Stanford University Computer Security Team

Stephen E. Hansen
Computer Security Officer
David J. Brumley
Assistant Computer Security Officer
security@Stanford.EDU

Overview

- Who we are.
- What we have.
- What do we see.
- What do we do about it.

History

- Computer Security Office created in September 1994
- Sunset established in May 1995
- Current staffing:
  - 2 full time CSO's
  - 3 part time student interns

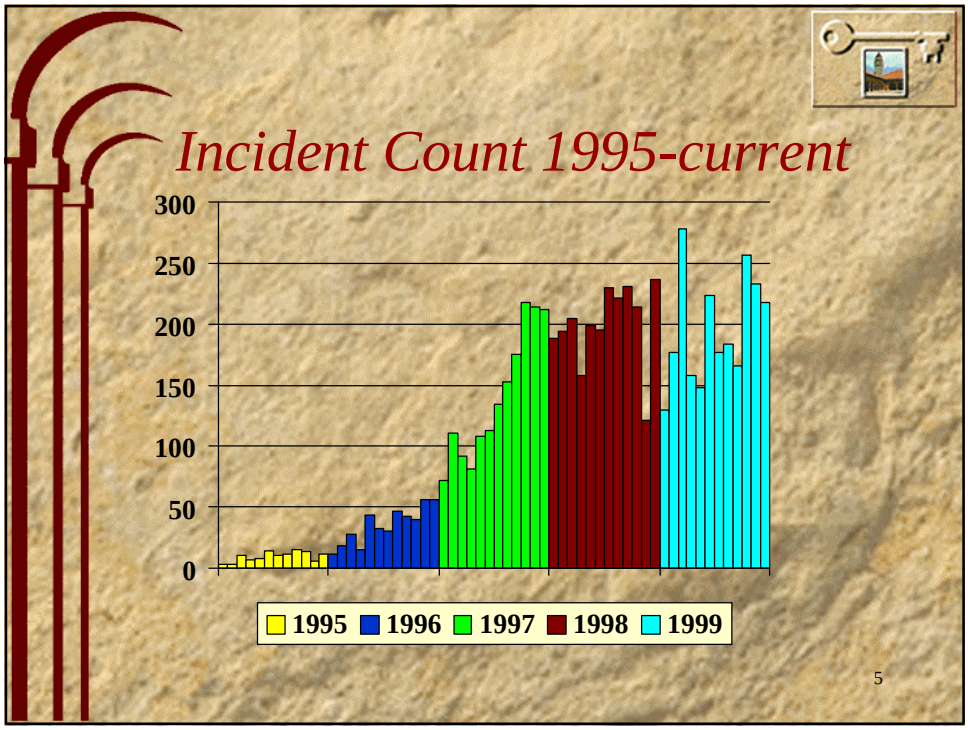
3

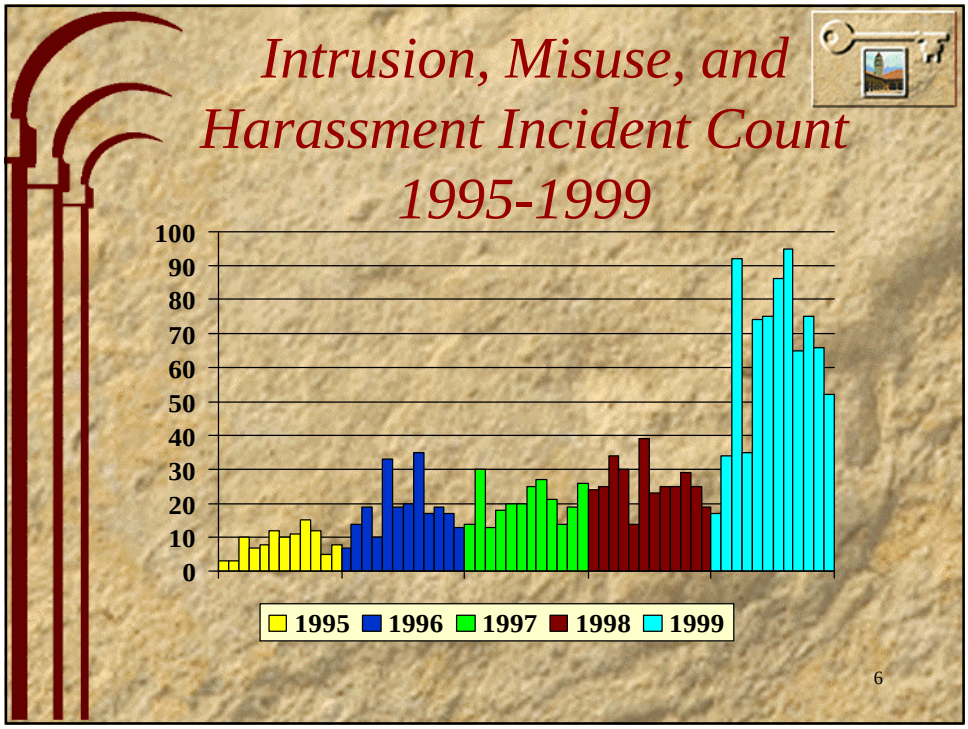
What Are We Protecting?

