



**19th Department of Energy  
Computer Security Group Training Conference**

**An Update—CIAC's Efforts  
Today's Threats**

UCRL-MI-120632, Rev-3

**Sandra L. Sparks  
CIAC Project Leader  
April 29, 1997**

Work performed under the auspices of the U.S. Department of Energy by Lawrence  
Livermore National Laboratory under Contract W-7405-Eng-48

# Today's presentation

---

- Highlights of incident response since last year
- Today's threats
- Changing intrusion profile
- Protecting ourselves
- Current CIAC team
- Contacting CIAC

# Incident activity

---

- **Number of Incidents reported to CIAC = 138**
  - **Number of Cases\* = 99**
  - **Number of Actions\*\* = 506**

\*Cases are incidents involving multiple sites

\*\* Actions are all of the activities by CIAC in responding to the incident

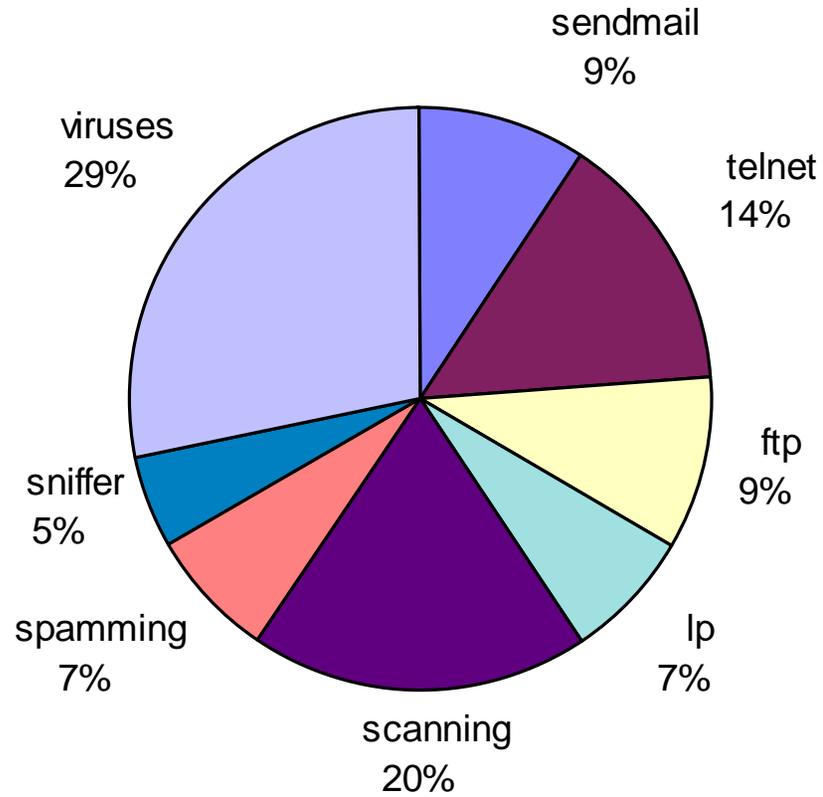
- **We believe these represent only a fraction of the actual incidents occurring around the DOE complex**

# Non-virus vs. virus incidents



# Further breakdown

---



# Specific viruses

---

- AntiEXE
- AOLGOLD Trojan
- BUPT
- Concept Macro Virus
- D3 virus (AntiEXE)
- Da'Boys Virus
- Dishwasher Virus
- Internet AIDS
- IVP.BUBBLES
- Junkie
- Michaelangelo
- Monkey
- NATAS Virus
- PKZIP300.V Virus
- Wazzu Virus
- WinZip
- XIBN Virus (AntiCMOS B)

