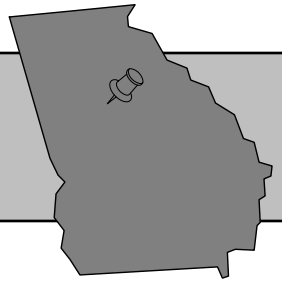
TCP/IP Security



Survival on the Internet

1992 Spring DECUS Symposium - Atlanta, Georgia

Session SE136/NE153, Monday 4 May 1992, GWCC 160

Presented By

John "Fast-Eddie" McMahon

TGV, Incorporated

603 Mission Street

Santa Cruz, California 95060

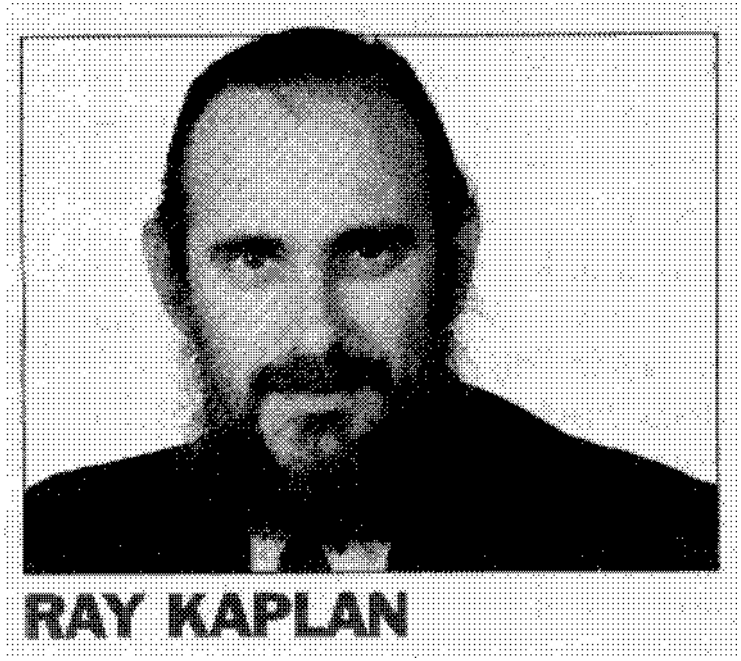
800-848-3440

MCMAHON@TGV.COM

Survival on the Internet

"Would the bad guys please stand up ?"

Borrowed (without permission) from Ray Kaplan



Survival on the Internet

Disclaimer

- All of the information in this talk was derived from public sources. It is presented for informational purposes only. Neither the author, nor his employer, assume responsibility for any use of the information contained in this presentation.
- We talk about testing in this session. I advocate using these ideas to verify that your systems are secure. I do not advocate using these techniques to go test a system that doesn't belong to you.
  - If you do go test someone else's system I hope they lock you up in a nice cell for a long time.
- Please, no tomato throwing until the Q&A period.

Survival on the Internet

A related session you should see this week

- "An Evening with Berferd: Fun With Internet Security"
  - By Bill Cheswick of AT&T
  - Tuesday at 6PM in GWCC 367
  - UN049/SE143

Survival on the Internet

A few common misconceptions

- The Internet is dangerous
  - No. It is an unsecure network with a lot of people on it.
  - Not all of those people are "good guys."
  - Benefits of connectivity are usually greater than the risk, especially if you take steps to reduce the risk.
  - Your machine is probably tied to an even larger network that has bad guys on it, the POTS (Plain Old Telephone System).

Survival on the Internet

A few common misconceptions

- Data Encryption
  - Currently, data is not encrypted on the Internet. Everything is carried across the wire in "plain text".
  - Any data encryption is handled by the application program, not by the underlying network layers.
  - Most applications were not designed to encrypt data before transmission.

Survival on the Internet

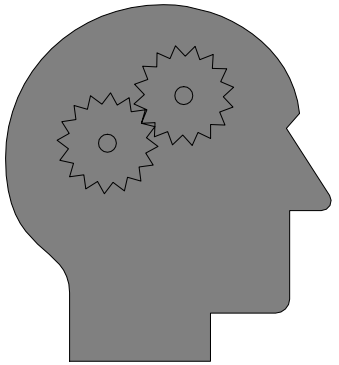
A few common misconceptions

- Fix It Once
  - Everything in Computing changes.
  - Anything, from a network topology change to a software upgrade can influence security.
  - Test your systems carefully and thoroughly on a regular schedule. Don’t assume that any security issue is permanently closed.
    - That is, unless the machine is unplugged and buried in 30 feet of concrete on the Moon!