- Active subnets: 505, nodes: 53216*
  - 18116 IBM PC compatible
  - 9305 Macintosh
  - 2629 UNIX
  - 2299 Network Infrastructure
  - 711 Other
  - 1997 Printer
  - 338 Unknown
  - 258 X-terminal

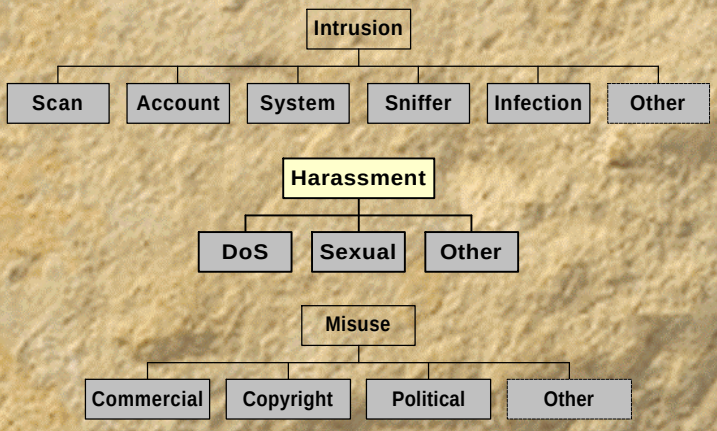
* As of Oct 7, 1999

4


Incident Count 1995-current
300
250
200
150
100
50
0
1995 1996 1997 1998 1999
5


Intrusion, Misuse, and Harassment Incident Count 1995-1999
100
90
80
70
60
50
40
30
20
10
0
1995 1996 1997 1998 1999
6