# Incidents are costly

---

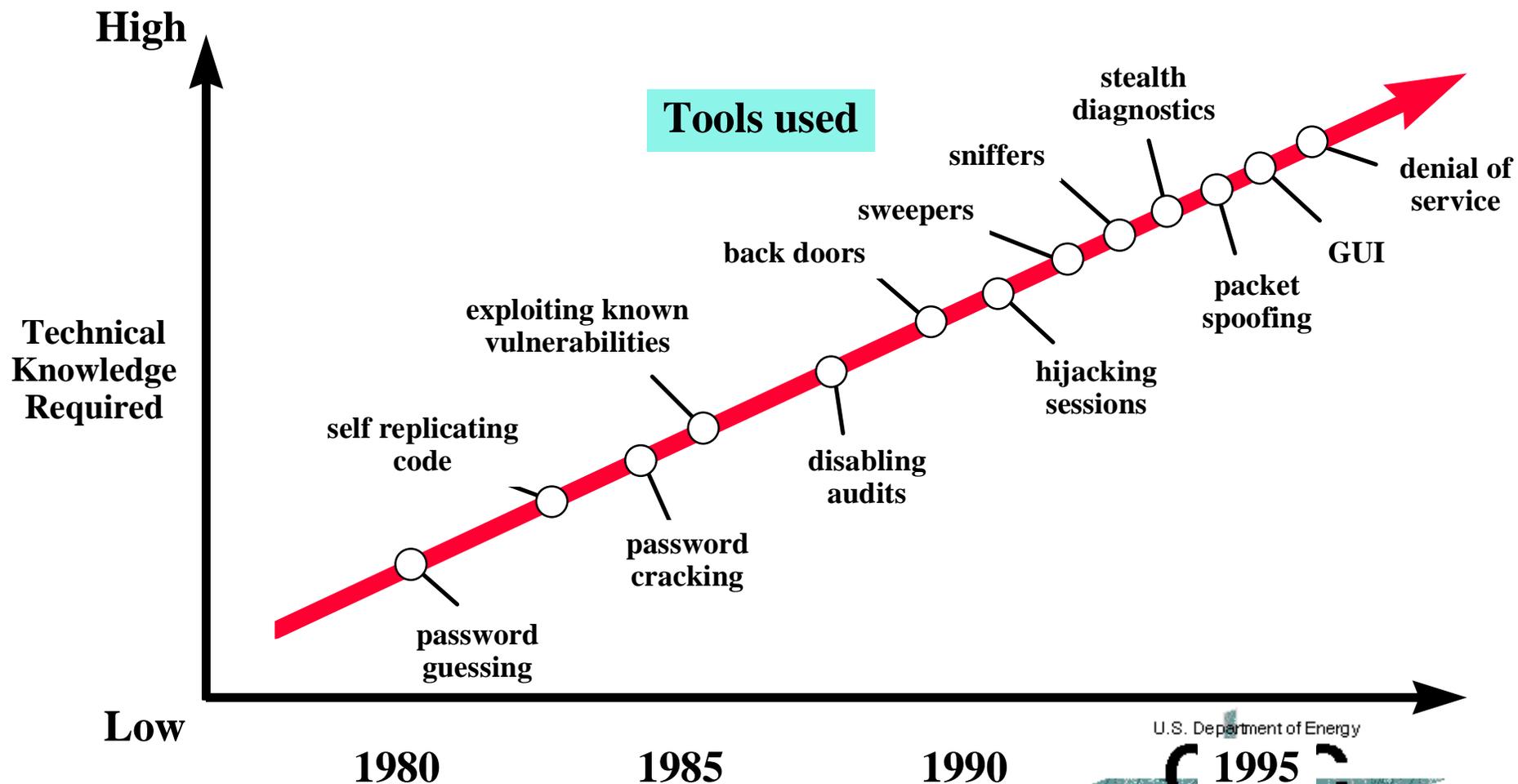
- **When you detect an intrusion, containing it and restoring your site back to normal operations is costly**
  - **Another government site infected with the Tentacle virus**
    - 7 servers, 700 workstations infected
    - Estimated cleanup cost = \$100,000.00
    - Estimated lost time = unknown
  - **One site had to disconnect from the Internet in order to stop an ongoing hacker attack**
    - Disconnect their site from the Internet for 24 hours
    - Push-button tool exploiting captured passwords, trusted host relationships and the syn attack made the hacker a moving target
  - **Cleanup from sniffer attacks still cost from \$40-100K**

# The changing threat environment

---

- **Attack trends**
  - Increased sophistication
    - More stealth
    - More automation
  - Changing motives and agenda
  - Changing environment

# More sophistication



# More automation

---

- **Complex attacks are now automated**
  - Sophistication for the Masses
  - 8lgn exploitation scripts
  - Rootkit
- **Tedious vulnerability information collection can be automated**
  - Internet Security Scanner (ISS)
  - Security Analysis Tool for Auditing Networks (SATAN)

# Changing operating environment

---

- Increasingly, our information assets reside on computer systems
- Larger reliance on networks and network services outside our control
- Information to use in perpetrating an intrusion is readily available
  - Mailing lists
  - World Wide Web (WWW) servers
  - Internet Relay Chat (IRC) lines, Bulletin Boards (BBS)

# Changing motives

---

- **Computer attacks are an economical way of gaining advantage**
  - Politically
  - Economically
- ***“Internet is now the fastest growing means for foreign governments and firms to gather information about U.S. businesses.”***
  - Source: National Counterintelligence Center

# 1996 CSI/FBI Computer Crime and Security survey

---

- **“The results serve as a profound warning and a wake-up call”**
  - 42% acknowledged they experienced unauthorized use of their computer systems within the last 12 months
  - These attacks included:
    - Brute force password guessing (13.9%)
    - Scanning (15%)
    - Denial of service (16.2%)
    - Data diddling (15.5%)

# 1996 CSI/FBI Computer Crime and Security survey

---

- The data diddling occurred primarily in financial institutions (21%) and medical institutions (36.8%)
- According to the study, 50% of reported incidents occurred on internal nets and ~40% came via remote dial-in and Internet connections
- 61% of 104 federal agencies surveyed sited viruses as the source of frequent security breaches

