40 Years of Internet Security: Are we There Yet?

Bill Cheswick
AT&T Research
ches@research.att.com
The first characters were sent in 1969

- The third character hung the server
- We’ve been dealing with the problem ever since
- Speaking of measurement: .67 reliability?
Bad Stuff on the Internet

- 1988: Morris worm
- Late 1980s: first PC viruses
- 1996: SYN attacks at Panix and elsewhere
- Late 1990s: DDoS
- Now: the pros are involved, big time
Security Properties of the Early Internet

- It works! Who cares?
- We still run many of those protocols
The Early Internet: the end-to-end principle

- Everyone can talk to everyone else
- The middle of the network is, and must be, dumb
- Any two computers can define and use a new protocol, without further permission
- This was the rule until 1987
1987: Packet filtering

- *Mogul, Rashid, Accetta*. SOSP Nov. 1987
- Found in routers
- Easy to implement
- Efficient, mostly
- Can implement a variety of security policies
- *Mogul*: screend
1987: Application level gateways

- Dave Presotto at Bell Labs rewrote mailer because he didn’t trust sendmail
- This is the firewall I inherited.
- DEC Gatekeeper and DEC SEAL
  - Ranum, Avolio, Reid, Vixie
“Design of a Secure Internet Gateway”

- 1990 Summer Usenix paper
- Belt-and-suspenders gateway design
- Described Presotto’s work, and my additions
- Coined the term *proxy*. 
Original firewall
My (Safer!) Firewall
Referee’s suggestion
A simile for the ages?

- “All of [the gateway’s] protection has, by design, left the internal AT&T machines untested---a sort of crunchy shell around a soft, chewy center.”
Behind firewalls

• Standard servers are too dangerous to expose to outside access
• TCP/IP packets are too dangerous
• No IP connectivity to outside
Advantages

• Expertise focused at the gateway
• Security is cheaper
• Stopped the Morris worm, and many many other evil probes
• Isolated address space doesn’t leak information, maybe easier to manage
Firewalls book (1994)

- The timing was perfect
- The world adopted many of our suggestions
At this point (1994)

- The web was just spreading in a big way
- No real crypto available
- All networked hosts run Unix
- Attacks are against servers
- Servers and protocols are of “it works!” quality
Disadvantages of perimeter defenses

• Lose much of the innovation potential of the end-to-end principle
• Hard to keep up with new desired services
• Mechanism for outgoing TCP connections very helpful
  • reflected in modern NAT security
Chewy Center is a problem

- Host weakness “OK” if firewall is present, but isn’t really
- By 1996, AT&T/Lucent had 130,000 hosts “inside” the perimeter
The Internet

Lucent - 130,000, 266K IP addresses, 3000 nets ann.

thousands of telecommuters

~200 business partners

SLIP
PPP
ISDN
X.25
cable
...

Holmdel
Allentown
Columbus
Murray Hill
Murray Hill
Internet Skinny Dipping
Research question

• Can one use the Internet in a rich way, safely, without perimeter defenses?

• If so, what does it take?
Threat Model

• Attacks from without: evil software actively probing our software
• Invited attacks: clicking on the wrong thing
• Eavesdropping in the endpoints or in transit data
Security elements

- Secure servers, highly resistant to crafted attacks
- Secure communication, resistant to man-in-the-middle attacks and eavesdropping
- Clients strong enough to protect their users’ secrets and software integrity
- The bozo in the chair
Measuring Computer Security
When you can measure what you are speaking about, and express it in numbers, you know something about it. But when you cannot measure it, when you cannot express it in numbers, your knowledge is of a meager and unsatisfactory kind: it may be the beginning of knowledge, but you have scarcely... advanced to the state of science.

