SITE EXPERIENCE

MIT

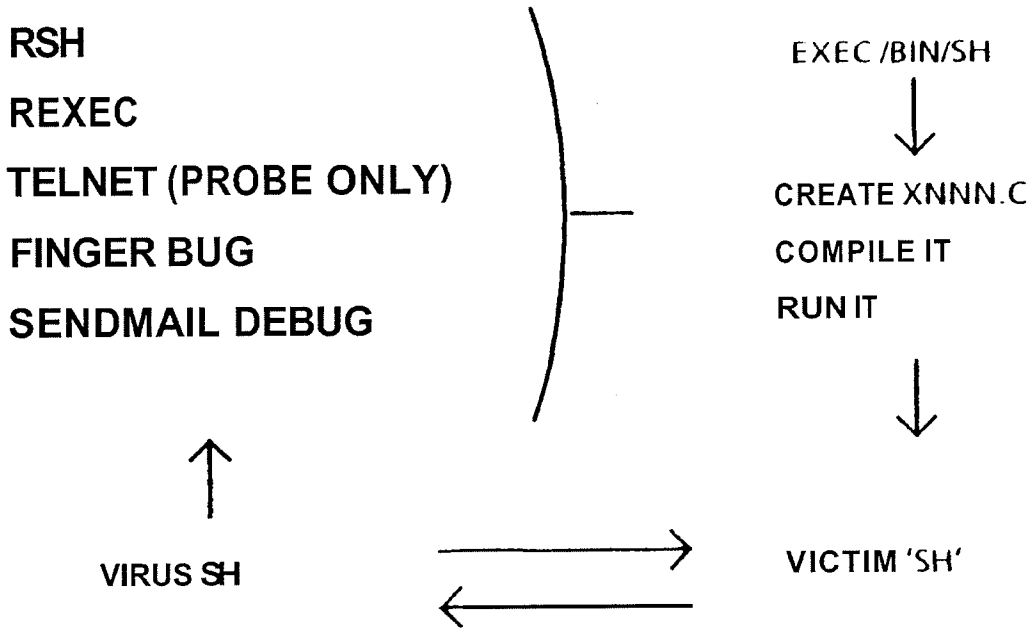
D. ALVAREZ
M. EICHIN
J. ROCHLIS

TACTICAL/MANAGEMENT ISSUES

- o SMALL GROUPS 3 TO 5 +
- o PHYSICAL PROXIMITY
- o FUNCTIONAL BREAKDOWN
  - COORDINATING
  - PROTECTING
  - RESEARCHING
- ● INTERGROUP CONTACTS
  - "OLD BOY NETWORK"
  - TELEPHONES - CAREFUL OF IDSN
- ● 16 HOURS TO COMMANDS POST
- ● 3 HOURS TO SECURE (THANKS PETER YEE)
- ● FEAR/MORALE/COCKPIT ERRORS
- ● REPORTING KEY TO INTEGRATING - SECURITY COMMUNITY INTO SYSTEM MANAGER COMMUNITY
- ● EMERGENCY BROADCAST NETWORK - 1200 BAND DIGITAL TAPE RECORDER