# Intrusion models

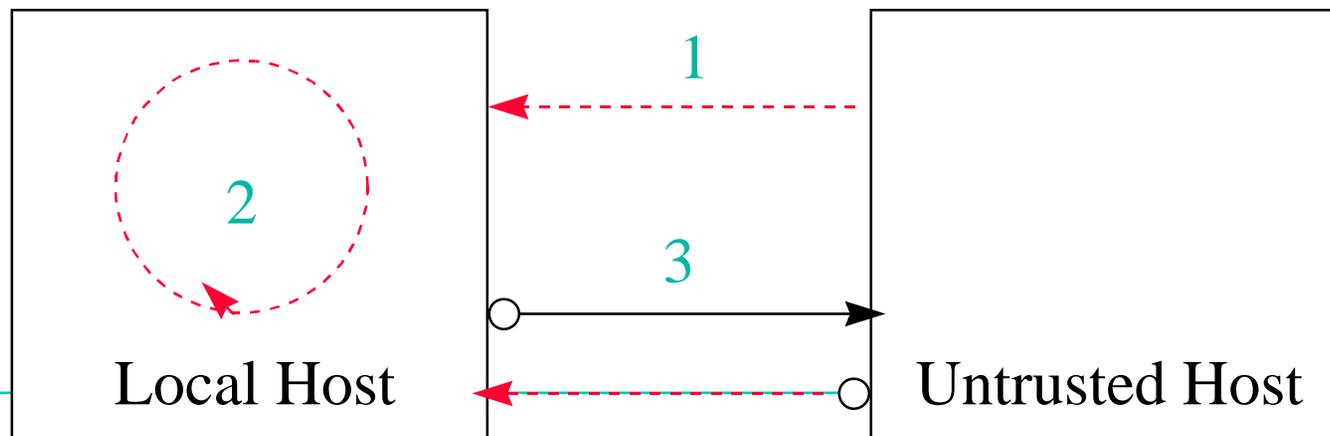
**Type 1: Attacks on network and dial-up services**

**Type 2: Physical attacks against a local system**

- Virus attacks using current privilege
- Non-privileged users attempting to gain privilege to view, alter, or control

**Type 3: Server attacks on client applications**

**NEW**



# Changes in intrusion profile - 1988

---

- **1988 Profile**

- Mostly **Type 1 & 2**
- **Password Guessing** - gain access to systems through easy to guess passwords
- **Widely know vulnerabilities** - gain control of systems by exploiting vulnerabilities widely known and discussed by the technical community
- **Boot sector viruses** became a threat
- **Program viruses** became prevalent

# Changes in intrusion profile - 1995

---

- **1995 Profile**

- **Type 1 & 2**
- **Sniffer attacks - capturing data as it traverses the net**
- **E-mail attacks - gaining system access through vulnerabilities in network service software**
- **Network File System attacks - gaining data access through vulnerabilities in operating system software**
- **Network Infrastructure attacks - denial-of-service through attacks on routers and name servers**
- **IP Spoofing attacks - gaining system access by tunneling through firewalls**
- **Emergence of self encrypting, polymorphic viruses**

# Changes in intrusion profile - 1996

---

- **1996 Profile**

- Still mostly **Type 1 & 2**
- Exploiting passwords
- Exploiting known vulnerabilities
- Exploiting protocol flaws
- Examining source files for new security flaws
- Using ICMP attacks
- Abusing anonymous FTP, web servers, e-mail
- Installing sniffer programs
- IP source address spoofing
- Denial-of-service attacks
- Easy-to-use virus creation tool kits

# Today's threats--1997

---

- **Hackers are working smart**
  - At least one new vulnerability discovered per week
    - *Scriptors of Doom* targeting HP regularly
  - Hacker web sites, BBS, Chat rooms abound
  - Take advantage of poor software development practices
  - Web sites are plentiful and these attacks are fun if they embarrass the “enemy”
  - Malicious web server software (Type 3 attack)
  - Widespread, large-scale attacks on the Internet Infrastructure
    - **Attacks against NNTP (Network News Transport Protocol) servers throughout the world**
      - NNTP servers are commonly referred to as USENET news servers

# Today's threats--1997

---

- **We aren't applying what we know**
  - Many known vulnerabilities still being exploited even though patches available
    - Unix is still the OS of choice to exploit
  - Password cracking still produces results
  - Sniffers are actively used and are still effective
    - Sniffer detectors are available for several OS
    - <ftp://ciac.llnl.gov/pub/ciac/sectools/unix/sniffdetect>

# Denial of service (DoS) attacks

---

- **Denial-of-Service attacks continue to increase**
  - Services such as DNS, News servers, Internet service providers (ISP)
    - <http://ciac.llnl.gov/ciac/bulletins/g-14.shtml>
    - <http://ciac.llnl.gov/ciac/bulletins/h-34.shtml>
    - <http://ciac.llnl.gov/ciac/bulletins/h-43.shtml>
  - *SYN Flood* attack
    - <http://ciac.llnl.gov/ciac/bulletins/g-48.shtml>
    - <http://ciac.llnl.gov/ciac/bulletins/h-02.shtml>
    - <http://ciac.llnl.gov/ciac/bulletins/h-12.shtml>
  - *Ping o' Death* attack
    - <http://ciac.llnl.gov/ciac/bulletins/h-04.shtml>
    - <http://ciac.llnl.gov/ciac/bulletins/h-12.shtml>
    - <http://ciac.llnl.gov/ciac/bulletins/h-18.shtml>
    - <http://ciac.llnl.gov/ciac/bulletins/h-42.shtml>

