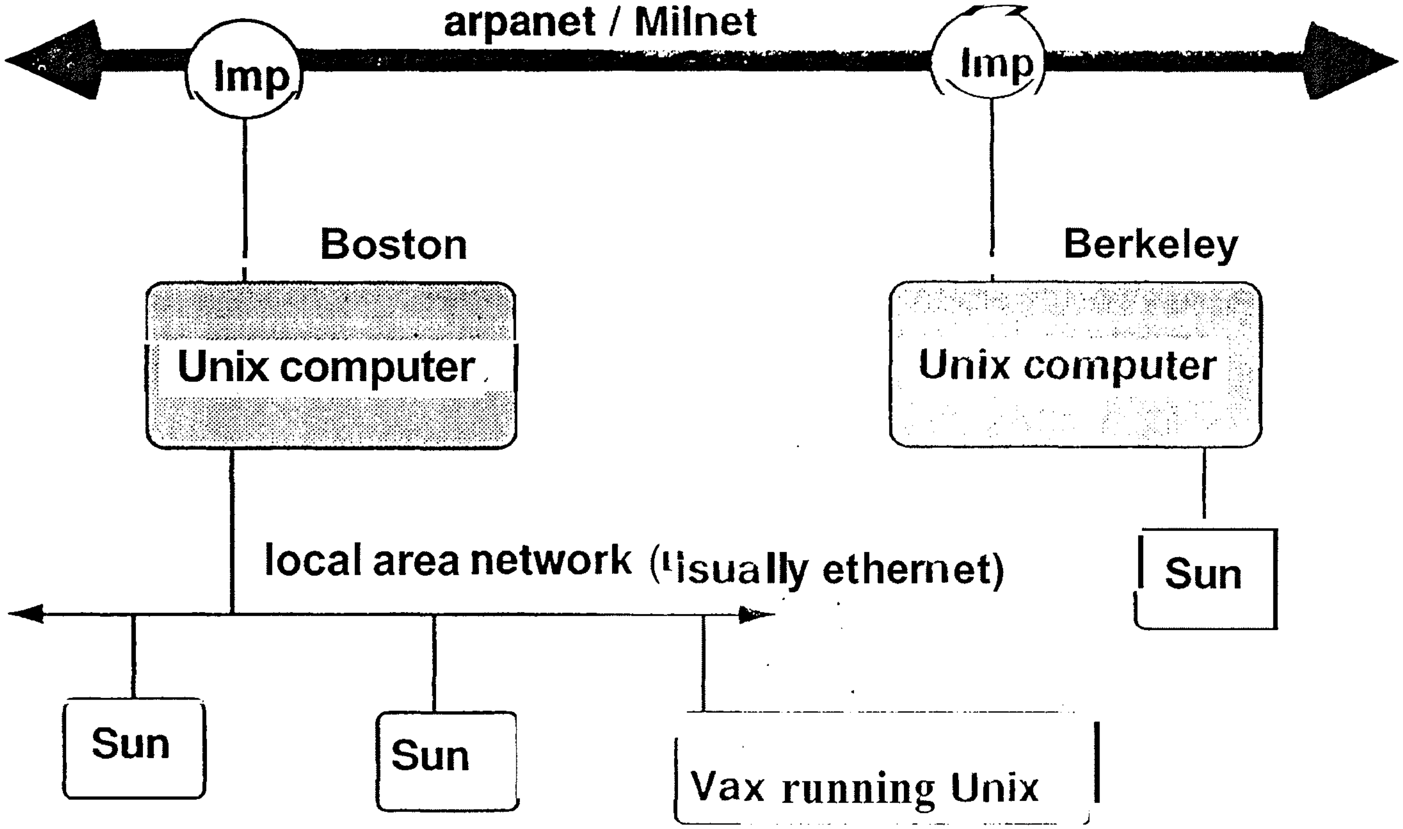
SITE EXPERIENCE

HARVARD

CLIFF STOLL

Arpanet as a Backbone



arpanet / Milnet

Imp

Imp

Boston

Berkeley

Unix computer

Unix computer

local area network (usually ethernet)

Sun

Sun

Sun

Vax running Unix

What holes did the Virus exploit?

- Sendmail

  Utility to copy network packets into mail files
  Sometimes used to move packets into processes
  (news feeds)

- Finger Daemon
  Utility to find out where someone is

+ The virus was specifically designed for Unix 4.3BSD it could not spread to non-unix computers, like a VMS system, or an IBM PC.

+ Sun workstations, Vax 780's and Vax 8800's were hit.