Survival on the Internet

A few common misconceptions

- The company Security Officer says my system is safe
  - It's your system and your responsibility to keep it running.
  - Take advice, but also take charge of securing YOUR system.
  - Security Officers (sometimes) are people with big titles and little brainpower.
    - On the other hand, some are brilliant. Your mileage will probably vary.



Survival on the Internet

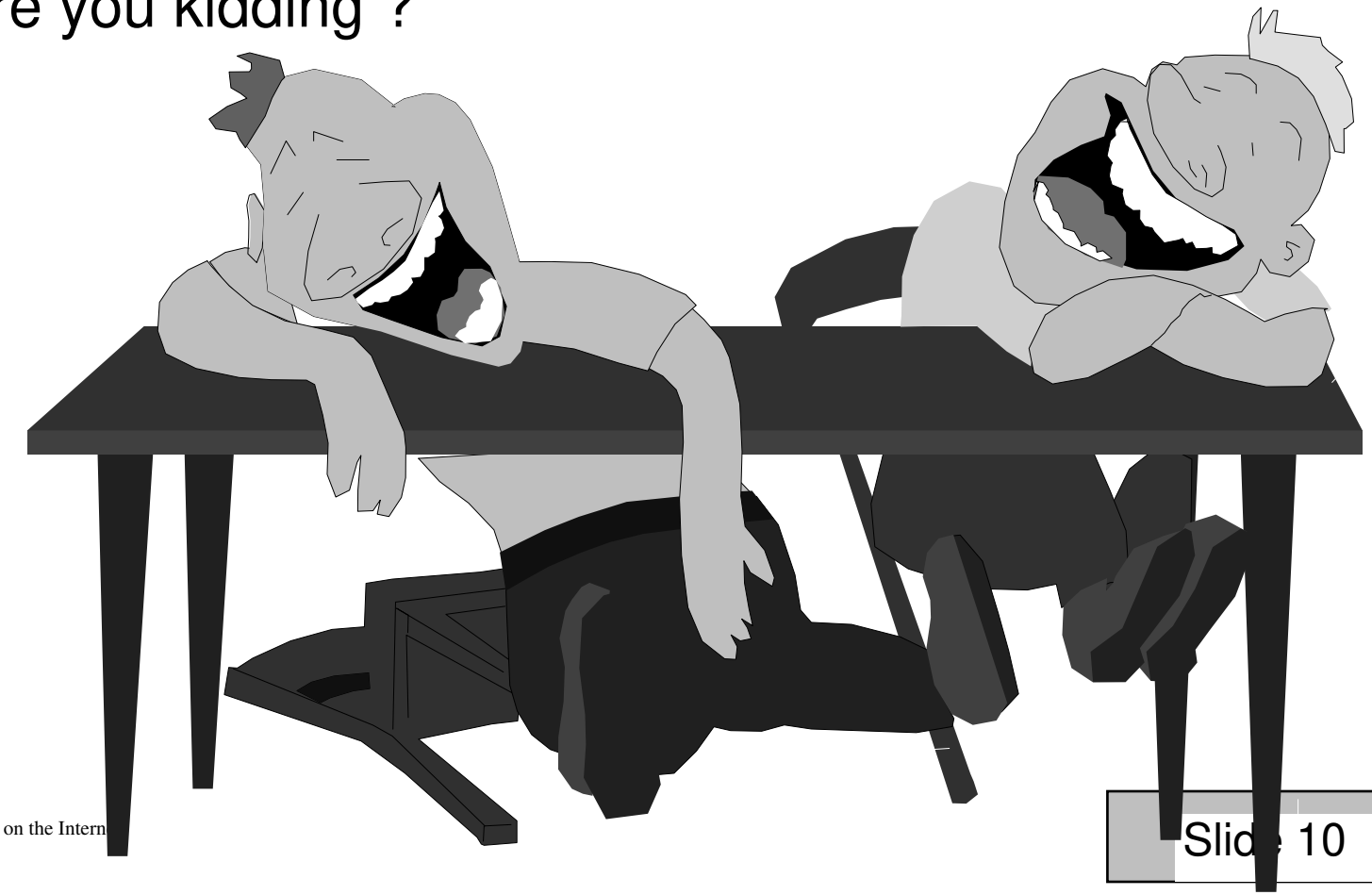
A few common misconceptions

- Accounting does nothing but consume disk space
  - Accounting Data = Evidence
  - Evidence can lead to a Conviction.
  - You can’t hang the guy who is breaking into your machine unless you can prove it.
  - Have you read "The Cuckoo’s Egg" ? That whole story started with a 75 cent accounting error!

