



校園網路安全事故  
防治系統之設計與實作

---

賴守全

國立清華大學  
計算機與通訊中心



**Houston, we have a problem!**

---



## 校園網路安全事故

---

- 網路病毒防治
- 開放性郵件中繼主機防治
- 主動式網路安全事故處理



## 自動防治系統之設計與實作

---

- 校園網路自動隔離阻斷系統
- 校園網路病毒之偵測
- 校園郵件中繼主機之偵測



## Defending against Infestations of Internet Worms

---



### The Threats

---

- Malicious codes, such as Code Red, Nimda, Blaster, occurs more frequently and severely then ever.
- The Code Red worm infected more than 250,000 computers in just 9 hours.
- Internet worms have become vital threats to network and security management.



## Code Red Worm (7/19/2001)

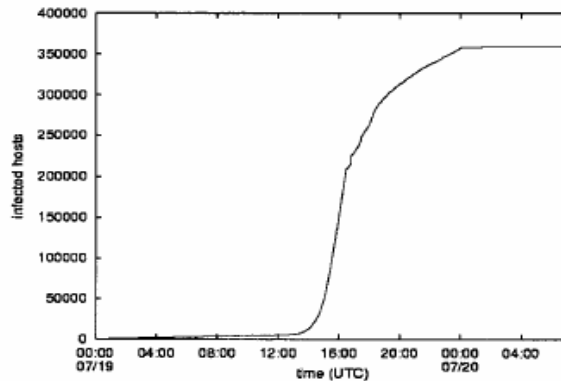


Fig. 2. Cumulative total of unique IP addresses infected by the first outbreak of Code-RedI v2.

source: David Moore, Colleen Shannon, k claffy, "Code-Red: a case study on the spread and victims of an Internet worm," Internet Measurement Workshop, 2002.



## The Problem

- In the old days, a host infected by a computer virus may be a matter of its own.
- In recent days, once a host is infected by an Internet worm, it may generate extra high volume of packets.
- Network administrator may be shaken up by totally unplanned network outage.



## The Challenge

---

- Cope with Internet worm incidents
  - *Figure out what happens to the network.*
  - *Mitigate the effect of Internet worms.*
  - *Restore the network back to normal operation.*



## Previous Works

---



## Internet Worm Detection

---

- Internet worm detection
  - *Many of these worm detection mechanisms have Unix-like based prototypes which require specific modification of the kernel.*
  - *Some require specific software to installed on each hosts.*
- These experimental prototypes may not suit the emergency and **readiness needs** of network administrators.

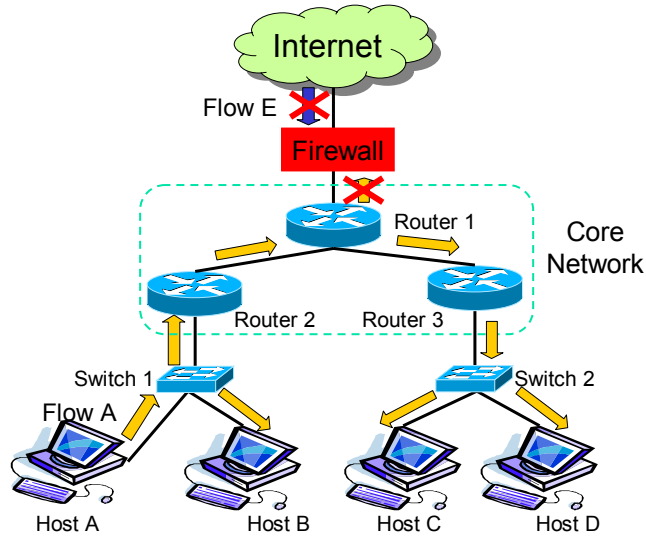


## Responding to Internet Worms

---

- Seal off the infestations of Internet worms
  - *Urge the users to recover compromised hosts and have their vulnerable hosts patched.*
- Security advisories usually suggest blocking traffic to/from worm-related services ports.
  - *Firewall is a solution to mitigate the impact.*

## The Firewall Architecture



## The Firewall

- A double-edged sword.
- It may not a good idea to block traffic when the worm attacks some mandatory public service ports, such as HTTP, SMTP, DNS.
- If possible, it is more desirable to isolate infected hosts instead of filtering traffic at network borders.



## The Power of Taiwan



## Code Red Infected (07/19/2001)

Top 10 Countries		
Country	hosts	hosts(%)
United States	157694	43.91
Korea	37948	10.57
China	18141	5.05
Taiwan	15124	4.21
Canada	12469	3.47
United Kingdom	11918	3.32
Germany	11762	3.28
Australia	8587	2.39
Japan	8282	2.31
Netherlands	7771	2.16

TABLE I

TOP TEN COUNTRIES WITH CODE-RED INFECTED HOSTS ON JULY 19.