- Lord Kelvin
Many want to measure computer security

- change one bit of Vista?
- There always seems to be a human judge at one step
Measuring Computer Security

```
netstat -an | wc -l
```
## Active Connections - Win ME

<table>
<thead>
<tr>
<th>Proto</th>
<th>Local Address</th>
<th>Foreign Address</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>127.0.0.1:1032</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>TCP</td>
<td>223.223.223.10:139</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>UDP</td>
<td>0.0.0.0:1025</td>
<td><em>:</em></td>
<td></td>
</tr>
<tr>
<td>UDP</td>
<td>0.0.0.0:1026</td>
<td><em>:</em></td>
<td></td>
</tr>
<tr>
<td>UDP</td>
<td>0.0.0.0:31337</td>
<td><em>:</em></td>
<td></td>
</tr>
<tr>
<td>UDP</td>
<td>0.0.0.0:162</td>
<td><em>:</em></td>
<td></td>
</tr>
<tr>
<td>UDP</td>
<td>223.223.223.10:137</td>
<td><em>:</em></td>
<td></td>
</tr>
<tr>
<td>UDP</td>
<td>223.223.223.10:138</td>
<td><em>:</em></td>
<td></td>
</tr>
<tr>
<td>Proto</td>
<td>Local Address</td>
<td>Foreign Address</td>
<td>State</td>
</tr>
<tr>
<td>-------</td>
<td>---------------</td>
<td>-----------------</td>
<td>-----------</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:135</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:445</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:1029</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:1036</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:1078</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:1080</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:1086</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:6515</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>TCP</td>
<td>127.0.0.1:139</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>UDP</td>
<td>0.0.0.0:445</td>
<td><em>:</em></td>
<td></td>
</tr>
<tr>
<td>UDP</td>
<td>0.0.0.0:1038</td>
<td><em>:</em></td>
<td></td>
</tr>
<tr>
<td>UDP</td>
<td>0.0.0.0:6514</td>
<td><em>:</em></td>
<td></td>
</tr>
<tr>
<td>UDP</td>
<td>0.0.0.0:6515</td>
<td><em>:</em></td>
<td></td>
</tr>
<tr>
<td>UDP</td>
<td>127.0.0.1:1108</td>
<td><em>:</em></td>
<td></td>
</tr>
<tr>
<td>UDP</td>
<td>223.223.223.96:500</td>
<td><em>:</em></td>
<td></td>
</tr>
<tr>
<td>UDP</td>
<td>223.223.223.96:4500</td>
<td><em>:</em></td>
<td></td>
</tr>
</tbody>
</table>
### Win XP pre-SP2

<table>
<thead>
<tr>
<th>Proto</th>
<th>Local Address</th>
<th>Foreign Address</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>ches-pc:epmap</td>
<td>ches-pc:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>TCP</td>
<td>ches-pc:microsoft-ds</td>
<td>ches-pc:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>TCP</td>
<td>ches-pc:1025</td>
<td>ches-pc:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>TCP</td>
<td>ches-pc:1036</td>
<td>ches-pc:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>TCP</td>
<td>ches-pc:3115</td>
<td>ches-pc:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>TCP</td>
<td>ches-pc:3118</td>
<td>ches-pc:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>TCP</td>
<td>ches-pc:3470</td>
<td>ches-pc:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>TCP</td>
<td>ches-pc:3477</td>
<td>ches-pc:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>TCP</td>
<td>ches-pc:5000</td>
<td>ches-pc:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>TCP</td>
<td>ches-pc:6515</td>
<td>ches-pc:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>TCP</td>
<td>ches-pc:netbios-ssn</td>
<td>ches-pc:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>TCP</td>
<td>ches-pc:3001</td>
<td>ches-pc:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>TCP</td>
<td>ches-pc:3002</td>
<td>ches-pc:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>TCP</td>
<td>ches-pc:3003</td>
<td>ches-pc:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>TCP</td>
<td>ches-pc:5180</td>
<td>ches-pc:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>UDP</td>
<td>ches-pc:microsoft-ds</td>
<td><em>:</em></td>
<td></td>
</tr>
<tr>
<td>UDP</td>
<td>ches-pc:isakmp</td>
<td><em>:</em></td>
<td></td>
</tr>
<tr>
<td>UDP</td>
<td>ches-pc:1027</td>
<td><em>:</em></td>
<td></td>
</tr>
<tr>
<td>UDP</td>
<td>ches-pc:3008</td>
<td><em>:</em></td>
<td></td>
</tr>
<tr>
<td>UDP</td>
<td>ches-pc:3473</td>
<td><em>:</em></td>
<td></td>
</tr>
<tr>
<td>UDP</td>
<td>ches-pc:6514</td>
<td><em>:</em></td>
<td></td>
</tr>
<tr>
<td>UDP</td>
<td>ches-pc:6515</td>
<td><em>:</em></td>
<td></td>
</tr>
<tr>
<td>UDP</td>
<td>ches-pc:netbios-ns</td>
<td><em>:</em></td>
<td></td>
</tr>
<tr>
<td>UDP</td>
<td>ches-pc:netbios-dgm</td>
<td><em>:</em></td>
<td></td>
</tr>
<tr>
<td>UDP</td>
<td>ches-pc:1900</td>
<td><em>:</em></td>
<td></td>
</tr>
<tr>
<td>UDP</td>
<td>ches-pc:ntp</td>
<td><em>:</em></td>
<td></td>
</tr>
<tr>
<td>UDP</td>
<td>ches-pc:1900</td>
<td><em>:</em></td>
<td></td>
</tr>
<tr>
<td>UDP</td>
<td>ches-pc:3471</td>
<td><em>:</em></td>
<td></td>
</tr>
</tbody>
</table>
Guiding security principle for servers