Survival on the Internet

A few common misconceptions

- This guy McMahon is a security expert
  - Are you kidding ?



Survival on the Internet

Problems/Testing/Correction

- Passwords
  - Without good passwords any additional security measures are worthless.
  - Investigate the password history ("I'm sorry... you can't continue to use the same password.") and password syntax ("The word 'secret' is an invalid password. Try again.") capabilities of your system. You can help (force) your users to pick better passwords.

Survival on the Internet

Problems/Testing/Correction

- Passwords
  - Avoid generators that create such gook that your users are forced to write down passwords just to be able to get back into the machine.
  - No sense in boarding up the basement windows if you leave the front door wide open.
    - Apologies to Bill Cheswick who points out the vice-versa case is true.

Survival on the Internet

Problems/Testing/Correction

- Applications that use passwords
  - Several networking protocols use passwords to verify authentication.
  - Examples:
    - PCNFS (NFS authentication services for PCs)
    - REXEC (Remote command execution)
    - FTP (File transfer)
    - POP (Remote mail storage)
  - Depending on vendor implementation, password checking may not be wired into the accounting system or break-in detection.

Survival on the Internet

Problems/Testing/Correction

- Applications that use passwords (con't)
  - As a result, a cracker could use these services as a remote procedure call for password guessing.
  - Any of these can be tested by using a client and sending a few bad passwords to the server. Then check your system accounting or OPCOM for signs of trouble.
  - No signs of trouble ? Make sure you are at the current revision level for these servers. If you are, start screaming at your vendor.

Survival on the Internet

Problems/Testing/Correction

- TFTP
  - Trivial File Transfer Protocol used to support diskless booting of machines.
  - Similar in function to DECnet MOP.
  - No password protection!
  - First question you should ask youself is

    "DO I NEED TO RUN TFTP ?"
  - This service is pretty worthless unless you are downloading diskless machines. FTP is a much more robust (and usually safer) protocol.

Survival on the Internet

Problems/Testing/Correction

- TFTP (con't)
  - Some versions of TFTP may allow capability to download ANY file off your system. This is a typical bug in older UNIX systems.
  - Cracker could use TFTP to grab key files that contain information useful to the cracker (e.g. /etc/passwd, RIGHTSLIST.DAT, secret-formula-for-coca_cola.txt).

Problems/Testing/Correction

- TFTP (con't)
  - Testing can be performed using a TFTP client. Can you grab files other than the proper download images ?
  - Problems ? Upgrade your software to current revision levels. Check to see if there are download restrictions that can be applied to the TFTP server (e.g. UNIX chroot). Yell at your vendor!

Survival on the Internet

Problems/Testing/Correction

- Anonymous FTP
  - Allows a user to log into a system as a guest to download public files.
  - Although passwords are used, typically "guest" or a valid e-mail address is accepted for entry. Passwords are used to provide information to the server, not for authentication.
  - If misconfigured, could allow a user to upload files or download files from any part of the system. This is similar to the problems with TFTP.

Survival on the Internet

Problems/Testing/Correction

- Anonymous FTP (con't)
  - Can be tested with a FTP client. Can you CD (Change Default) to any directory on the System ? Can you download any files other than the ones that are in the Anonymous directory ?
  - UNIX Anonymous FTP often requires access to a /etc/passwd style file as part of the configuration. It shouldn't be the same one as your real /etc/passwd file.
  - Problems ? Anonymous FTP problems often are the result of misconfiguration. Check your user documentation and installation first. Call your vendor if you can't fix the problem.