Top 10 Domains		
Domains	hosts	hosts(%)
Unknown	169584	47.22
home.com	10610	2.95
rr.com	5862	1.63
t-dialin.net	5514	1.54
pacbell.net	3937	1.10
uu.net	3653	1.02
aol.com	3595	1.00
hinet.net	3491	0.97
net.tw	3401	0.95
edu.tw	2942	0.82

TABLE III

TOP TEN DOMAINS WITH CODE-RED INFECTED HOSTS ON JULY 19.





## Patching Rate (08/14/2001)

Patch Rate in Top 10 Countries		
Country	patched (%)	unpatched (%)
United Kingdom	65.65	34.34
United States	59.59	40.41
Canada	57.57	42.42
Germany	55.55	44.44
Netherlands	46.46	53.53
Japan	39.39	60.61
Australia	37.37	62.62
Korea	20.20	79.79
Taiwan	15.15	84.84
China	13.13	86.86

TABLE V

PATCHING RATE SEEN ON AUGUST 14TH FOR THE TEN COUNTRIES WITH CODE-RED INFECTED HOSTS ON JULY 19. PERCENTAGES ARE OF INFECTED HOSTS IN EACH COUNTRY THUS EACH ROW ADDS UP TO 100%



## Patching Rate (cont.)

Domain	Unpatched IIS (%)	Patched IIS (%)	Conn. Timeout (%)	Conn. Refused (%)
in-addr.arpa	40	7	30	11
home.com	44	5	30	8
rr.com	44	5	27	10
t-dialin.net	0.4	0	81	16
aol.com	0.3	0	39	61
pacbell.net	29	8	24	23
uu.net	0.6	0.2	51	47
hinet.net	20	0	46	25
net.tw	32	1	46	13
edu.tw	60	2	20	5

TABLE VI

PERCENTAGE BREAKDOWN OF PATCHING SURVEY RESPONSES BY CATEGORY FOR THE TOP DOMAINS ORIGINALLY INFECTED WITH CODERED V2. ROWS ADDING TO LESS THAN 100% ARE DUE TO RESPONSES NOT BEING CLEARLY CATEGORIZABLE AS PATCHED IIS OR UNPATCHED IIS. MOST DOMAINS SHOW A LARGE PERCENTAGE OF CONNECTION REFUSED OR CONNECTION TIMEOUT SUGGESTION FILTERING OF TRAFFIC, DISABLING OF PREVIOUSLY RUNNING IIS SERVERS OR DHCP.



## Open Mail Relay Problem

---

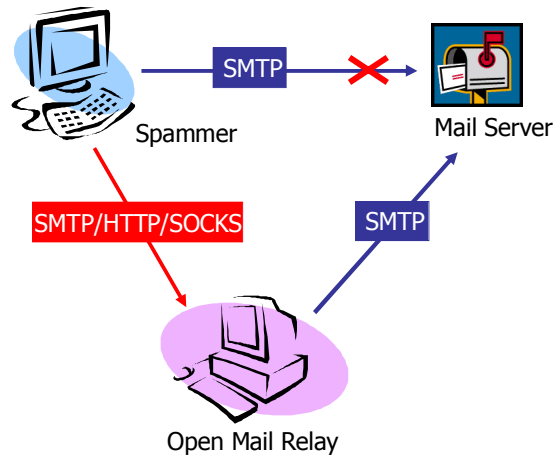


### The Threats

---

- Network administrators receive lots of emails complaining about or protesting against receiving spam emails from managed networks.
  - *Hosts in the managed network may become open mail relays for spam emails.*

## Transport of spam mails



## The Problem

- Spammer's IP address is dynamically changing.
  - *The spammer's IP address is dynamically assigned.*
  - *The spammer make use of open mail relays.*
- Blocking spammer's IP addresses becomes less effective.



## The Problem (cont.)

---


- The spammer does not use always SMTP as the mail relaying protocol
  - *The HTTP or SOCKS protocols are used for mail relaying.*
  - *Cannot trace back to the originator.*
- Cannot solely rely on SMTP to check or discover the existence of open mail relays.



## The Challenge


---

- Cease the existence of open email relays in the managed network.