• “You’ve got to get out of the game.” - Fred Grampp

• “Best block is not be there.” - Mr. Miyagi, Karate Kid 2
My FreeBSD machine

Active Internet connections (including servers)
Proto Recv-Q Send-Q Local Address
tcp4 0 0 *.22
tcp6 0 0 *.22
Microsoft wasn’t the first
<table>
<thead>
<tr>
<th>Service</th>
<th>Type</th>
<th>Protocol</th>
<th>Options</th>
<th>User</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>ftp</td>
<td>stream</td>
<td>tcp</td>
<td>nowait</td>
<td>root</td>
<td>/v/gate/ftpd</td>
</tr>
<tr>
<td>telnet</td>
<td>stream</td>
<td>tcp</td>
<td>nowait</td>
<td>root</td>
<td>/usr/etc/telnetd</td>
</tr>
<tr>
<td>shell</td>
<td>stream</td>
<td>tcp</td>
<td>nowait</td>
<td>root</td>
<td>/usr/etc/rshd</td>
</tr>
<tr>
<td>login</td>
<td>stream</td>
<td>tcp</td>
<td>nowait</td>
<td>root</td>
<td>/usr/etc/rlogind</td>
</tr>
<tr>
<td>exec</td>
<td>stream</td>
<td>tcp</td>
<td>nowait</td>
<td>root</td>
<td>/usr/etc/rexecd</td>
</tr>
<tr>
<td>finger</td>
<td>stream</td>
<td>tcp</td>
<td>nowait</td>
<td>guest</td>
<td>/usr/etc/fingerd</td>
</tr>
<tr>
<td>bootp</td>
<td>dgram</td>
<td>udp</td>
<td>wait</td>
<td>root</td>
<td>/usr/etc/bootp</td>
</tr>
<tr>
<td>tftp</td>
<td>dgram</td>
<td>udp</td>
<td>wait</td>
<td>guest</td>
<td>/usr/etc/tftpd</td>
</tr>
<tr>
<td>ntalk</td>
<td>dgram</td>
<td>udp</td>
<td>wait</td>
<td>root</td>
<td>/usr/etc/talkd</td>
</tr>
<tr>
<td>tcpmux</td>
<td>stream</td>
<td>tcp</td>
<td>nowait</td>
<td>root</td>
<td>internal</td>
</tr>
<tr>
<td>echo</td>
<td>stream</td>
<td>tcp</td>
<td>nowait</td>
<td>root</td>
<td>internal</td>
</tr>
<tr>
<td>discard</td>
<td>stream</td>
<td>tcp</td>
<td>nowait</td>
<td>root</td>
<td>internal</td>
</tr>
<tr>
<td>chargen</td>
<td>stream</td>
<td>tcp</td>
<td>nowait</td>
<td>root</td>
<td>internal</td>
</tr>
<tr>
<td>daytime</td>
<td>stream</td>
<td>tcp</td>
<td>nowait</td>
<td>root</td>
<td>internal</td>
</tr>
<tr>
<td>time</td>
<td>stream</td>
<td>tcp</td>
<td>nowait</td>
<td>root</td>
<td>internal</td>
</tr>
<tr>
<td>echo</td>
<td>dgram</td>
<td>udp</td>
<td>wait</td>
<td>root</td>
<td>internal</td>
</tr>
<tr>
<td>discard</td>
<td>dgram</td>
<td>udp</td>
<td>wait</td>
<td>root</td>
<td>internal</td>
</tr>
<tr>
<td>chargen</td>
<td>dgram</td>
<td>udp</td>
<td>wait</td>
<td>root</td>
<td>internal</td>
</tr>
<tr>
<td>daytime</td>
<td>dgram</td>
<td>udp</td>
<td>wait</td>
<td>root</td>
<td>internal</td>
</tr>
<tr>
<td>time</td>
<td>dgram</td>
<td>udp</td>