Incident Classification

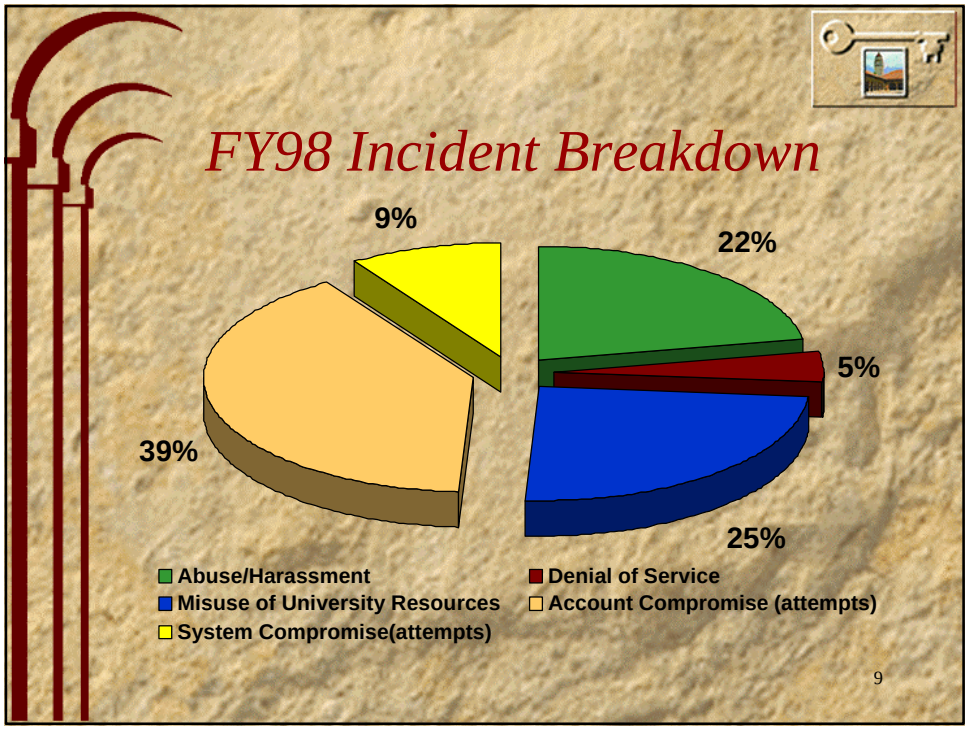


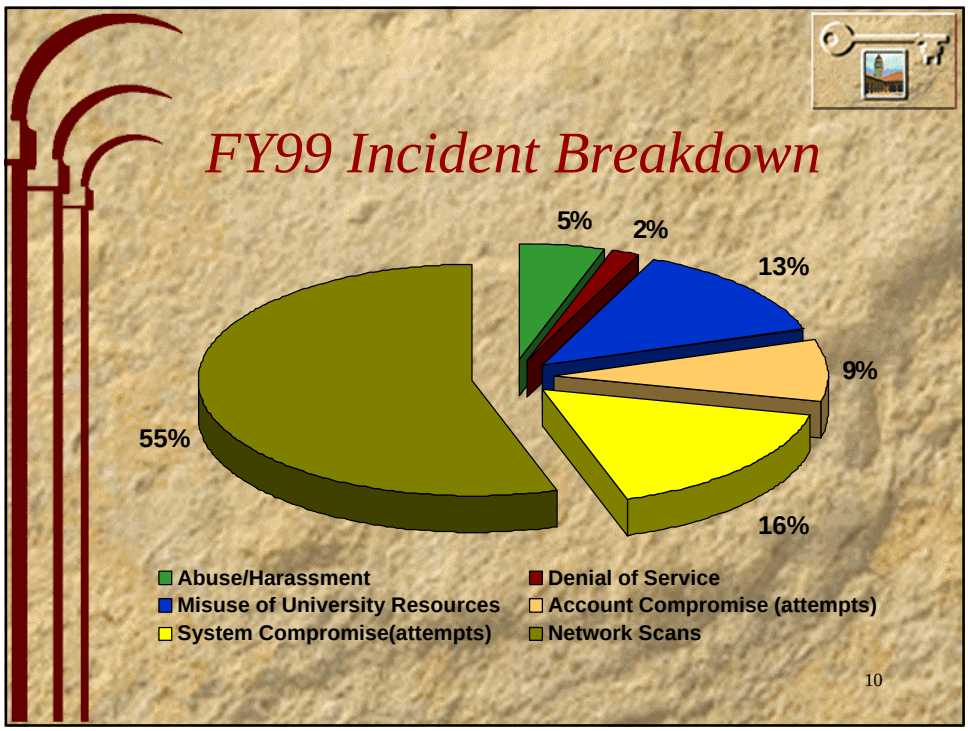
7

Incident Breakdown: July 1999

- *Total Incidents: 69*
  - *Abuse/Harassment: 2*
  - *Denial of Service Attacks: 1*
  - *Misuse of University Resources: 4*
  - *Chain Letters: 3*
  - *Account Incidents (actual/attempted): 7/8*
  - *System Incidents (actual/attempted): 10/51*

8


FY98 Incident Breakdown
9%
22%
5%
39%
25%
Abuse/Harassment
Denial of Service
Misuse of University Resources
Account Compromise (attempts)
System Compromise(attempts)
9