# **Our Suggestion**

---



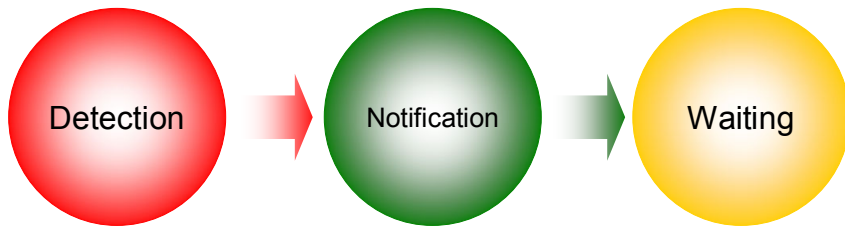
# **Responding to Network Security Incidents**

---



## Passive Responding Scheme

---



## Our Goal

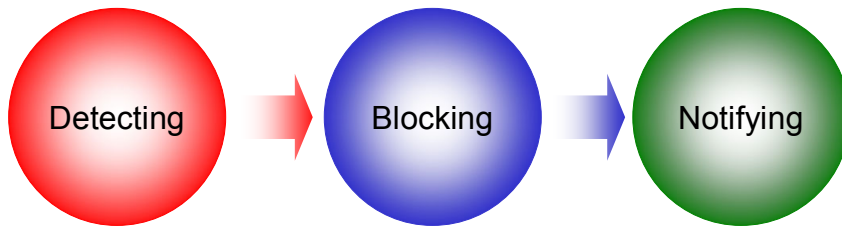
---

- Design and implement a **pro-active network defense system** to fight against Internet worms and open mail relays.
- Make use of **readiness techniques** to ease the implementation of the system.



## Pro-active Responding Scheme

---



## Responding to Internet Worms

---

- Detect hosts which is infected by Internet worms.
- Block traffic coming from worm-infected hosts.
- Notify local network administrators and persons who are related to the security incidents.



## Responding to Open Mail Relays

---

- Block all out-going SMTP traffic from hosts which is not in the “white” list.
- Detect hosts which has became open mail relays.
- Block traffic coming from open-mail-relay hosts.
- Notify local network administrators and persons who are related to the security incidents.



## Our Implementation

---





## **Network Security Incidents Responding System**

---

- Internet Worm Responding System (IWRS)
- Open Mail Relay Responding System (OMRRS)



## **Internet Worm Responding System**

---

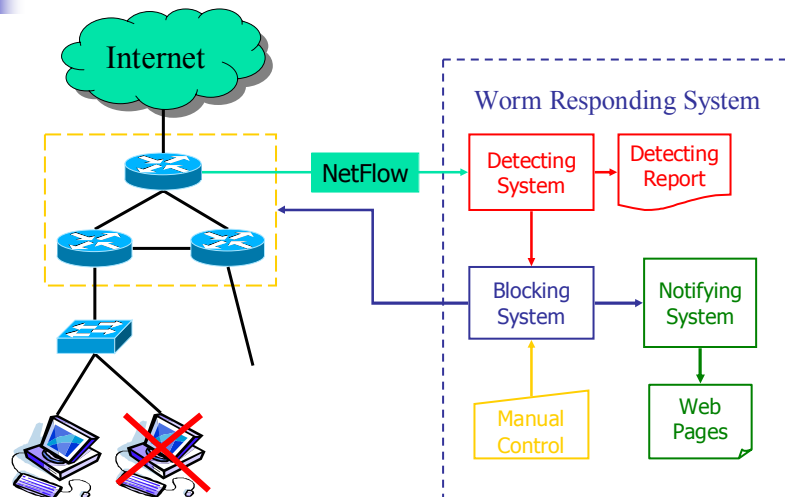


## Internet Worm Responding System

- Cope with hosts which generate extra high volume of probing packets and pose threats to normal network operations.



## IWRS Architecture



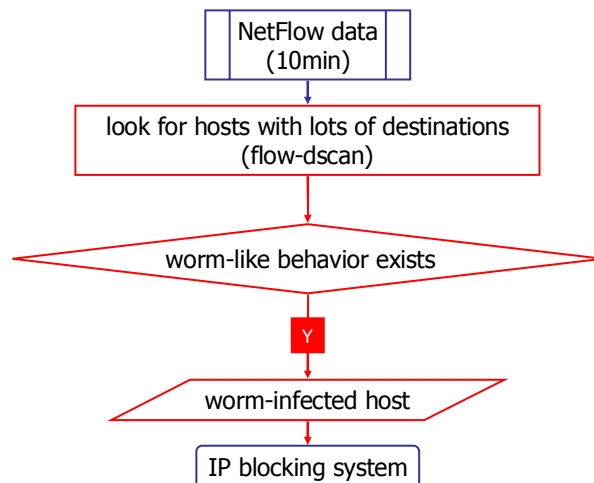


## Worm Detecting

- The facts
  - *Internet worms tend to search hosts with same vulnerability to do **rapid self-propagation**; thus it may produce lots of probing packets **to the same service ports on many different hosts**.*
- NetFlow data is collected and analyzed to figure out worm-infected hosts.