<td>wait</td>
<td>root</td>
<td>internal</td>
</tr>
<tr>
<td>sgi-dgl</td>
<td>stream</td>
<td>tcp</td>
<td>nowait</td>
<td>root</td>
<td>/rcv dgld</td>
</tr>
<tr>
<td>uucp</td>
<td>stream</td>
<td>tcp</td>
<td>nowait</td>
<td>root</td>
<td>/usr/lib/uucp/uucpd</td>
</tr>
</tbody>
</table>
mountd/1  stream   rpc/tcp wait/lc  root  rpc.mountd
mountd/1  dgram   rpc/udp wait/lc root  rpc.mountd
sgi_mountd/1  stream  rpc/tcp wait/lc root  rpc.mountd
sgi_mountd/1  dgram  rpc/udp wait/lc root  rpc.mountd
rstatd/1-3  dgram  rpc/udp wait   root  rpc.rstatd
walld/1     dgram  rpc/udp wait   root  rpc.rwalld
rusersd/1   dgram  rpc/udp wait   root  rpc.rusersd
rquotad/1   dgram  rpc/udp wait   root  rpc.rquotad
sprayd/1    dgram  rpc/udp wait   root  rpc.sprayd
bootparam/1 dgram  rpc/udp wait   root  rpc.bootparamd
sgi_videod/1 stream  rpc/tcp wait root  ?videod
sgi_fam/1    stream  rpc/tcp wait root  ?fam
sgi_snoopd/1 stream  rpc/tcp wait root  ?rpc.snoopd
sgi_pcsd/1   dgram  rpc/udp wait   root  ?cvpcsd
sgi_pod/1    stream  rpc/tcp wait root  ?podd
tcpmux/sgi_scanner stream tcp nowait root  ?scan/net/scannerd
tcpmux/sgi_printer stream tcp nowait root  ?print/printerd
9fs          stream  tcp     nowait     root  /v/bin/u9fs u9fs
webproxy    stream  tcp     nowait     root  /usr/local/etc/webserv
And they are still making mistakes

• *Finding User/Kernel Pointer Bugs with Type Inference*. Rob Johnson, David Wagner, Usenix Security 2004

• Unchecked user-space pointers in systems calls on Linux

• New bugs appearing in secure OSes
Secure Servers
We can do pretty well with servers

• If we try. Ask Amazon, Fedex, etc., etc.
• We have experts designing and running these machines
• Server software can be quite robust
  • sshd, postfix, apache (maybe)
• Systems don’t default to safe servers
Secure Communications

• The crypto export wars of the 90s are over

• In June 2003, NSA said that a properly implemented and vetted version of AES is suitable for Type 1 cryptography

• SSL is holding up well

• So is ssh
Secure Clients: Windows

- Has had server problems (see above) and poor or no software containment
- Microsoft’s security press is real, and Vista is going to be an improvement
- This is going to take time: an Augean stable
Vista: good signs

• It took longer than they expected to get it out

• Not a mythical man month problem, they had to dig deeper

• A lot of applications need modifications to run (that first trip to the dentist is painful)