# Poor software practices plague us..

- **Taking advantage of poor bounds checking**
  - H-08: Ipr Buffer Overrun Vulnerability
  - H-17: cron/crontab Buffer Overrun Vulnerabilities
  - H-22: talkd Buffer Overrun Vulnerability
  - H-23: Sendmail MIME Conversion Buffer Overrun Vulnerability
  - H-24: IBM AIX(r) Buffer Overrun Vulnerability
  - H-27: HP-UX vgdisplay Buffer Overrun Vulnerability
  - H-30: Solaris ffbconfig Buffer Overrun Vulnerability
  - H-37: Solaris 2.x passwd buffer Overrun Vulnerability
  - H-41: Solaris 2.x eject Buffer Overrun Vulnerability
  - H-44: Solaris 2.x fdformat Buffer Overflow Vulnerability
  - H-32: HP-UX ppl Core Dump Vulnerability

# Automatic execution is convenient, but . . .

---

- **Taking advantage of automatic execution of software**
  - Macro viruses
  - Java applets
  - Other server driven software

# What about Windows NT? .....

- It is subject to **Type 3** Intrusions
  - Internet Explorer 3.x (Windows NT and 95)
    - Five serious security bugs discovered in March, 1997
    - Malicious .url or .lnk files
    - Malicious icon embedded within a web page
    - Version 3.02 is now available and claims to fix these problems
  - Active X
    - ActiveX enabled browsers inherit capabilities of the local user, thus enabling an accepted malicious ActiveX control to execute arbitrary commands
  - Shockwave
    - Allows malicious web page developers to create a Shockwave movie that will read through a user's e-mail and potentially upload it to their web server

# Hoaxes

---

- **Hoaxes are developing lives of their own**
  - Deeyenda, Good Times, Irina
    - *CIAC 2301 Virus Update*
  - Denial of Service attack in their own right
- **CIAC's Internet hoax bulletin was widely used**
  - <http://ciac.llnl.gov/ciac/bulletins/h-05.shtml>
- **CIAC's hoax page has become one of the hottest sites on the Internet**
  - 163,715 visitors by 4/13/97
  - <http://ciac.llnl.gov/ciac/CIACHoaxes.html>
- **One ISP reported that 80% of their hotline calls were dealing with hoaxes**

# **It's a hoax! It's a Trojan! It's both!!**

---

- **AOL4FREE--the program**
  - A student actually created a program to gain free access to AOL
  - Currently serving time for his act
- **AOL4FREE--the hoax e-mail message**
  - Reading an e-mail message does not infect systems
- **aol4free.com--the Trojan horse software**
  - Erases your C: drive on DOS and windows systems
  - Does not affect Macintosh systems
- **Keep checking CIAC's hoax page for the latest information**

# How to identify hoax warnings.....

---

- Watch for **red** flag alerts
  - FCC warnings
    - FCC does not disseminate virus warnings
  - Warning urges you to pass it on to your friends
  - No PGP signature from authoritative source
    - Response team
    - Antivirus organization
- When in doubt, do not send it out

# If you suspect a hoax, . . .

---

- **Check for sender of message**
  - Contact the individual
    - Find out if the individual wrote the warning or if they have touched the virus
    - If address does not exist or if you have questions about the authenticity: **DO NOT CIRCULATE....**
- **Have the warning validated**
  - Check with your CPPM, CSSM or other local computer security professional
  - Check CIAC's hoax page
  - Call CIAC

