | 26416 |
| 6 | 445 | 68.91.68.103 | 141.223.82.32 | 26672 |
| 6 | 445 | 68.91.68.104 | 141.223.82.32 | 26928 |
| 6 | 445 | 68.91.68.105 | 141.223.82.32 | 27184 |
| 6 | 445 | 68.91.68.106 | 141.223.82.32 | 27440 |
| 6 | 445 | 68.91.68.107 | 141.223.82.32 | 27696 |
| 6 | 445 | 68.91.68.108 | 141.223.82.32 | 27952 |

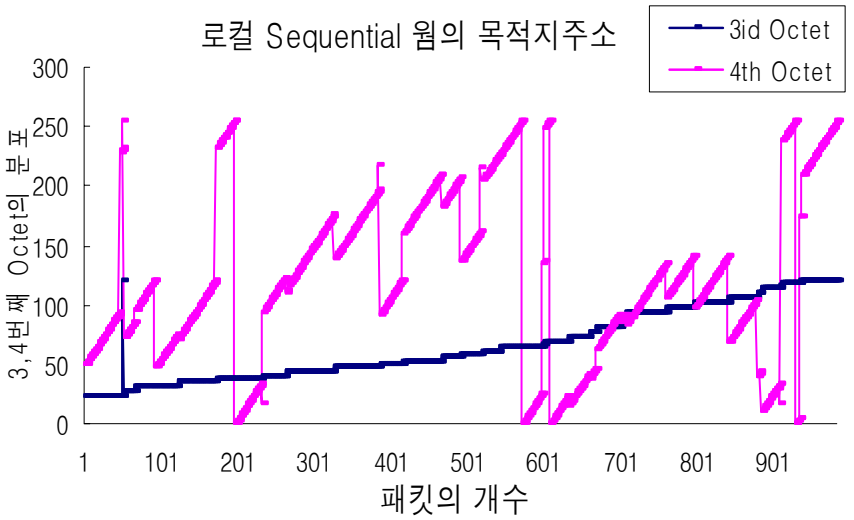
WDS에서 수집된 Sequential 웜 트래픽



# 알고리즘의 검증(4)

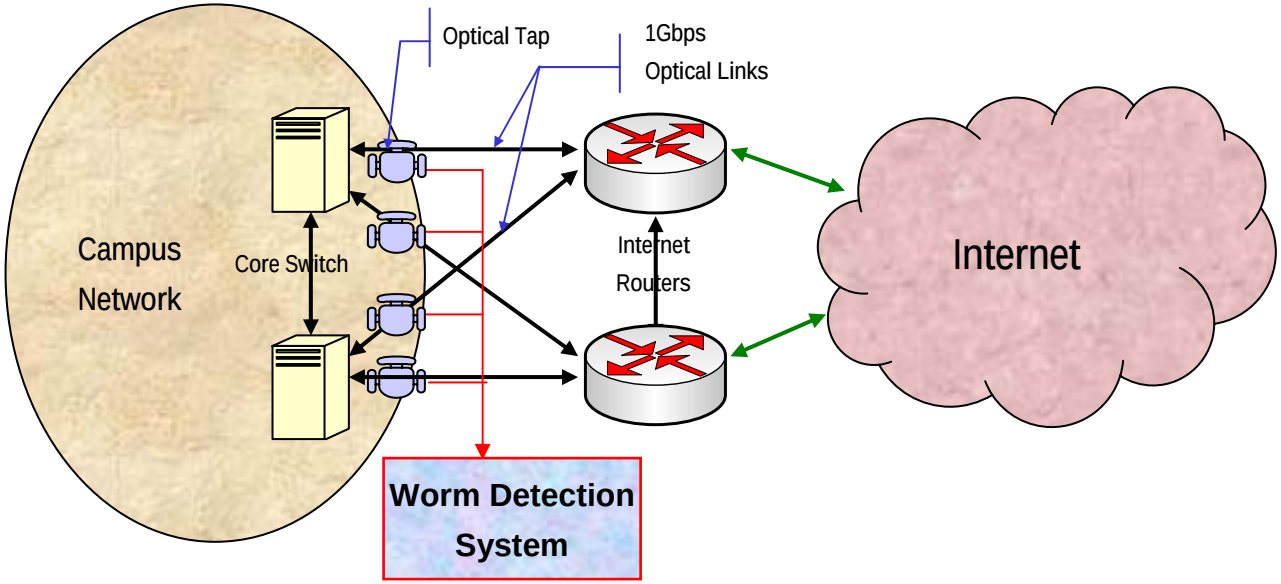
- Local Random/Sequential 웜 트래픽 탐지
  - 2005년 12월 17일 04:31, 04:33



# POSTECH 네트워크에서의 탐지환경

- 트래픽의 수집과 웜 탐지 시스템(WDS)