DON ALVAREZ

MIT SITE EXPERIENCES



MARK EICHIN

MIT SITE EXPERIENCES

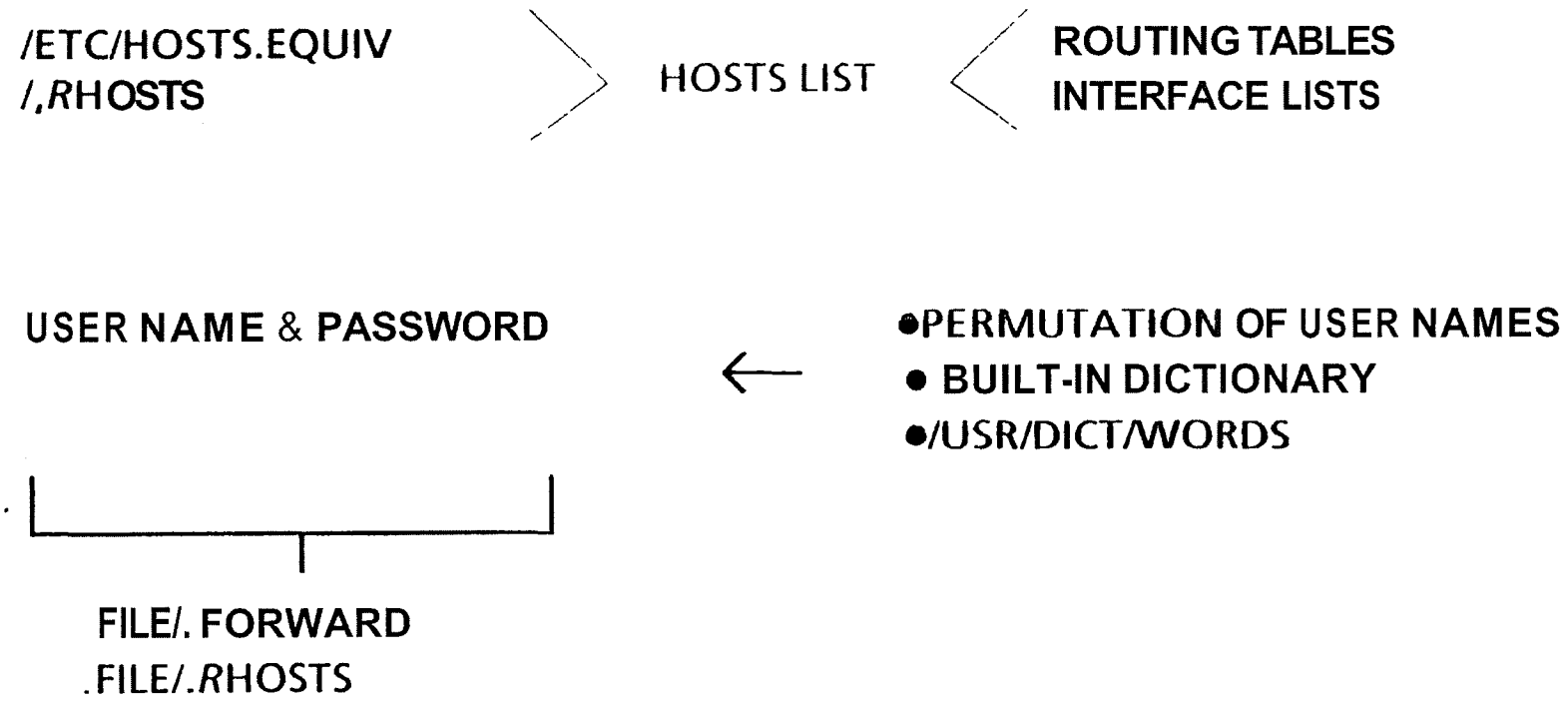
JOHN ROCHLIS, MIT NETWORK GROUP

MARK EICHIN, MIT PROJECT ATHENA

- STUDENT INFORMATION PROCESSING BOARD
- PROJECT ATHENA 'WATCHMAKERS'
- MIT LAB FOR COMPUTER SCIENCE
- MIT MEDIA LAB

"THE INTERNET VIRUS OF NOVEMBER 3, 1988"

MIT SITE EXPERIENCES



MARK EICHIN

Don Alvarez
MIT Center for Space Research

boomer@space.mit.edu
(617) 253-7457

Observations on [illegible] to rpan Virus at MIT

1. Work was performed primarily by small, isolated **groups**. **Three to five** members seems typical.

2. Groups seem to form first by **physical proximity**, then connect to other groups through "**old boy network**".

3. Groups seem to break along **functional lines**:
   Coordinating and communicating information.
   Protecting and disinfecting machines,
   Researching and disassembling virus.

4. Most sites were able to **isolate and secure** their machines in about **three hours** after receipt of **Peter Yee**'s message.

5. Very little effort made to contact persons not in "old boy" network. **little effort** to contact government, etc. until quite late.

6. Initial **inter-group** communications primarily over **telephones**. Some later communications possible by **computer mail**.

7. Groups worked largely in a **vacuum**, isolated from others simply because they **did not try** to contact others.

8. [illegible] **unnecessary** duplication of effort.

9. [illegible] **10 hours** before any kind of central **command** post was set up at MIT. Post came about largely when two very competent groups began working on disassembly of virus and needed to **pool resources**.

10. Most sites seemed to have **expected** (and experienced) relapses due to incomplete inoculation, but were not **concerned** by this.

11. Group members seemed to be hit by **fear** only when the virus reinfected supposedly "**safe**" machines **long after** the threat was believed over (as with the finger daemon attacks). The illusion of security was **shattered**.

Don Alvarez
MIT Center for Space Research

boomer@space.mit.edu
(617) 253-7457

om ions for the the Future.

1. **Safe use of telephones** is essential. Information on the virus could not have been transmitted between workers without them. **Mixed voice/data** systems make cleanup much more difficult and **dangerous**

2. **Greater mixing** between system managers and government security professional is necessary if a **nationally coordinated** response is to be possible in the future. Most system managers don't know any security professionals, and hence can not include them in their "**old boy network**"

3. A two-pronged, **time-delayed** attack would be extremely demoralizing, particularly if the second attack was timed to hit just when groups were **disbanding** and felt a sense of confidence and security from their work.

4. A computer equivalent of the **Emergency Broadcasting Network** would be extremely important. **Peter Yee's** message was probably the single most decisive factor in a timely response to this virus. Suppose **UUNET** had gone down. The emergency system could take the form of a large bank of phone lines terminating in a **digital tape recorder** containing auto-answering at 1200 or 2400 baud. (This solution would be much cheaper than an equivalent bank of modems and less susceptible to hacking). Users would be able to upload system patches and code from this **clearing house** in a timely manner