# The Web

---

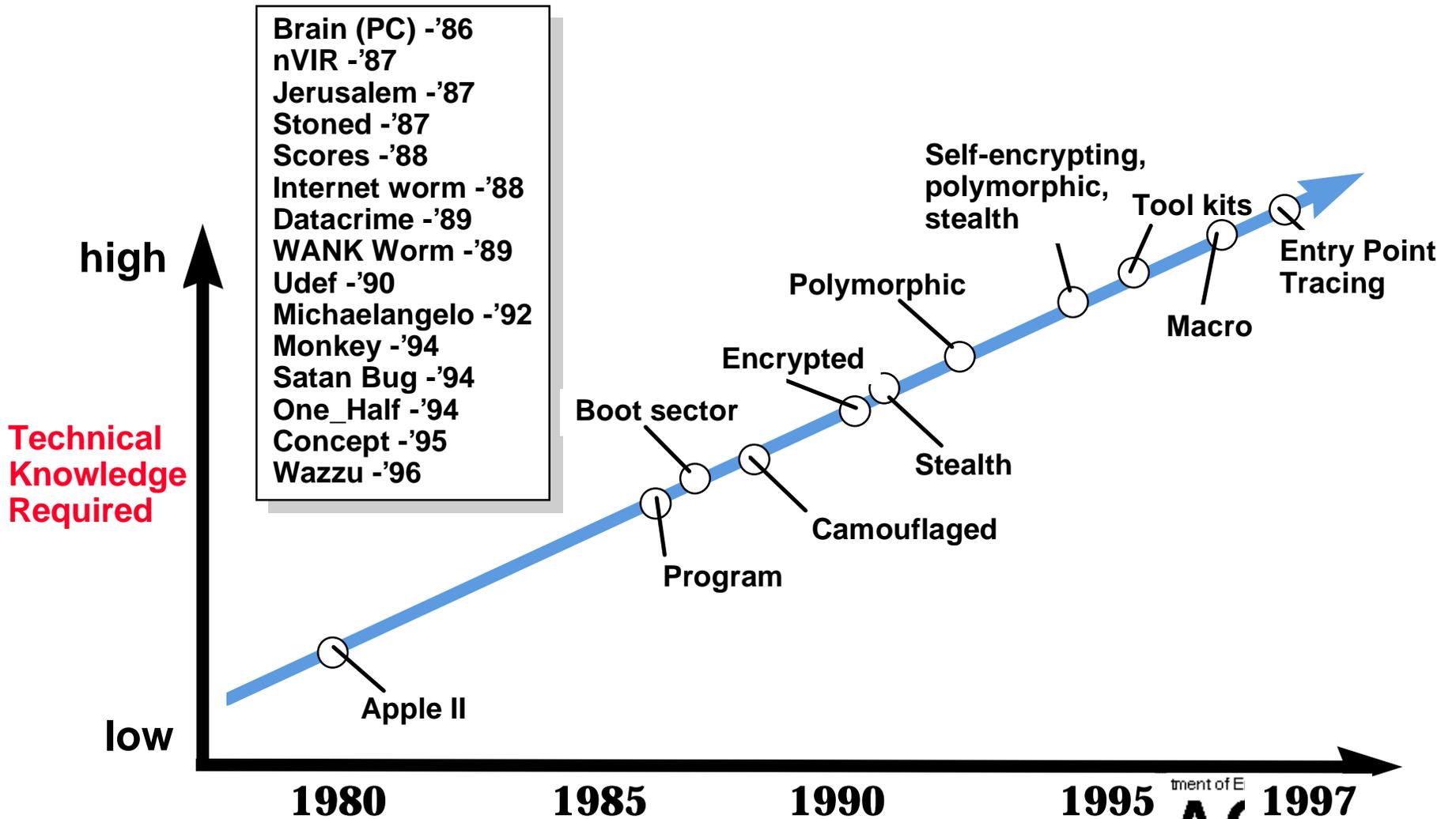
- **General web security is not adequate**
- **Web home pages being altered**
  - DOJ, CIA, NASA
- **Type 3 attacks will continue increasing**
- **phf attacks very common**
  - Thousands of systems scanned
  - Files stolen