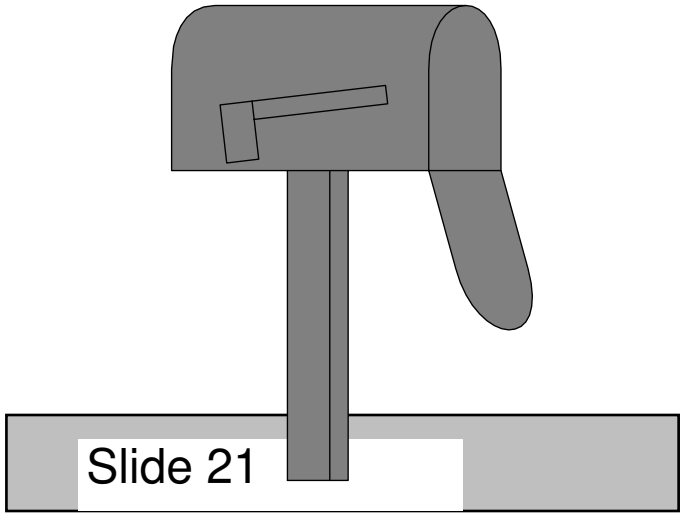
Survival on the Internet

Problems/Testing/Correction

- Bogus Mail
  - Design of SMTP mail provides no verification that the mail actually came from the person that it claims to be coming from.
  - It's a design flaw... you can't fight it.
  - Short term resolution: Teach your users that SMTP mail can be untrustworthy. Use your head while reading your mail. Try to use a mailer that has connection logging capability.
    - Last time we checked, George Bush doesn't have a public E-mail account, so if you get mail from him... be suspicious.

Problems/Testing/Correction

- Bogus Mail (con't)
  - Note: DECnet Mail-11 has the same design flaw.
  - Long term resolution: Additions to E-mail to provide "digital signatures" using public-key (RSA) cryptography. It's being tested now. Standards and implementations are coming soon.



Survival on the Internet

Problems/Testing/Correction

- Mail Servers with "extra" functionality

  Aliases that run programs:

  - A SMTP mail server may have additional functionality built into it in the form of a mail alias. These mail aliases typically pipe the mail message into a program.
  - The message is used either as a source of data or as commands.
  - E-mail based servers are based on this technique.

Survival on the Internet

Problems/Testing/Correction

- Mail Servers with "extra" functionality

  Aliases that run programs (con't):

  - Problem: Some vendors install 'nifty' aliases which perform file decoding (e.g. UUENCODE files) and write the files into the file system. With a bit of tweaking, the server could replace your SYSUAF.DAT file or any other system file.
  - Testing: Check your configuration files for "non-user" aliases. Figure out what they do, and whether or not they have boundary checks on them. A good one to look for is the 'decode' alias in older versions of UNIX sendmail.

Survival on the Internet

Problems/Testing/Correction

- Mail Servers with "extra" functionality

  Debug routines:

  - Some mail servers have a set of commands to allow a user root/SYSTEM access to a system via the MAIL server. These features were intended to be used for debugging the mail server only.
  - At least one vendor has (in the past) shipped their production code with the debugging commands enabled.
  - Bug became "well known" and "popular" thanks to

    Robert T. (expletive deleted) Morris Junior, who used this trick in the Internet worm program.

Survival on the Internet

Problems/Testing/Correction

- Mail Servers with "extra" functionality

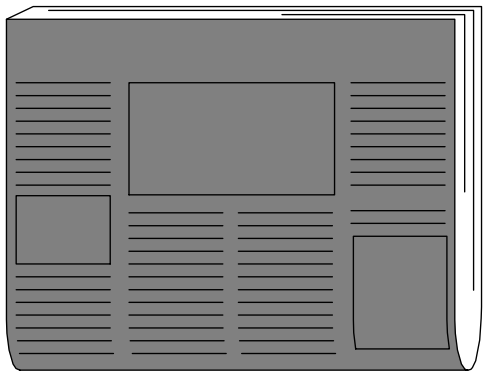
  Debug routines:

  - Testing: Use TELNET to connect to the SMTP port (25). Issue the DEBUG command. If you receive a reply of "500 Command Unrecognized" you are safe. If you get "200 Debug Set" you are in trouble. Repeat with the "WIZ" command.
  - Always try to run the most current version of sendmail. Older versions (pre-5.59) had this bug. If you are using a commercial port of sendmail, make sure it is the vendor's latest and greatest version.

Survival on the Internet

Problems/Testing/Correction

- Bogus USEnet
  - Design of NNTP provides no verification of where an article really came from.
  - Tell your users, they need to know this.
  - Fixing: Problems that originate at your NNTP server could be curbed by installing the NNTP authentication hooks. This forces a user to send a Username/Password before posting.
    - This is not implemented heavily, but it is gaining popularity.



