# SITE EXPERIENCE

## ARMY BALLISTIC
## RESEARCH LAB

M. MUUSS

Post-Mortem of 3-Nov ARPANET Incident

# The Ballistic Research Laboratory Anti-Viral Program

*Michael J. Muuss*

The Advanced Computer Systems Team
U S Army Ballistic Research Laboratory

# “VIRUS” **From Websters 9th**

- From Latin: slimy liquid, poison, stench.
- Causative agent of an infectious disease.
- Complex molecules capable of growth and multiplication only in living cells.

# GLOBAL OUTLINE

- BRL
- History of Events
- The People Involved
- The BRL Approach
- Attack & Propagation Modes
- Network Sweep Tools
- Fixes
- BRL Status

# What is BRL?

- U. S. Army Ballistic Research Laboratory
- One of America's foremost research and development labs.
- 700 Scientists & Engineers pursuing in-house research programs
- 5 Scientific Divisions
- 3 Support Divisions
- Networked Computers are all pervasive: throughout research **and** administrative staffs
- > 200 systems
- UNIX Cray X-MP/48 and Cray-2

## History, Part 1

*o* 1800 PST Wed: virus seen at Rand Corp.

- 2345 EST Wed: virus enters VGR.BRL.MIL.
- 0300 Thu: VGR was seen attacking other machines.
- 1000 Thu: BRL disconnected from MILNET, DISNET. NSI; VGR totally isolated.
- 1200 Thu: BRLXET checking complete: no virus on inside.
- 1600 Thu: Coordinating w/other researchers. DCA orders MILNET hosts shutdown. blows MIL/ARPA gws.
- 2200 Thu: Virus. was Lead story on CNN
- **2300** Thu: VGR "Test Cell" prepared, connected to MILNET.

## History, Part 2

- 0645 Fri: MIL/ARPA gateways restored
- 0030 Sat: Virus trapped in "Test Cell", UCB src rcvd.
- 0630 Sat: BRL-wide power outage (sigh)
- 0600 Mon: 2 Additional attack modules rev-eng.
- 1200 Mon: BRL "Vulnerability Sweep" programs operating
- 1600 Mon: Patched servers installed
- ~1200 Tue: reattach BRL to network

## Who BRL Worked With Through the Night

- Tim Smith, US Naval Academy
- Cliff Stoll, Harvard
- Keith Bostic, Berkeley
- Rick Adams, Seismo

a Jenny, CONUS MILNET Monitoring

e Bob Fields, CONUS MILNET Monitoring

- CPT Bill Arbaugh, Pentagon
- Peter Yee, NASA/Berkeley

# The BRL Approach

- Use instrumented “Test Cell”
- Analyze attack modes
- Coordinate community efforts via telephone
- Assist with reverse engineering
- Relay info on attack modes (incl flukes):

— 2nd priv inetd (3 sites)

— Ingres lock daemon

— System accounting

# The Attack Modes

## External

a Sendmail SMTP Server

- Finger Daemon

## Internal

e Password attack [word list]

- /.rhosts

- /etc/hosts.equiv

- .forward

# After Penetration

- “Gorch Attack” — sends l1.c sources, compiles and run.
- ‘‘L1, Loading’’ — gets Sun and VAX obj from network.
- ‘‘L1, Shell” — Links 2nd stage: ‘‘P’’
- ‘‘P Attack’’ — Crack & Propagate

# Network Sweep Tool

+ Finger Daemon buffer over-run

— FTP bugs

— TFTP bugs

— passwd/rsh

+ SMTP/Sendmail [Wiz, Debug]

a40: Tue Nov 8 07:59:04 EST 1988

## Fixes

- Improved fingerd, with logging
- FTPD fixes
- TFTPD fixes

- Code installed on VAXen, Suns: Goulds
- In progress on Crays, Alliant, Convex: SGI
- BRL has source code licenses.

## Books, News

- ‘‘Adolescense of P1’’
- ‘‘Sole on Saphire”

- Press Coverage was remarkable good. My congratulations to the Public Relations folks.
- My fear: these headlines:

  ‘‘Computer Virus Spreads to Humans: 96 Left Dead...’’

# BRL Status

- No information lost
- Minor disruption of work schedules due to network disconnection
- BRL Computers now secure against this threat
- Anti-Viral Team used ~500 man-hours
- Incidental people used ~1000 man-hours

— Copy of virus still captive in test cell

# Who is This MUUSS Fellow, Anyway?

Michael Muuss
Leader, Adv. Computer Systems Team
Ballistic Research Laboratory
APG, MD 21005-5066, U.S.A.

(301)-278-6678
AV 283-6678

ArpaNet: <Mike @ BRL.MIL >

# The BRL “Virus Busters”

- Mike Muuss
- Phil Dykstra
- Doug Gwyn
- Terry Slattery
- Bob Reschly
- Sue Muuss
- Lee Butler [NASA STScI]