# Virus incidents--1997

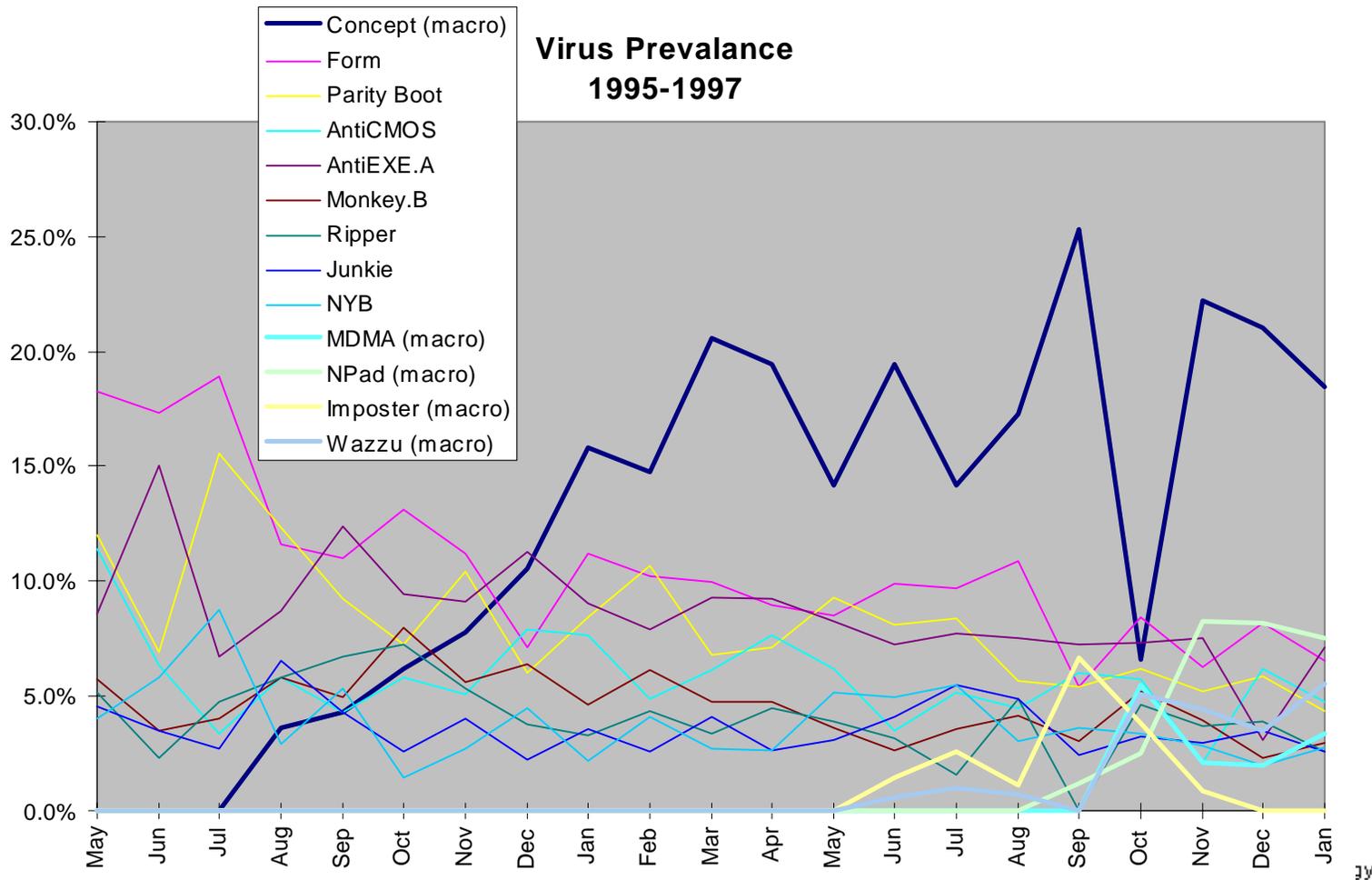
---

- **National Computer Security Association (NCSA) reports:**
  - In 1984,
    - One virus incident per 1000 PCs within a three month period
  - In 1996,
    - One virus incident per 1000 PCs per month
    - Between 9,500 - 11,000 viruses including more than 100 Macro viruses
- **CIAC also continues to experience growth in the number of virus incidents**
  - Virus incidents over the past two years are much more damaging than in the past

# Virus incidents are more damaging



# Virus prevalence chart



Source: Virus Bulletin, Virus Bulletin Limited, 1995-97



# What does the future hold? .....



- **More attacks on Microsoft products**
  - G-06A: Win95 Vulnerabilities
  - G-10A: Winword Macro Viruses
  - H-38A: Internet Explorer 3.x Vulnerabilities
  - H-45: Windows NT SAM permission Vulnerability
- **More hoaxes**
- **More DoS attacks**
- **Less trust in required services**

# More on Windows NT

---

- **Appears to be hacker's next target**
- **Public announcements of attacks**
  - **Scriptors of Doom to hit NT**
    - **Announcement by editor of Phrack Magazine**
  - **Emerging NT newsgroups**
    - **Bug reports starting to show up**
    - **New NT bugtraq**
- **Hackers don't do cost benefit analysis but . . .**
  - **NT provides a new area of challenge to hackers**
    - **Encouraged by promotion of NT "security"**
  - **NT supports the traditional network services that have been so effective in hacking Unix machines**

# Who and what can you trust? .....

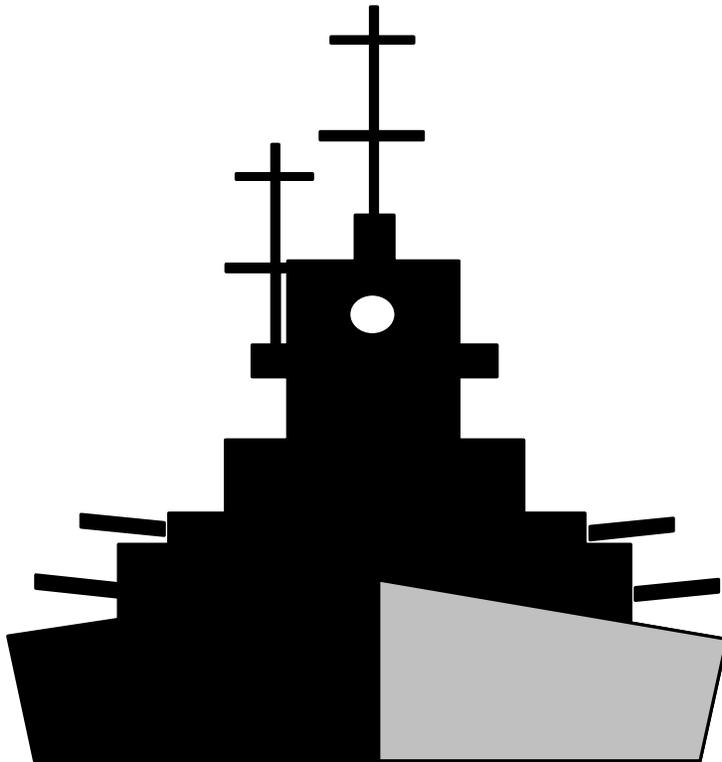
- **Hackers actively develop and use Trojan programs**
  - rootkit
  - <http://ciac.llnl.gov/ciac/bulletins/g-03.shtml>
  - AOL4FREE
- **IP Spoofing attacks are still active**
- **E-mail spoofing occurs**
- **Hoax messages propagate**

# Where are we today?

---

- **Prevention** through **protection**
- Incidents will happen, therefore **detection** is needed
  - One organization using NID reports that during normal business hours, they usually spot an intrusion as soon as it occurs