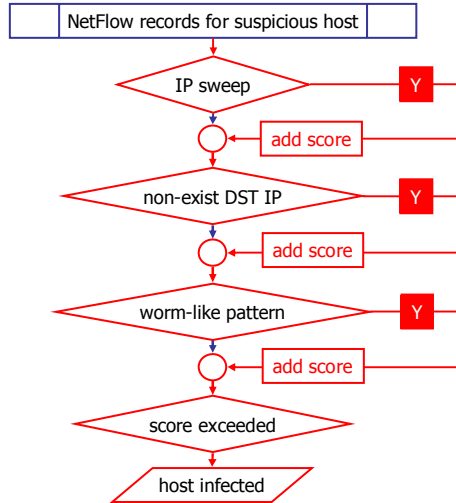


## Worm Detecting System





## Worm-like Behavior



## Worm-like Behavior (cont.)

```
1213.17:13:45.689 140.114.218.165:0 140.111.0.108:0 1 1 92
1213.17:13:45.778 140.114.218.165:0 140.111.0.117:0 1 1 92
1213.17:13:45.786 140.114.218.165:0 140.111.0.127:0 1 1 92
1213.17:13:45.898 140.114.218.165:0 140.111.0.202:0 1 1 92
1213.17:13:45.944 140.114.218.165:0 140.111.0.225:0 1 1 92
1213.17:13:45.991 140.114.218.165:0 140.111.0.248:0 1 1 92
1213.17:13:46.037 140.114.218.165:0 140.111.1.12:0 1 1 92
1213.17:13:46.055 140.114.218.165:0 140.111.1.21:0 1 1 92
1213.17:13:48.100 140.114.218.165:0 140.111.1.45:0 1 1 92
1213.17:13:48.149 140.114.218.165:0 140.111.1.67:0 1 1 92
1213.17:13:48.194 140.114.218.165:0 140.111.1.90:0 1 1 92
1213.17:13:48.207 140.114.218.165:0 140.111.1.98:0 1 1 92
```



## Worm-like Behavior (cont.)

---

```
1206.21:29:33.572 140.114.55.228:1303 80.180.211.233:80 6 3 144
1206.21:29:33.576 140.114.55.228:1311 80.180.211.237:80 6 3 144
1206.21:29:43.331 140.114.55.228:1301 80.180.211.232:80 6 1 48
1206.21:29:43.332 140.114.55.228:1281 80.180.211.222:80 6 1 48
1206.21:29:43.334 140.114.55.228:1313 80.180.211.238:80 6 1 48
1206.21:29:48.561 140.114.55.228:2934 80.180.211.253:80 6 3 144
1206.21:29:48.568 140.114.55.228:2944 80.180.212.2:80 6 2 96
1206.21:29:48.570 140.114.55.228:2954 80.180.212.7:80 6 3 144
1206.21:29:48.573 140.114.55.228:2952 80.180.212.6:80 6 3 144
1206.21:29:49.458 140.114.55.228:2970 80.180.212.15:80 6 2 96
1206.21:29:58.317 140.114.55.228:2924 80.180.211.248:80 6 1 48
1206.21:29:58.320 140.114.55.228:2968 80.180.212.14:80 6 1 48
```



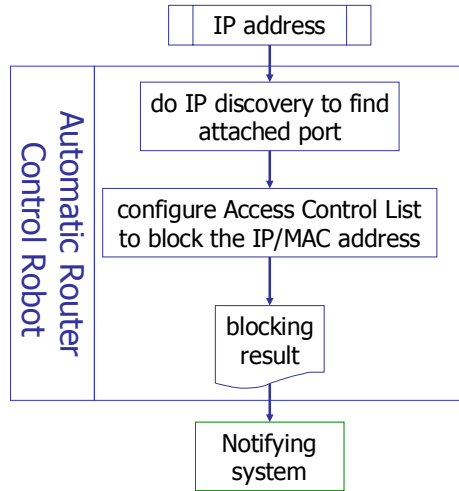
## IP Blocking System

---

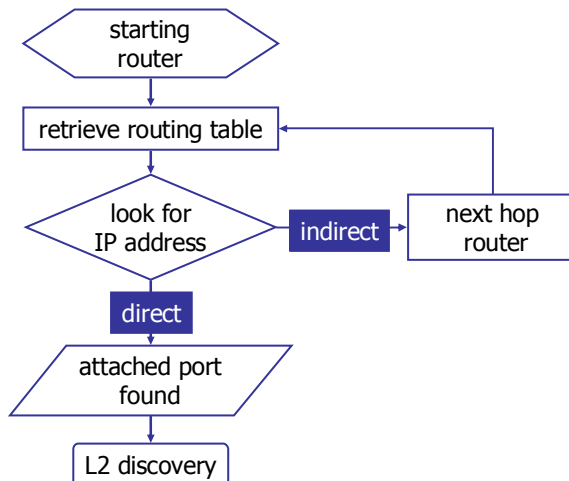
- Punish the bad ones not all other innocent ones.
  - *Make use of the **access control** function on routers and switches to block harmful traffic.*
  - *It is best to **isolate the infected host** without affecting other hosts.*
  - *More controllable network devices we have, better blocking we can do.*



