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

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
Incident Classification

Intrusion
- Scan
- Account
- System
- Sniffer
- Infection
- Other

Harassment
- DoS
- Sexual
- Other

Misuse
- Commercial
- Copyright
- Political
- Other

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
FY98 Incident Breakdown

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

FY99 Incident Breakdown

- Abuse/Harassment: 55%
- Denial of Service: 13%
- Misuse of University Resources: 16%
- Account Compromise (attempts): 9%
- System Compromise (attempts): 5%
- Network Scans: 2%
Topology of Network

Commercial Internet:
100 MB/S Fiber via GTE

internet 2
(calren project)

Dual OC3’s
Currently, OC12’s planned

SUNET
HyperCube

DMZ
Argus

The Stanford CUBE!
**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

**Commercial Gateway**

![Diagram of commercial gateway networks](Image)
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.
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.

---

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).
NetView

NetView Attempted Intrusions
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
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.

Intruder Tracking Map
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