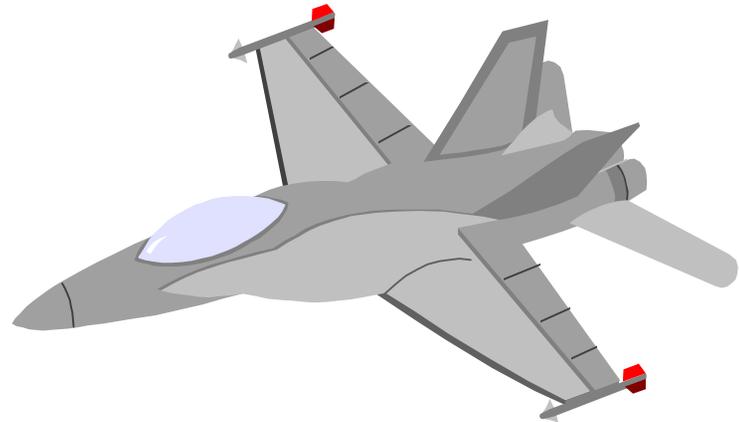
# How do we protect ourselves? .....



- Install firewalls and monitor them
- Monitor network traffic
- Segment internal networks
  - Makes it easier to protect key functions from compromises on other parts of your network
- Use secure connections
  - *ssh*
  - Tunneling
  - Imperative if working with off-site collaborators
    - Otherwise passwords are captured
    - Sensitive sessions can be tapped
- Monitor your most sensitive systems closely

# How do we protect ourselves? .....

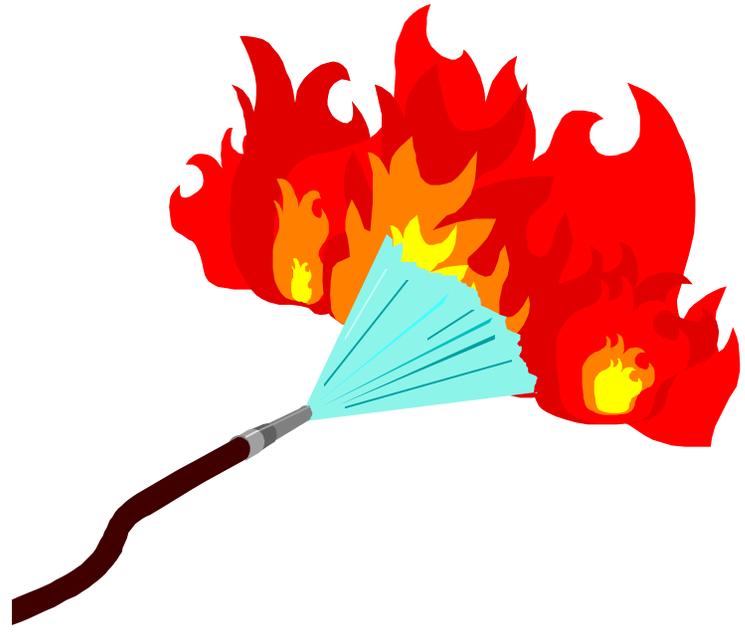
- Place public services outside your firewall
- Make your e-mail server single purpose with lots of disk space
- Use one time password (OTP) or at least, choose good passwords
- Use authentication and encryption
- Use antivirus (AV) software
- Develop risk-based, enforceable policies and procedures
- Provide awareness, training, and education