FY99 Incident Breakdown
5%
2%
13%
9%
55%
16%
Abuse/Harassment
Denial of Service
Misuse of University Resources
Account Compromise (attempts)
System Compromise(attempts)
Network Scans
10

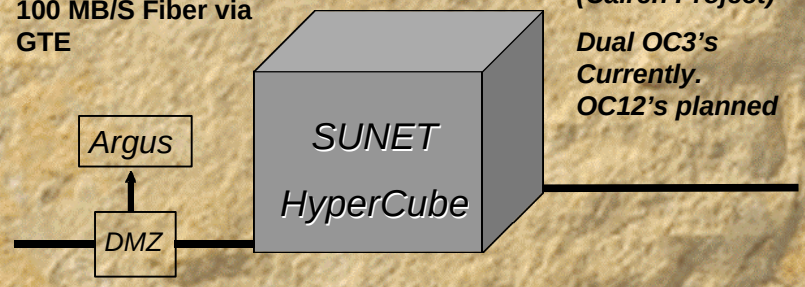
Topology of Network

Commercial Internet:

100 MB/S Fiber via GTE

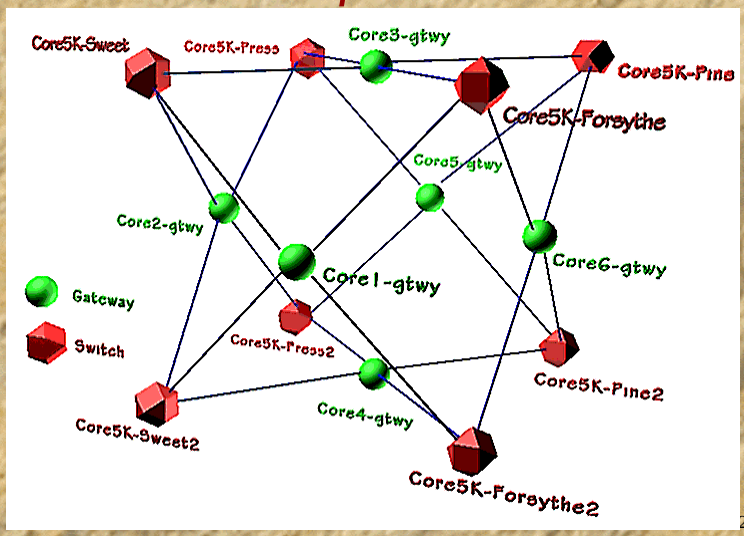
Internet 2 (Calren Project)

Dual OC3's Currently. OC12's planned



11

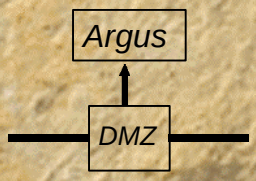
The Stanford CUBE!



12

Commercial Net Monitoring

- **Argus** (from CMU) is used to log connection flows
- **Average Day:**
  1 GB of TCP flows
  1.4 GB total flows



A Flow contains:

- Date/time stamp
- Source/Destination IP, Protocol, Port
- Number of bytes and number of packets seen

13

Commercial Gateway

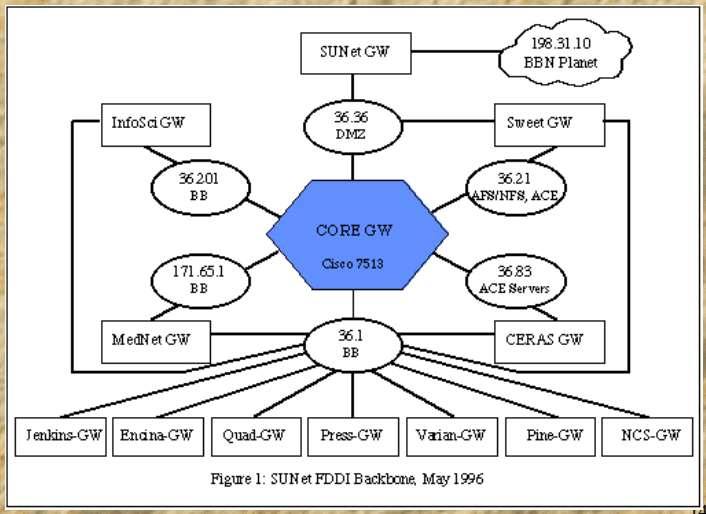


Figure 1: SUNet FDDI Backbone, May 1996

14

What Do We Look for?