Survival on the Internet

Problems/Testing/Correction

- Trusted "R" services
  - Examples: RLOGIN, RCP
  - Not the REXEC service.
    - REXEC uses passwords.
  - Allows users in system without passwords. Authorization is dependent on files stored in a system area (HOSTS.EQUIV) or in a user's account (.RHOSTS).
  - Question: Are these files (and the directories) World or Group writeable ? Can someone else create or change these files ?

Problems/Testing/Correction

- Trusted "R" services
  - If you allow users to use R services from "off-site," you are now betting your security on machines that you may not administer. If someone cracks the remote system, they can hop over to yours quite easily without the bother of a password or any challenge/verification.
  - Consider auditing .RHOSTS files put in place by users. Check for entries that are off-site.
  - One advantage of "R" services worth mentioning: no clear-text passwords are transmitted between the client and server.

Survival on the Internet

Problems/Testing/Correction

- NFS
  - Bad export lists may allow access by remote (unauthorized) clients.
  - Can someone mount your file systems without explicit entries in the /etc/exports (or equivalent) file ?
  - Exported archive disks ("Anonymous NFS")
    - Export them as read-only to prevent tampering

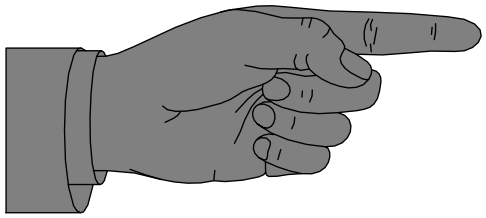
Problems/Testing/Correction

- NFS (con't)
  - Test with the SHOWMOUNT command to see export restrictions on a remote server, or just try mounting a file system that is supposed to be restricted.
  - Servers usually allow you to export with or without the client having root access. Best to export "root" only to other machines you administer or trust.

Survival on the Internet

Problems/Testing/Correction

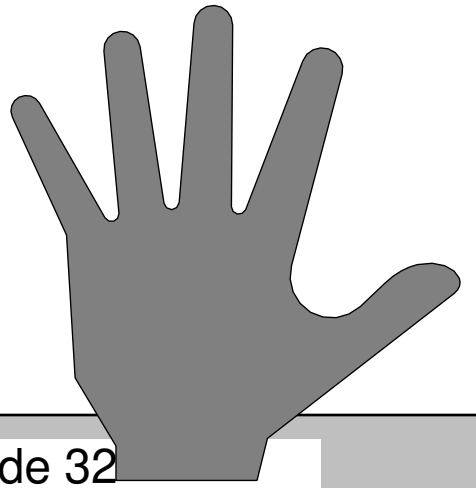
- FINGER
  - Another Morris Worm problem.
  - FINGER could be misused to issue shell commands to the UNIX operating system under user root.
  - Solution: Install the latest software. The problem has been corrected by your vendors.



Survival on the Internet

Problems/Testing/Correction

- FINGER
  - Question: Anyone can FINGER your machine to get information from your users. Is this information useful to crackers ?
    - That question opens up a BIG can of worms!



Survival on the Internet

Problems/Testing/Correction

- Non-Priv'd TCPDUMP/ETHERFIND
  - TCPDUMP/ETHERFIND - Poor Man's Ethernet/FDDI Packet Analyzer
  - Typically requires root or SYSPRV or something to run.
  - Do not "install" this image so everyone can use it.
    - These programs provide dumps of the data in network packets. Including unencrypted passwords!
  - The tools are useful in the right hands (e.g. the Network Manager) but not in the hands of every user.

Survival on the Internet

Problems/Testing/Correction

- Non-Priv'd TCPDUMP/ETHERFIND
  - Such programs are not hard to write, even on "simple" machines like PCs
    - Ethernet/FDDI link level encryption may be the only (costly) solution.