H'OWTO SOLVE A VIRUS

SOLVING A VIRUS

1 REVERSE ENGINEERING:
DISASSEMBLE THE MACHINE CODE
RECONSTRUCT THE ORGINAL PROGRAM
TRY TO UNDERSTAND IT

2 TREAT IT AS A BLACK BOX:
MONITOR ALL ITS INPUTS & OUTPUTS
FIND WHAT IT RESPONDS TO
. . . ITS TRANSFER FUNCTION

3 TRACK IT BACK TO THE AUTHOR

WAYS TO PREVENT SOLVING

1 HIDE THE CODE BY ENCRYPTION
MAKE SELF-MODIFYING CODE
ADD MISLEADING SEGMENTS
INSERT NON-OPERATING CODE

2 BUILD MANY DIFFERENT MODULES
MAKE IT TIME DEPENDENT
HAVE IT SENSE LOTS OF PARAMETERS
USE SEVERAL ATTACK MECHANISMS

3 START THE VIRUS FROM A DISTANT SITE
DON'T PUT YOUR NAME ON THE VIRUS

SENDMAIL BUG

- SENDMAIL: MOVES NETWORK PACKETS INTO MAIL FILES
  TRANSFERS NETWORK TRAFFIC INTO MAIL FILES
  CAN MOVE TRAFFIC INTO CERTAIN PROCESSES (FOR NETNEWS FEEDS)

- WHEN COMPILES WITH DEBUG, AND DEBUG IS SET
  LETS YOU SEND TRAFFIC INTO ANY PROCESS
  THROUGH A UNIX PIPE, WITHOUT CHECKING