Most scans, including port and service scans, can be detected by simple hashing of IP + Source Port!

- This method detects programs that do multiple connect()'s to a host or range of hosts. Why? The source port will change.
- This will **miss** scans where the source port is deliberately left constant (some types of nmap scans, for example).

A daily scan for a "hot list" of suspect IP addresses and ports complements the scan detection program.

15

Commercial Internet Link

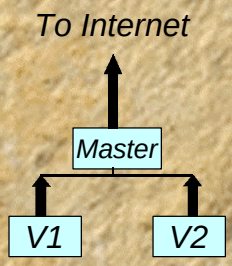
What we see

```
dbrumley@sunset> sura -n -r badguys.990902 host 213.8.12.127 | tail -10
09/02 05:43:40 tcp  213.8.12.127.3735        o> 171.64.67.66.23          TIM
09/02 05:43:45 tcp  213.8.12.127.3736        o> 171.64.67.67.23          TIM
09/02 05:43:50 tcp  213.8.12.127.3737        o> 171.64.67.68.23          TIM
09/02 05:43:51 tcp  213.8.12.127.3738        o> 171.64.67.69.23          TIM
09/02 05:43:52 tcp  213.8.12.127.3739        o> 171.64.67.70.23          TIM
09/02 05:43:56 tcp  213.8.12.127.3740        o> 171.64.67.71.23          TIM
09/02 05:43:58 tcp  213.8.12.127.3741        o> 171.64.67.72.23          TIM
09/02 05:41:30 tcp  213.8.12.127.3653        -> 171.64.66.243.23         CLO
09/02 05:44:49 tcp  213.8.12.127.4319       <o> 171.64.54.10.23          TIM
Total records displayed: 12007
dbrumley@sunset>
```

16

Internet 2 Monitoring

Challenge - The network bandwidth is too great for normal “sniffer” based products.



- Stanford developed ***NetViewer*** to mimic Argus flow records via Cisco’s exported NetFlow data.
- Each router exports data to a local ***NetView***, which analyzes the data.
- Each ***NetView*** can export data to other ***NetView***’s, creating a virtual IDS network.

17

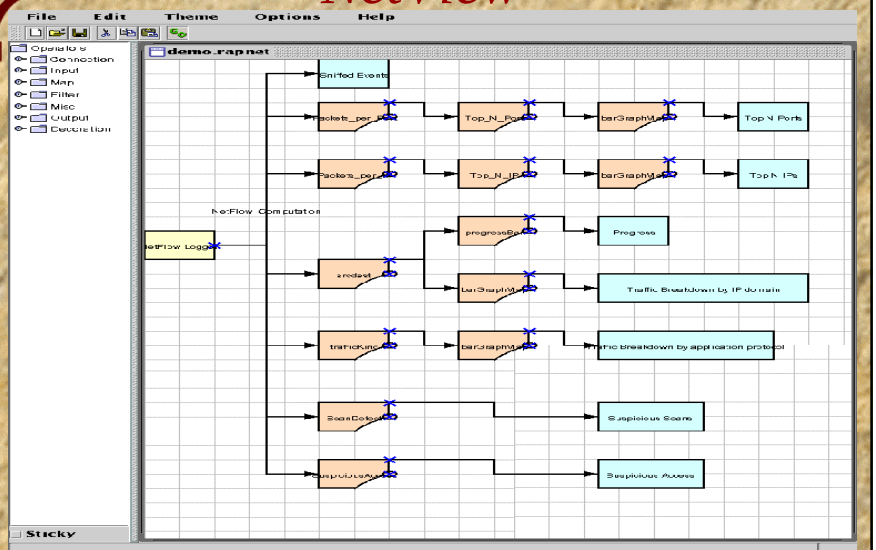
NetView Capabilities

NetView provides a *language* for defining an Intrusion Detection System or IDS.