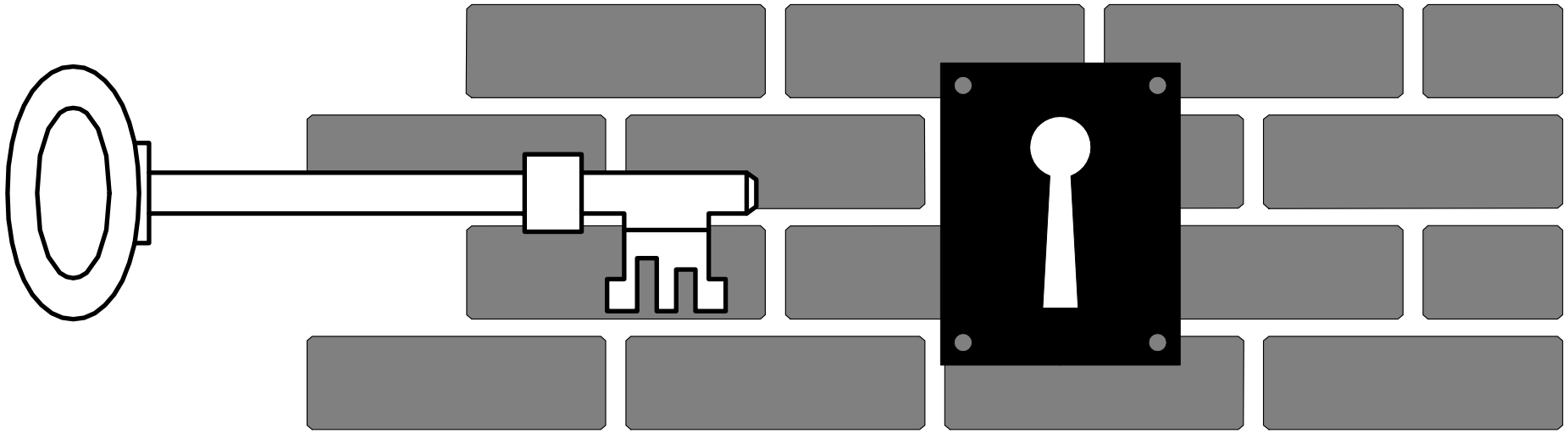
Survival on the Internet

Problems/Testing/Correction

- X windows
  - X windows allows a remote client program to access resources on the server. These resources include the contents of the screen and what keys are typed on a keyboard.
  - Many users turn their security completely off because they find dealing with X security annoying.
  - Result, cracker writes program to monitor remote "open" X workstation. Reads password out of a DECterm window. Game over.
  - Solution: Educate your users about good X windows security.

Firewall

- Definition
  - A software/hardware construct that acts as a mechanism to selectively allow traffic between the Internet and your machines.



Firewalls

- Host Protection: Application Server Firewall
  - The server program (Telnet, FTP, RLOGIN) or server dispatcher (inetd, MASTER_SERVER) is designed to check an access list before accepting the connection.
  - Typically the access list is nothing more than a list of valid IP network/node numbers.

Firewalls

- Host Protection: Application Server Firewall (con't)
  - Requires that the application be coded to do this.
    - Hopefully your vendor has already done the hard work for you.
  - Very useful when you don't want to grant access to every service to every node on the net.
    - E-mail from anywhere is probably ok, but we probably don't want an FTP connection coming in from our competition.

Survival on the Internet

Firewalls

- Host Protection: Packet Accept & Reject
  - Policy module loaded into VMS kernel space at system boot.
  - Headers for every received packet are sent to the Policy module for approval/disapproval.
  - Approval sends packet on for further processing. Disapproval could cause packet to be ignored, trigger a TCP reset, or other appropriate results.

Firewalls

- Host Protection: Packet Accept & Reject (con't)
  - Contact your VMS vendor for more details on how to use the policy module.
    - Some vendors have this feature (not all do).
  - Advantage is that the policy is independent of application design.
    - Your database vendor doesn't have to write network security hooks for you.

Survival on the Internet

Firewalls

- Network Protection: Simple Routing Firewall
  - Good when you have two categories of machines on your local network.
    - Those you want on the Internet, and those you don't.
  - Most Internet connections consist of a set of routers connected to your local network. A default route (or routing update) tells machines on your network how to get to the Internet.

Firewalls

- Network Protection: Simple Routing Firewall (con't)
  - No default route (or dynamic routing daemon) on hosts that you don't want to be touched by the Internet. Since almost all applications require that packets flow in both directions, the "no default route" machines will be unable to reply to connection requests from the Internet.
  - Note: Just flushing the routing table here may not be enough. Make sure that any routers your machine talks to do not IP forward. Make sure that any dynamic routing software (routed, gated) won't put the route back in when you aren't looking.

Survival on the Internet

Firewalls

- Network Protection: Router Hardware Packet Filtering
  - Router used to filter packets passing through it.
  - Available on several commercially available routers now.
  - Decisions can be made on source/destination addressing and application/port numbers.