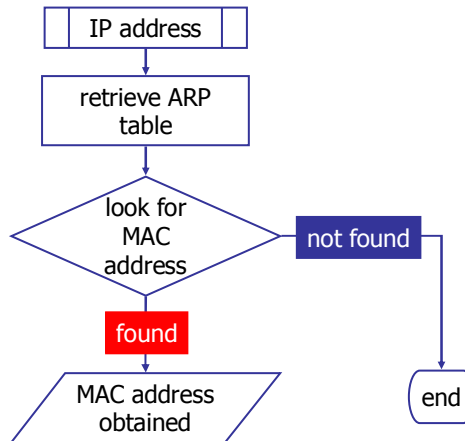
## IP Blocking System



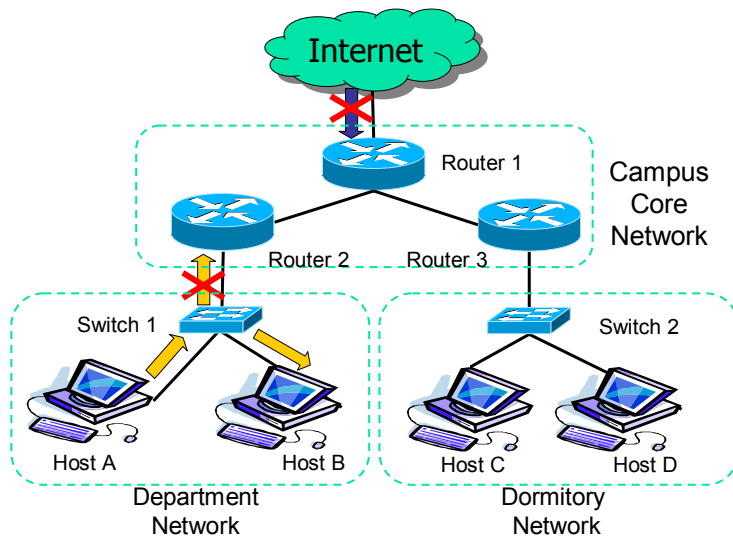
## IP Discovery



## L2 Discovery (optional)



## An IP Blocking Example



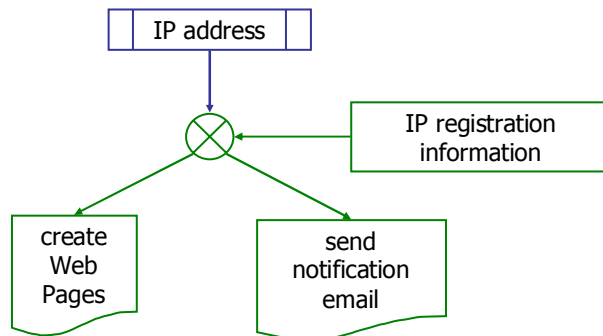


## Notifying System

- Inform system administrators or persons who are related to the security incidents.
  - *create web pages*
  - *send emails*
  - *send short messages to mobile phones*