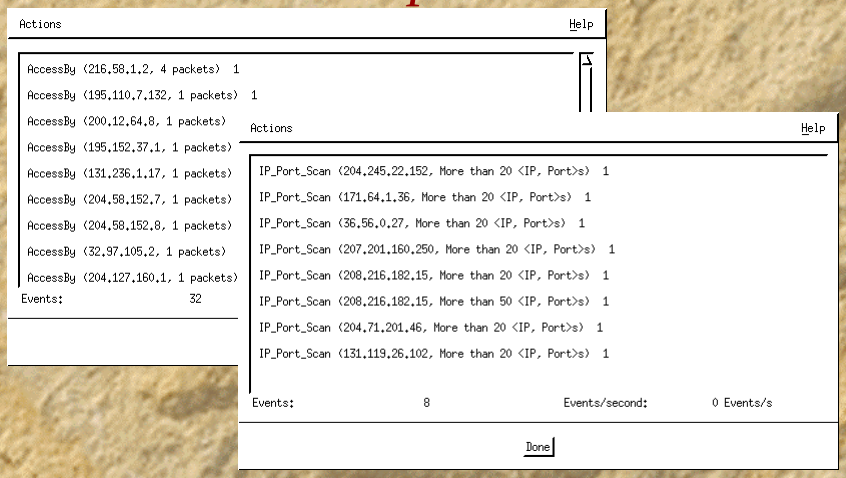
- Maps can easily be written in a C-like language
- When speed is essential, maps can be written completely in C
- Current speed: around 500 records/second, depending on number of maps
- Redundant communication with other Event Viewers (EV) and Event Processing Networks (EPN).

18

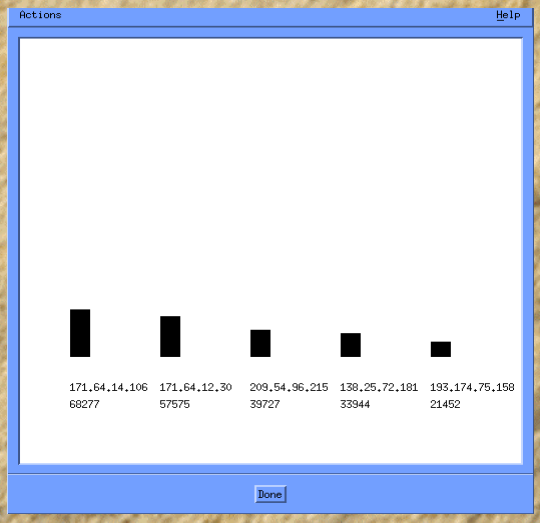
NetView



NetView Attempted Intrusions



NetView Network Statistics



21

IDS: Beyond Monitoring

We occasionally miss intrusions or intrusion attempts. So we compliment our intrusion detection system with:

- *NMAP Scans* - Look for hosts listening to port 1524, 530, and other ports hackers use for backdoors
- *IRC Monitoring:*
  - "whois" logs
  - channel logs (public channels only)
  - tcpdumps of intruder's BNC or Eggdrop traffic

22

Dealing With Intrusions

Stanford intrusion response step by step

- Step 1 - Detect the intrusion.
- Step 2 - Determine the extent of the compromise (remotely if possible).
- Step 3 - Look for other possible victims.
- Step 4 - Notify the proper sites, including source of scan, intrusion, and further connection attempts.
- Step 5 - Add all information obtained to MO file.
- Step 6 - Write incident summary report.

23

Intruder Tracking Map

24


Sunset Contact Information
E-mail: security@Stanford.EDU
Include 'Emergency" in subject field for immediate response.
Telephone: +1 650-723-2911
Tools available at
http://security.Stanford.EDU/FIRST
More info on the web at
http://security.Stanford.EDU
PGP Fingerprint:
PGP RSA Key 1024/736EEC29
4B 1A 84 3D 1E E4 6B CC 19 30 EA CB 5A B0 FF 42
15