Firewalls

- Network Protection: screend
  - UNIX host used as Filtering Router
  - Modifications to UNIX networking kernel force packets that are crossing the router ("forwarded") to be fed to a user-mode program "screend" (screening daemon) first. This process decides whether the packet should be forwarded or not.
  - Highly programmable.
  - Available "free" from DEC. Anonymous FTP to GATEKEEPER.DEC.COM look in directory /pub/DEC/screend.
    - "free" actually means "free with some strings attached." Check the README files for details.

Survival on the Internet

Firewalls

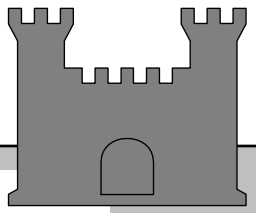
- Network Protection: Kernel hooks to ip_forwarding routines
  - VMS host used as filtering router. Somewhat like "screend" in concept, but all work done in the networking kernel.
  - Policy module loaded into VMS kernel space at system boot.
  - Headers for every packet to be forwarded are sent to the policy module for approval/disapproval.

Firewalls

- Network Protection: Kernel hooks to ip_forwarding routines (con't)
  - Approval sends packet on for further processing. Disapproval could cause packet to be ignored, trigger a TCP reset, or other appropriate results.
  - Contact your vendor for more details on how to use the policy module.
    - Some vendors have this feature (not all do).

Firewalls

- Network Protection: Application Level Gateway
  - Set up a machine that is a "gatehouse" between your network and the outside world.
    - Smart Mailer for gatewaying between internal/external network
    - User has to pass through this system to get into/out of internal network. Can be guarded by password systems.
    - AT&T uses a challenge/response system based on DES-based smart cards.
    - Application level gateways for allowing connections from internal network to externals services like FTP and TELNET.
    - Gatehouse is used to facilitate connections only.
  - This can be fairly complicated to set up!
  - Bill Cheswick talks about this in the "Berferd" talk.



Survival on the Internet

Ongoing security initiatives

- Organizations
  - CERT - Computer Emergency Response Team
    - "Who you gonna call when something bad is happening ?"
    - Based at the Software Engineering Institute, CMU.
    - Funded by USDoD/DARPA.
    - Founded in December 1988 (After the Morris worm).
    - Central clearing house for security incidents, information, expertise.
    - E-Mail: cert@cert.sei.cmu.edu
  - Note: The CERT is switching to domain CERT.ORG sometime soon.
    - Phone: 412-268-7090
    - Has issued 50+ advisories covering operating system problems and security incidents.

Survival on the Internet

Ongoing security initiatives

- Organizations
  - FIRST - Forum of Incident Response and Security Teams
    - All the different CERT-like organizations lumped together.
  - DoE, NASA, Major Corporations
    - Some initiatives to get vendors involved in this group as well.
    - Inter-organization communication.
  - IETF - Internet Engineering Task Force
    - SSPHWG - Site Security Policy Handbook Working Group
  - SSPHWG Working Group archives are stored (Anonymous FTP) at cert.sei.cmu.edu in /pub/ssphug.
    - Privacy Enhanced Mail Group
  - PEM developers list subscriptions send to PEM-DEV-REQUEST@TIS.COM.

Survival on the Internet

Ongoing security initiatives

- Informational
  - VIRUS-L/comp.virus
    - Public discussion about computer viruses and related security matters. Primarily addresses the PC and Macintosh platforms, but occasionally discusses larger machines.
    - Available via USENET News as ’comp.virus’.
    - E-Mail: Send e-mail to LISTSERV@IBM1.CC.LEHIGH.EDU (or LISTSERV@LEHIIBM1 for you Bitnetters) stating: "SUB VIRUS-L your-name".
    - Archives: Anonymous FTP at cert.sei.cmu.edu in /pub/virus-l.

Survival on the Internet

Ongoing security initiatives

- Informational
  - VALERT-L
    - Virus alert messages only
  - e.g. "Hey I found another one! Here is what it looks like."
    - E-Mail: Send e-mail to LISTSERV@IBM1.CC.LEHIGH.EDU (or LISTSERV@LEHIIBM1 for you Bitnetters) stating: "SUB VALERT-L your-name".