  FROM:</DEV/NULL>
  RECEIVE TO:< /SED>
  MAIL BODY ....DATA TO SEND TO THE PROCESS

- SUN & BERKELEY UNIX DISTRIBUTED W/DEBUG ENABLED

  SO THIS BUG WAS IN 20,000 + COMPUTERS

PASSWORD GUESSING

- VIRUS ATTEMPTTO GUESS PASSWORDS BY READING THE LISTS OF USERS NAMES AND PERMUTATIONS OF THEIR NAMES

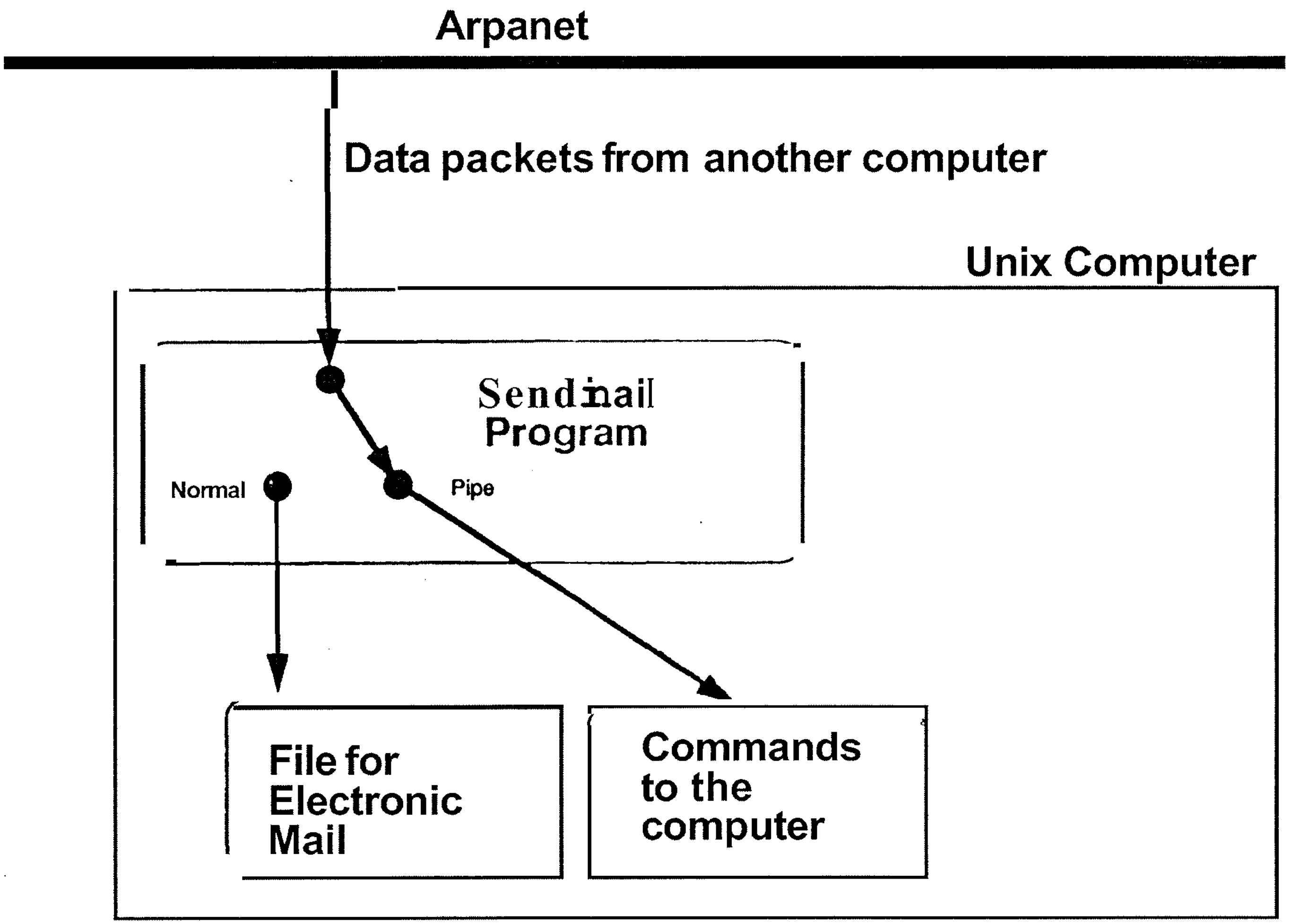
Quick Reaction Across the Nation

- UC Berkeley -
  Experimental Computing Center for Disease Control
- Stanford
- NASA/AMES
- Ballistics Research Lab
- MIT
- Lawrence Berkeley Labs
- Lawrence Livermore Labs
- Univ. Rochester
- Harvard-Smithsonian Center for Astophysics

Stamping it Out

- Initial cures: disconnect from networks
  reboot standalone
  erase the x files
  disable sendmail
  boot nearby computers
- Problem: virus reinfected from nearby computers (**.rhosts** especially)
  virus used other holes (fingerd, password crackinj)
  very frustrating
- Hard to communicate with other sites:
  many disconnected from network
  all the virus packets saturated some nets
  nobody was coordinating
- Hard to understand: encryption tough to disassembly

Exploiting a hole in Sendmail



Normally, data goes through the mailer into mail files.
Data can be sent as commands to special programs.
When Debug is enabled, data can be sent as commands any program

HOW MANY COMPUTERS INFECTED?

- THESE ARE GUESSES. I KNOW OF NO CENSUS

- HOW MANY COMPUTERS ARE ON THE ARPANET?
  ABOUT 100 CLASS A NODES
  CLASS A NODES ARE EXPLICITLY TARGETED

- HOW MANY NODES ON THE SUBNETS?
  ABOUTA HUNDRED PER CLASS A NODE?

e WHAT PERCENTAGE WERE INFECTED?
10%? 50%? AT HARVARD/SMITHSONIAN, ABOUT 80%
(NONE OF OUR DISKLESS NODES, BUT THEN THEY WERE USELESS WHEN THE FILESERVER WAS DEAD)
AT LAWRENCE BERKELEY LABS, ABOUT 50% WERE INFECTED

- *SO* ABOUT 1000 TO 10,000 COMPUTERS WERE HIT.

Virus or Worm?

Virus: Self replicating program that infects other programs

Worm: Program that snakes through computers, copying itself from one system to another.

Purists would call this a worm, not a virus. Makes’no difference to me.

Previous Viruses & Hacks

- '84 - 88 On personal computers:
  replication by infecting programs.
  Medium of transport: floppy discs & phone lines to bulletin boards

- 86 - '87 Intruders manually break into computers
  to embarrass companies, wreck programs, or steal information.
  Medium of transport: dial-up phone lines, networks

- '87 IBM Christmas tree virus:
  Replication by distributing a command file to many people.
  Each person executes the file & it mails itself to many others.
  Medium of transport: SNA networks, Bitnet

- '88 Arpanet virus: self replicates by entering Unix systems & breaking security to obtain a root shell. Medium of transport: TCP/IP networks (Arpanet/Milnet, local area networks)

☞This is the first virus to spread automatically across the networks.
The first virus to exploit multiple security holes

REAL EFFECTS

- HOW MUCH DAMAGE WAS DONE?
  10,000 PEOPLE LOST 2 DAYS OF WORK; AT $100/PERSON-DAY = $2,000,000

- INDIRECT COSTS - OPERATIONS DISRUPTED, SCHEDULES DELAYED

- CONSCIOUSNESS RAISING ABOUT COMPUTER SECURITY

- DID THIS GUY DO US A FAVOR BY SHOWING OUR VULNERABILITIES?
  WAS IT NECESSARY?
  A MONTH AGO, COVER OF TIME MAGAZINE WAS ABOUT VIRUSES!

What to learn

- Networking makes the problem much worse.
- Our society depends heavily on interlinked computers military, university, commercial systems are intertwined
- There's no central coordinating center or clearing house for emergencies.
- Nobody's in charge of our networks
- Security holes are subtle; introduced from strange sources and exploited by competent, aware people.