## Notifying System (First Time)

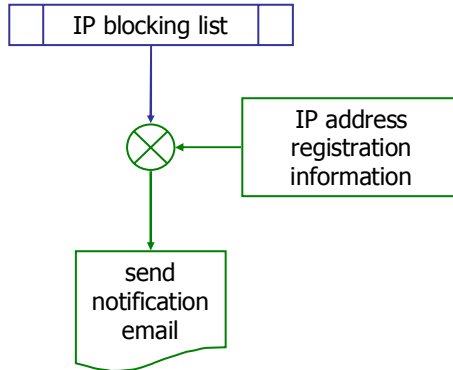






## Notifying System (Daily)

---



## Open Mail Relay Responding System

---



## Open Mail Relay (OMR) Responding System

---

- Cope with hosts which have become active open mail relays for spam mails

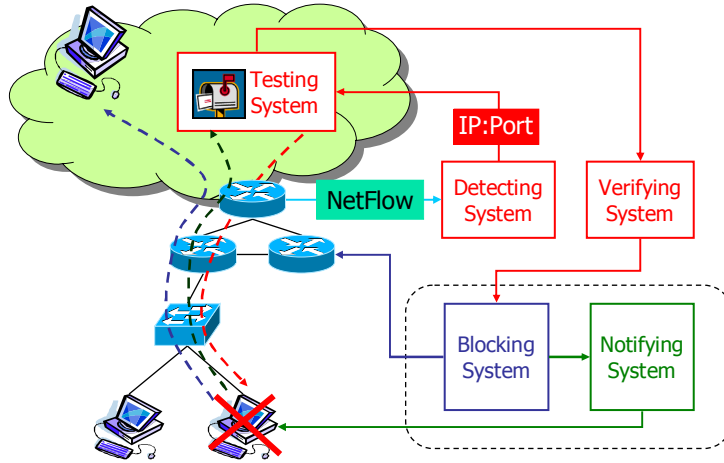


## OMR Detecting

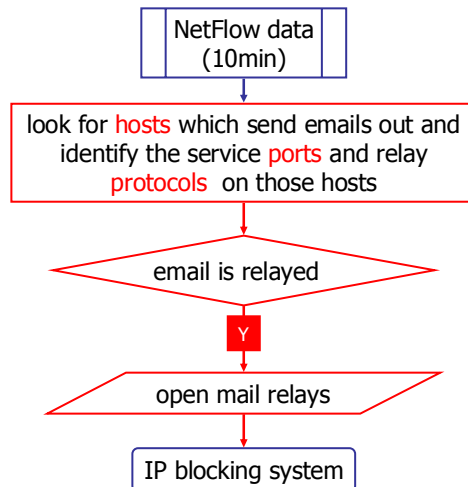
---

- The facts
  - *Active OMR tends to send lots of email out*
  - *At least one service port exists on OMR to relay emails*
- To identify
  - *Look for hosts which have sent email out*
  - *Analyze the service port on OMR*
  - *Identify the relay protocol on OMR*
  - *Check if an email could be successfully relayed from outside network*
- NetFlow data is collected and analyzed to figure out OMR candidate

# OMRRS Architecture

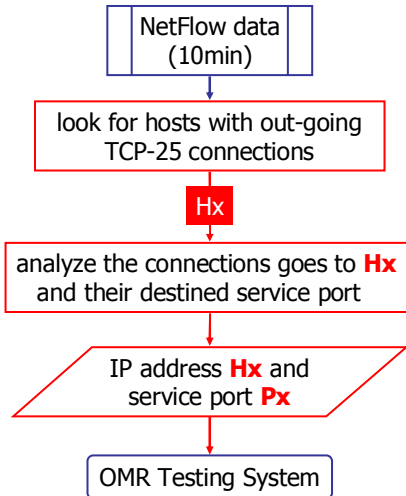


# OMR Detecting System





## OMR Searching System



## Hosts Which Sent Emails Out

srcIP	dstIP	srcPort	dstPort
192.168.131.56	209.248.80.98	2307	25
192.168.131.56	209.248.80.98	2311	25
192.168.131.56	209.248.80.98	2312	25
192.168.131.56	64.238.193.3	2314	25
192.168.131.56	216.83.165.21	2315	25
192.168.131.56	209.248.80.98	2323	25
192.168.131.56	209.248.80.94	2324	25
192.168.131.56	209.248.80.94	2321	25
192.168.131.56	61.78.53.18	2317	25
192.168.131.56	209.248.80.98	2329	25