<table>
<thead>
<tr>
<th></th>
<th>Windows Vista</th>
<th>Windows XP SP2</th>
<th>RHEL 4</th>
<th>OpenBSD 3.x</th>
<th>Mac OS X</th>
</tr>
</thead>
<tbody>
<tr>
<td>images</td>
<td>Section Reordering</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>EXE Randomization</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>DLL Randomization</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>stack</td>
<td>Frame Protection</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Exception Protection</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Local Variable Protection</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Randomization</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Non-Executable</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>heap</td>
<td>Metadata Protection</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Randomization</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Non-Executable</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

[full support] [partial support]
Vista: bad signs

- blacklisting, not white-listing, of attachments
- DRM requirements force software breakage (see Peter Guttman’s work)
- I haven’t heard of useful sandboxing yet
Secure clients: *nix

• “Unix is an administrative nightmare” - Dennis Ritchie

• Runs firefox, thunderbird, and other giant client programs, without containment
Macintosh clients

• Have been below the radar, making it an uneconomical target

• I expect Apple to double or quadruple their current market share. Still tiny.

• Basic OS is probably a better platform

• Open source software versions lagging
“Owned” computer

- Invader has unlimited access to the software on the owned machine

- In some cases, it may be possible to damage the hardware
Who does this?

- Criminal organizations (RBN?)
- Terrorists
- Consultants
- Spies, spooks, and the military
Botnets: hoards of “owned” computers

• Machines usually subjugated by automated means

• Typical botnet might have 10,000 members. Tendency towards smaller networks

• Owners of “owned” computers want to keep others out

• No incentive to kill the local computer
Phatbot

bot.command runs a command with system()
bot.unsecure enable shares / enable dcom
bot.secure delete shares / disable dcom
bot.flushdns flushes the bots dns cache
bot.quit quits the bot
bot.longuptime If uptime > 7 days then bot will respond
bot.sysinfo displays the system info
bot.status gives status
bot.rndnick makes the bot generate a new random nick
bot.removeallbut removes the bot if id does not match
bot.remove removes the bot
bot.open opens a file (whatever)
bot.nick changes the nickname of the bot
bot.id displays the id of the current code
bot.execute makes the bot execute a .exe
bot.dns resolves ip/hostname by dns
bot.die terminates the bot

bot.about displays the info the author wants you to see
shell.disable Disable shell handler
shell.enable Enable shell handler
shell.handler FallBack handler for shell commands.list Lists all available commands
plugin.unload unloads a plugin (not supported yet)
plugin.load loads a plugin
cvar.saveconfig saves config to a file
cvar.loadconfig loads config from a file
inst.svcadd adds a service to scm
inst.asadd adds an autostart entry
logic.ifuptime exec command if uptime is bigger than specified
mac.login logs the user in
mac.logout logs the user out
ftp.update executes a file from a ftp url
ftp.execute updates the bot from a ftp url
ftp.download downloads a file from ftp
Uses for Botnets

• spam relays
• DDoS packet sources (spoofing unnecessary)
• IP laundering stepping stones
• Web servers for phishing
• Keyboard sniffing
Measuring Unix Host Security