# POSTECH 네트워크에서의 탐지결과(1)

- 2005년 12월 20일 21:00에 탐지된 Suspicious List
- 20개의 Suspicious hosts와 6개의 Suspicious ports
- 1개의 웜에 감염된 호스트

| | | |
|---|---|---|
| #of Suspicious Host | 20 | Analyzing Time <<2005.12.20 09:00>> |
| #of Sequential Worm | 1 | |
| #of Other Worm | 0 | |

| No. | Protocol | Dest Port | Packets | Syn Pakcets | #of Victims | #of Sequential | #of Worm |
|---|---|---|---|---|---|---|---|
| 0 | UDP | 5445 | 1965 | 0 | 1 | 1 | 0 |
| 1 | TCP | 25 | 2205 | 2205 | 1 | 0 | 0 |
| 2 | TCP | 80 | 5668 | 5668 | 15 | 0 | 0 |
| 3 | UDP | 3309 | 3496 | 0 | 1 | 0 | 0 |
| 4 | UDP | 10025 | 1987 | 0 | 1 | 0 | 0 |
| 5 | UDP | 54171 | 1495 | 0 | 1 | 0 | 0 |

# POSTECH 네트워크에서의 탐지결과(2)

– 인터넷 웜에 감염된 호스트는 UDP 5445포트로 1965개의 순차적 스캐닝 패킷을 발생하였다.

| Time | Destinaiton Port | Infected Host | Protocol |
|---|---|---|---|
| 2005.12.20 21:00 | 5445 | 141.223.52.51 | UDP |

| No. | Dest Address | Bytes | Packets | SYN | ACK | Source Port |
|---|---|---|---|---|---|---|
| 0 | 149.230.151.1 | 78 | 1 | 0 | 0 | 1027 |
| 1 | 149.230.151.2 | 78 | 1 | 0 | 0 | 1027 |
| 2 | 149.230.151.3 | 78 | 1 | 0 | 0 | 1027 |
| 3 | 149.230.151.4 | 78 | 1 | 0 | 0 | 1027 |
| 4 | 149.230.151.5 | 78 | 1 | 0 | 0 | 1027 |
| 5 | 149.230.151.6 | 78 | 1 | 0 | 0 | 1027 |
| ... | | | | | | |
| 1959 | 149.230.160.241 | 78 | 1 | 0 | 0 | 1027 |
| 1960 | 149.230.160.242 | 78 | 1 | 0 | 0 | 1027 |
| 1961 | 149.230.160.243 | 78 | 1 | 0 | 0 | 1027 |
| 1962 | 149.230.160.244 | 78 | 1 | 0 | 0 | 1027 |
| 1963 | 149.230.160.245 | 78 | 1 | 0 | 0 | 1027 |
| 1964 | 149.230.160.246 | 78 | 1 | 0 | 0 | 1027 |

# POSTECH 네트워크에서의 탐지결과(3)

- 2005년 12월 20일 01:58에 탐지된 랜덤 스캐닝 웜
- 2307개의 랜덤 목적지 주소에 8713개의 스캐닝 패킷을 발생

| Time | Destinaiton Port | Infected Host | Protocol |
|---|---|---|---|
| 2005.12.20 01:58 | 64444 | 141.223.73.61 | TCP |

| No. | Dest Address | Bytes | Packets | SYN | ACK | Source Port |
|---|---|---|---|---|---|---|
| 0 | 217.250.255.107 | 82 | 6 | 0 | 0 | 1027 |
| 1 | 86.96.102.6 | 82 | 7 | 0 | 0 | 1027 |
| 2 | 58.11.84.91 | 82 | 8 | 0 | 0 | 1027 |
| 3 | 217.219.142.10 | 82 | 6 | 0 | 0 | 1027 |
| 4 | 84.167.219.62 | 82 | 6 | 0 | 0 | 1027 |
| 5 | 149.230.151.6 | 82 | 6 | 0 | 0 | 1027 |
| ... | | | | | | |
| 8708 | 60.237.174.120 | 82 | 8 | 0 | 0 | 1027 |
| 8709 | 85.97.137.132 | 82 | 1 | 0 | 0 | 1027 |
| 8710 | 60.212.162.17 | 82 | 4 | 0 | 0 | 1027 |
| 8711 | 217.245.192.111 | 82 | 5 | 0 | 0 | 1027 |
| 8712 | 219.95.156.133 | 82 | 4 | 0 | 0 | 1027 |
| 8713 | 84.5.0.224 | 82 | 3 | 0 | 0 | 1027 |

# 결론

- 요약
  - 엔터프라이즈 네트워크에 적합한 실시간 인터넷 웜의 탐지 알고리즘을 제시하고 알고리즘을 검증하였다.
  - 인터넷 웜 트래픽 Generator를 개발하였다.
  - 인터넷 웜의 탐지 시스템을 실제로 구현하여 POSTECH 네트워크에 적용하였다.

- 앞으로의 과제
  - 새로운 웜에 대응하는 방법에 대한 더 깊은 연구가 필요하다.
  - 다양한 범위의 엔터프라이즈 네트워크에서의 실험이 필요하다.
  - Ingress Network에서 탐지방법의 연구가 더 필요하다.

# 감사합니다!