# But when malicious activities occur

---

**Detection is necessary**



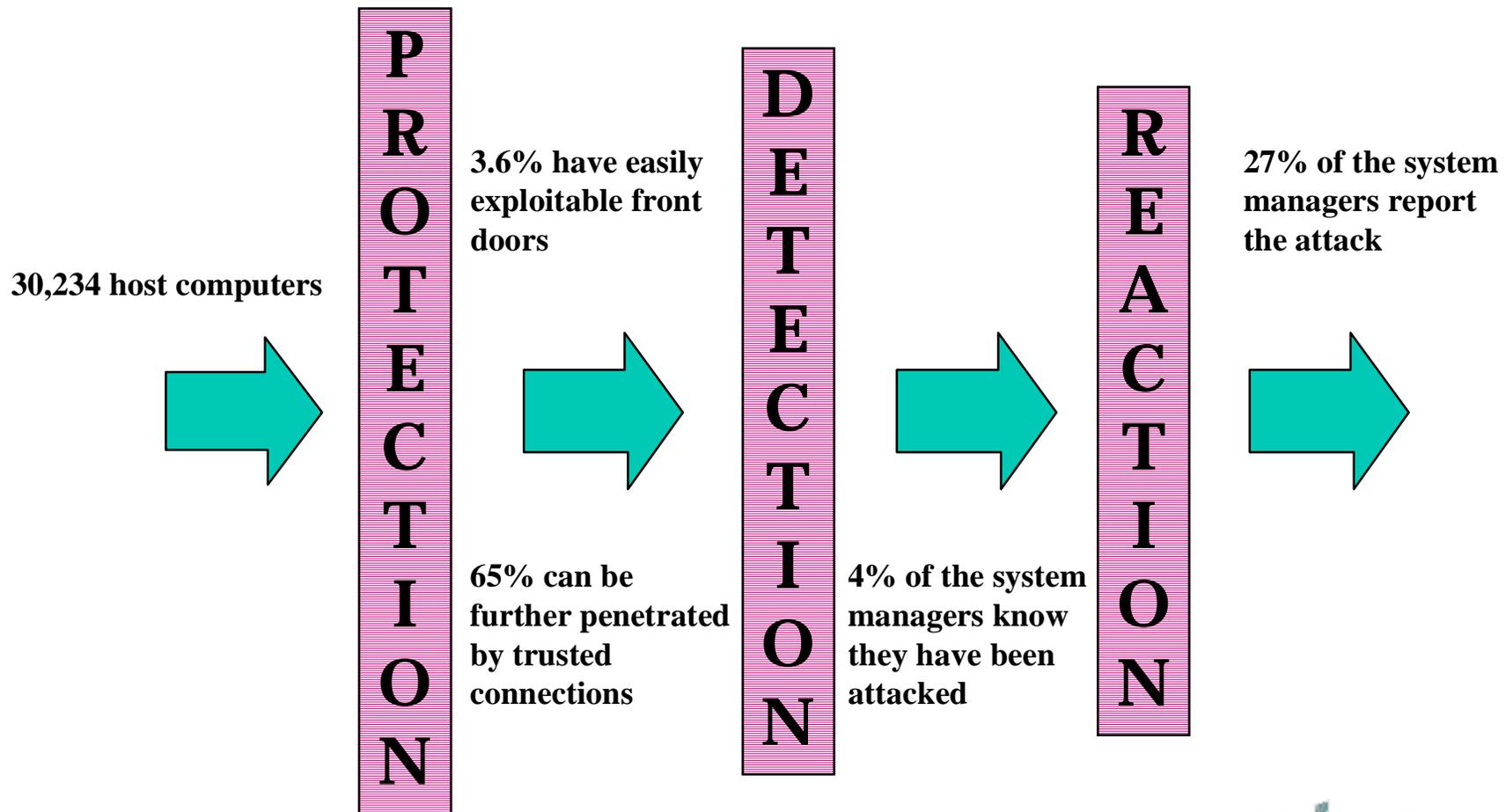
# Incident detection works

---

**Cheswick and Bellovin in *Firewalls and Internet Security - Repelling the Wiley Hacker* reported:**

**100** times as many incidents were detected with high quality intrusion detection in place than without it!!!

# Yet, most intrusions go undetected..



# So if it works, why . . .

---

- **... Are so many incidents not being detected (and damage controlled)**
  - Sites don't provide, and require the use of, up-to-date AV software
  - System administrators have other things to do in addition to reviewing audit logs
    - The size of the audit records produced in a day of normal use in a typical Unix-based timesharing environment is on the order of 100,000 characters [Proctor94]
    - A skilled system administrator, reviewing this much data manually, would need up to 2 hours/system
    - An unskilled system administrator, would need double this time
    - That is why intrusion detection tools and audit log reduction tools are so important

# DOE provides resources to help...

---

- **CIAC for incidence response**
- **Host security software**
  - SPI-net
  - SPI-NT
  - SSDS
  - Merlin
- **Network monitoring**
  - NID
  - NADIR
  - Courtney

# What one site is doing?

---

- **A centralized server for system administrators**
  - Tools
  - Bulletins
  - Training
- **Periodic scans with the SATAN looking for vulnerabilities**
  - From 95-96, quantum improvement
  - Lots of basic problems
  - Today fewer basics, different machines
  - Moving to Internet Security Scanner (ISS)

# CIAC services

---

- **Distribute more information via e-mail**
- **Greater use of the CIAC web server for “hot” news**
- **Asking for more details about your incidents**
  - Without your help, it is difficult to gather a comprehensive picture of the threat to the DOE complex
- **A survey regarding CIAC services**
  - Always looking for ways to serve you better

# CIAC's team today

---

- **Sandy Sparks**
- **Tom Christian**
- **David Crawford**
- **Marcey Kelly**
- **Paul Mauvais**
- **Bill Orvis 1/2**
- **Administrative support: Sandy Sydnor**

# Contacting CIAC

---

- You can contact CIAC by calling the:
  - Hotline: 510-422-8193
  - **Emergency Number: 1-800-skypage and entering pin number 8550070 (24x7)**
  - CIAC manager at 510-422-6856 or in an emergency at 1-800-skypage and entering pin number 8550074
  - FAX: 510-423-8002
  - STU-III: 510-423-2604
  - Internet E-mail: [ciac@llnl.gov](mailto:ciac@llnl.gov)

# Obtaining CIAC documents

---

- **CIAC's documents and other security Info.**
  - CIAC WWW server is available at <http://ciac.llnl.gov/>
  - CIAC anonymous FTP service:
    - [ciac.llnl.gov](http://ciac.llnl.gov) (IP address 128.115.19.60)
    - or via the www server
  - CIAC Bulletins/Advisories
    - send E-mail to: [ciac-listproc@llnl.gov](mailto:ciac-listproc@llnl.gov)
    - message: subscribe ciac-bulletins Full Name Phone Number

# Bibliography

---

- [Proctor94] P. Proctor, *A Computer Misuse Detection System*, 1994.