Survival on the Internet

Ongoing security initiatives

- Informational
  - CERT-TOOLS
    - Restricted security tool design mailing list.
    - E-Mail: CERT-TOOLS-REQUEST@CERT.SEI.CMU.EDU
  - CERT-ADVISORY/comp.security.announce
    - CERT advisories "hot off the press"
    - E-Mail: CERT-ADVISORY-REQUEST@CERT.SEI.CMU.EDU
    - Usenet: Subscribe to comp.security.announce

Survival on the Internet

Ongoing security initiatives

- Informational
  - DDN Management Bulletin
  - DDN Security Bulletin
    - DDN management and security advisories.
    - E-Mail: nic@nic.ddn.mil
    - Usenet: ddn.mgt-bulletin

Ongoing security initiatives

- Informational
  - Operating system specific groups, application specific groups, protocol specific groups
    - There may be specialized groups covering your type of environment. Always good to keep an ear to the ground there as well. Examples include:
  - comp.os.vms
  - comp.unix.ultrix
  - comp.protocols.tcp-ip
  - vmsnet.networks.tcp-ip.multinet, vmsnet.networks.tcp-ip.cmu-tek, vmsnet.networks.tcp-ip.wintcp
  - vmsnet.networks.tcp-ip.ucx (coming soon ?)
    - Some by E-mail or USENET only. Some are gatewayed between the two.

Survival on the Internet

Ongoing security initiatives

- Archives
  - Anonymous FTP archive at cert.sei.cmu.edu:
    - CERT Advisories
    - NIST FIPS Reports
    - Tools
  - COPS UNIX Security Package
  - VIRUS_SCAN (MS-DOS virus detection programs)
    - Documentation
    - VIRUS-L material
    - SSPHWG material

Survival on the Internet

Ongoing security initiatives

- Archives
  - Gatekeeper.Dec.Com
    - screend sources and reports
  - Research.Att.Com
    - Reports
  - Various.Vendor.Foo
    - Vendor patch kits.
    - Talk to your vendor for details.

Survival on the Internet

Questions and Answers

Thank you very much for coming!

Survival on the Internet

References

- "Improving the security of your UNIX system"
  By David A. Curry
  Report ITSTD-721-FR-90-21
  SRI International, Menlo Park, CA
  April 1990
  - Available by Anonymous FTP from CERT.SEI.CMU.EDU, file /pub/info/security-doc.txt

References

- "Simple and Flexible Datagram Access Controls for Unix-based Gateways" (WRL Research Report 89/4)

  By Jeffrey C. Mogul

  Western Research Laboratory

  Digital Equipment Corporation, Palo Alto, CA

  March 1989

  - Available by Anonymous FTP from GATEKEEPER.DEC.COM it is part of the 'screend' software package file /pub/DEC/screend/screend.tar.Z

Survival on the Internet

References

- "An Evening with Berferd... In Which a Cracker is Lured, Endured, and Studied"
  By Bill Cheswick
  AT&T Bell Laboratories, Murray Hill, NJ
  - Available by Anonymous FTP from RESEARCH.ATT.COM
    file /dist/berferd.ps

Survival on the Internet

References

- "The Design of a Secure Internet Gateway"
  By Bill Cheswick
  AT&T Bell Laboratories, Murray Hill, NJ
  - Available by Anonymous FTP from RESEARCH.ATT.COM
    file /dist/Secure_Internet_Gateway.ps

Survival on the Internet

References

- "The Cuckoo's Egg: Tracking a spy through the maze of computer espionage"

  By Cliff Stoll

  Doubleday 1989 - ISBN 0-385-24946-2

- "Cyberpunk: Outlaws and hackers on the computer frontier"

  By Katie Hafner and John Markoff

  Simon & Schuster 1991 - ISBN 0-671-68322-5

Reviewers

- The author thanks the following individuals for reviewing the content of this session prior to publication:
  - Ken Adelman, George Hoffer, Dave Kashtan, Patrick Mahan
    - TGV, Incorporated (TGV.COM)
  - Karl Auerbach
    - Empirical Tools & Technology (EMPIRICAL.COM)
  - Denise Cartwright
    - Yoyodyne Software Systems (YOYODYNE.COM)
  - Lisa Corsetti
    - Lawrence Livermore National Lab (LLNL.GOV)
  - Ray Kaplan
    - University of Arizona (ARIZONA.EDU)
  - and my bird PerryWidget who edited (and devoured) part of the original hardcopy.