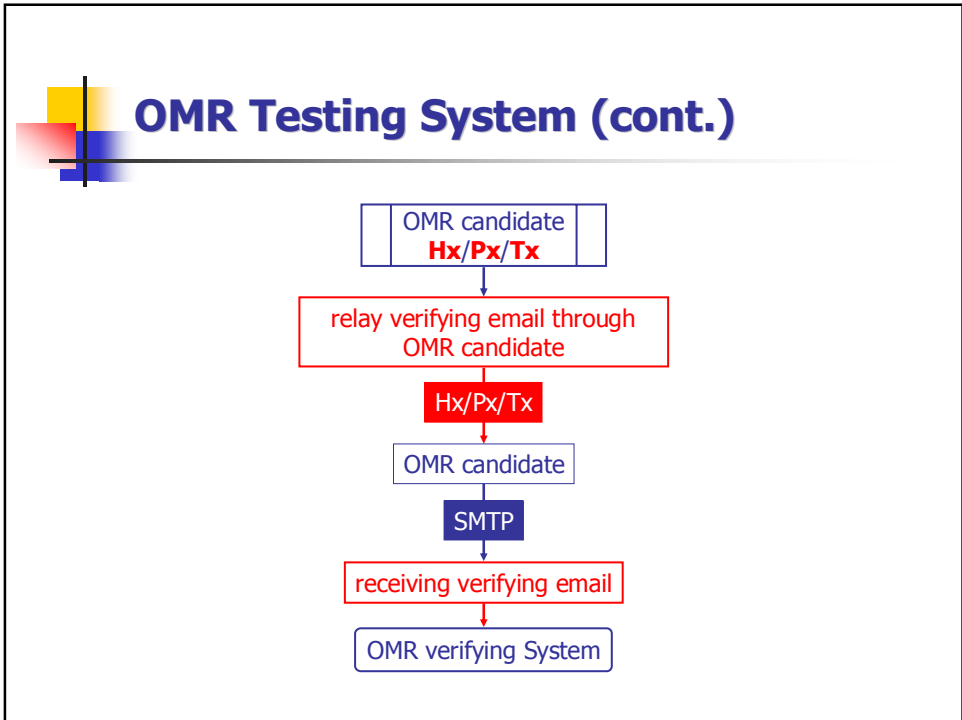
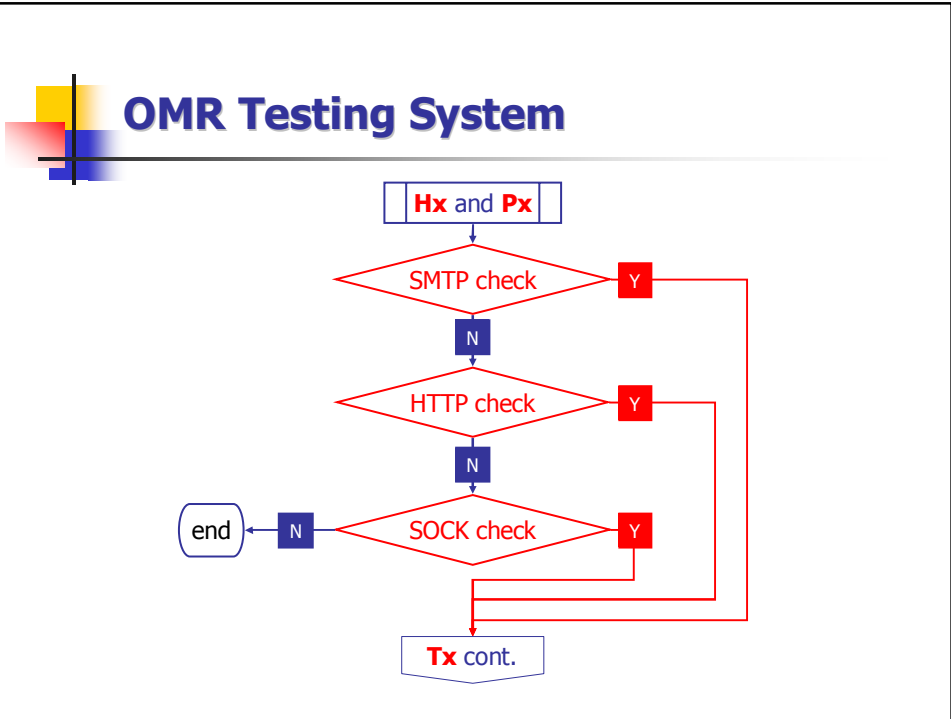
## Candidate Service Port (I)

srcIP	dstIP	srcPort	dstPort
216.83.165.21	192.168.131.56	25	2306
66.117.22.92	192.168.131.56	1306	9975
66.117.22.110	192.168.131.56	3082	9975
66.117.22.111	192.168.131.56	2313	9975
66.117.22.111	192.168.131.56	1704	9975
205.201.8.237	192.168.131.56	4518	9975
205.201.8.236	192.168.131.56	3884	9975
205.201.8.237	192.168.131.56	4901	9975
205.201.8.237	192.168.131.56	1214	9975
66.117.22.93	192.168.131.56	3137	9975



## Candidate Service Port (II)

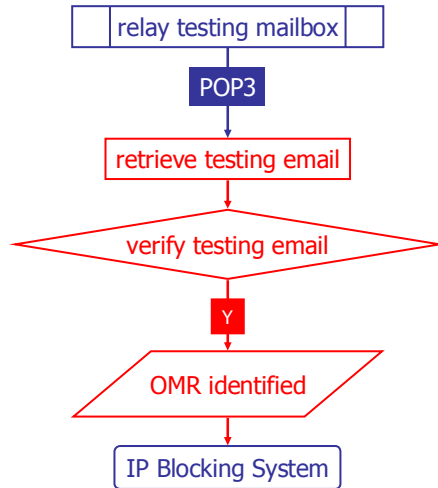
dstIP	dstPort	flows	octets	packets
192.168.131.56	113	1	120	2
192.168.131.56	2319	1	2664	44
192.168.131.56	2321	1	120	3
192.168.131.56	2324	1	120	3
192.168.131.56	2333	1	1734	33
192.168.131.56	2336	1	252	4
192.168.131.56	2339	1	1804	27
192.168.131.56	2340	1	2488	39
192.168.131.56	2342	1	252	4
192.168.131.56	9975	135	116224	926





## OMR Verifying System

---



## Network Security Incidents Responding System

---



## System Requirement

---

- NetFlow-enabled router or device (e.g. Cisco Catalyst 6509, Mirror-enabled router/switch + NetFlow export software)
- Personal Computer (e.g. Intel platform)
- UNIX-like OS (e.g. Linux, FreeBSD, Solaris,...)
- flow-tools (<http://www.splintered.net/sw/flow-tools/>)
- Perl v5.6 or above
- apache-1.x or above (<http://httpd.apache.org/>)



## System Requirement (cont.)

---

- IP Blocking System supported routers
  - *Extreme Routers with ExtremeWare 7.x*
  - *Cisco Routers with IOS 12.x*





## Source Code

---

- The source code and installation documents can be freely downloaded from:  
<http://cc.nthu.edu.tw/~chuan/>

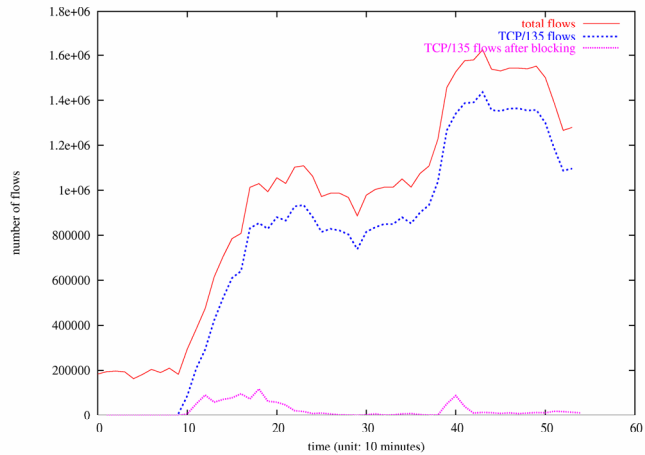


## The Results

---



## System Effectiveness (2003/8/12)

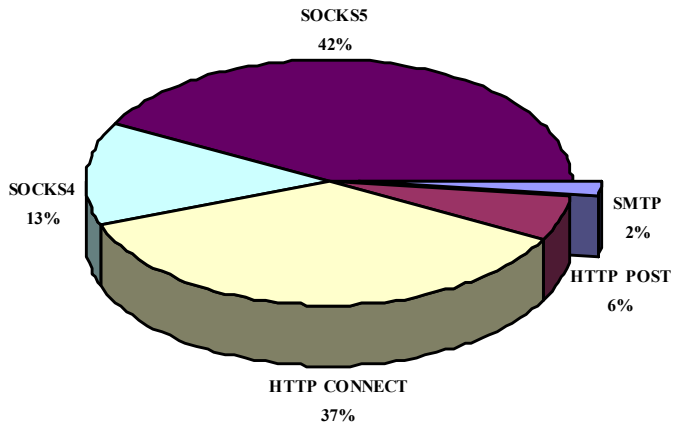


## System Results

76	2003/12/02 16:03:36	140.114.227.109	學生宿舍	<a href="#">IP-SCAN-ICMP-0</a>	2
77	2003/12/10 09:45:34	140.114.227.129	學生宿舍	<a href="#">IP-SCAN-TCP-445</a>	2
78	2003/12/05 02:34:08	140.114.227.180	學生宿舍	<a href="#">IP-SCAN-TCP-445</a>	
79	2003/12/10 08:14:31	140.114.227.197	學生宿舍	<a href="#">IP-SCAN-TCP-445</a>	3
80	2003/12/02 17:32:52	140.114.230.208	學生宿舍	<a href="#">IP-SCAN-TCP-135</a>	
81	2003/12/11 10:03:34	140.114.231.70	學生宿舍	<a href="#">IP-SCAN-TCP-135</a>	2
82	2003/12/11 16:13:54	140.114.231.160	學生宿舍	<a href="#">IP-SCAN-ICMP-0</a>	
83	2003/12/13 11:34:19	140.114.231.223	學生宿舍	<a href="#">IP-SCAN-ICMP-0</a>	
84	2003/12/08 12:05:16	140.114.232.84	學生宿舍	<a href="#">OPEN-PROXY</a>	



## Distribution of Relay Protocols



## Statistics of Out-going TCP-25 Traffic

	Flows	Bytes (G)	Packets
Total Traffic	1,770,010 (100%)	10.37 (100%)	26,088,642 (100%)
OMR Traffic	1,088,932 (61.52%)	3.96 (38.16%)	17,021,335 (65.24%)



## Problem Discussion

---



### Some issues

---

- Peer-to-Peer software may result in traffic patterns similar to the scanning behaviors generated by Internet worms.
- The IP address of a hosts may dynamically change if it is assigned randomly, such as a dial-up user or a DHCP client.



## Some issues (cont.)

---

- If the worm-infected host is inside a NAT network, the whole NAT network traffic may be blocked.
- Open Mail Relay Detecting System is not able to identify open mail relays which send emails through another internal mail relays.

報告完畢，敬請指教！