• Moving from user privileges to root
• Much too easy, in my judgement
  • Prefer single-user machines
• *Not* the right answer in many research environments
<table>
<thead>
<tr>
<th>Dll Base</th>
<th>Date Stamp</th>
<th>Name</th>
<th>Dll Base</th>
<th>Date Stamp</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>80100000</td>
<td>2be154c9</td>
<td>ntoskrnl.exe</td>
<td>80090000</td>
<td>2be154c9</td>
<td>hal.dll</td>
</tr>
<tr>
<td>80200000</td>
<td>2bd49628</td>
<td>ncrc710.sys</td>
<td>8025c000</td>
<td>2bd49688</td>
<td>SCSIPORT.SYS</td>
</tr>
<tr>
<td>80267000</td>
<td>2bd49683</td>
<td>scsidisk.sys</td>
<td>802a6000</td>
<td>2bd496b9</td>
<td>Fastfat.sys</td>
</tr>
<tr>
<td>fa800000</td>
<td>2bd49666</td>
<td>Floppy.SYS</td>
<td>fa800000</td>
<td>2bd496db</td>
<td>Hpfs_Rec.SYS</td>
</tr>
<tr>
<td>fa820000</td>
<td>2bd49676</td>
<td>Null.SYS</td>
<td>fa830000</td>
<td>2bd4965a</td>
<td>Beep.SYS</td>
</tr>
<tr>
<td>fa840000</td>
<td>2bd49688</td>
<td>i8042p185.SYS</td>
<td>fa850000</td>
<td>2bd5a020</td>
<td>SERMOUSE.SYS</td>
</tr>
<tr>
<td>fa860000</td>
<td>2bd49691</td>
<td>kbdclass.SYS</td>
<td>fa870000</td>
<td>2bd49671</td>
<td>MOUCLASS.SYS</td>
</tr>
<tr>
<td>fa880000</td>
<td>2bd9c0be</td>
<td>Videoprt.SYS</td>
<td>fa890000</td>
<td>2bd4963b</td>
<td>NCR77C22.SYS</td>
</tr>
<tr>
<td>fa0a0000</td>
<td>2bd4a4ce</td>
<td>Vga.SYS</td>
<td>fa0b0000</td>
<td>2bd496d0</td>
<td>Msfs.SYS</td>
</tr>
<tr>
<td>fa8c0000</td>
<td>2bd496c3</td>
<td>Npfs.SYS</td>
<td>fa8e0000</td>
<td>2bd496c9</td>
<td>Ntfs.SYS</td>
</tr>
<tr>
<td>fa940000</td>
<td>2bd496df</td>
<td>NDIS.SYS</td>
<td>fa930000</td>
<td>2bd49707</td>
<td>wdlan.sys</td>
</tr>
<tr>
<td>fa970000</td>
<td>2bd49712</td>
<td>TDI.SYS</td>
<td>fa950000</td>
<td>2bd5a7f3</td>
<td>nbf.sys</td>
</tr>
<tr>
<td>fa980000</td>
<td>2bd724f6</td>
<td>streams.sys</td>
<td>fa9h0000</td>
<td>2bd4975f</td>
<td>unhnh.sys</td>
</tr>
<tr>
<td>fa9c0000</td>
<td>2bd5b0d7</td>
<td>mcsxms.sys</td>
<td>fa9d0000</td>
<td>2bd4971d</td>
<td>netbios.sys</td>
</tr>
<tr>
<td>fa9e0000</td>
<td>2bd49678</td>
<td>Parallel.sys</td>
<td>fa9f0000</td>
<td>2bd4969f</td>
<td>serial.SYS</td>
</tr>
<tr>
<td>faaa0000</td>
<td>2bd49739</td>
<td>mp.sys</td>
<td>faa40000</td>
<td>2bd4971f</td>
<td>SMBTRSUP.SYS</td>
</tr>
<tr>
<td>faa10000</td>
<td>2bd6f2a2</td>
<td>srv.sys</td>
<td>faa50000</td>
<td>2bd4971a</td>
<td>afid.sys</td>
</tr>
<tr>
<td>faa60000</td>
<td>2bd6fd80</td>
<td>rdr.sys</td>
<td>faaa0000</td>
<td>2bd49735</td>
<td>bowser.sys</td>
</tr>
</tbody>
</table>

Address   dword    dump     Build [1381]

---

| fe9cdaec | fa84003c | fa84003c | 00000000 | 00000000 | 80149905
| fe9cdafe | 8025dfe0  | 8025dfe0 | ff8e6b8c | 80129c2c | ff8e6b94
| fe9cdba0 | 8013e53a  | 8013e53a | ff8e6b94 | 00000000 | ff8e6b94
| fe9cd18 | 8010a373  | 8010a373 | ff8e6df4 | ff8e6f60 | ff8e6c58
| fe9cdb38 | 80105683  | 80105683 | ff8e6f60 | ff8e6c3c | 8015ac7e
| fe9cdaa0 | 80104722  | 80104722 | ff8e6df4 | ff8e6f60 | ff8e6c58
| fe9cdaa | 8012034c  | 8012034c | 00000000 | 80088000 | 80106fc0

---

Name

- i8042p185.SYS
- SCSIPORT.SYS
- ntoskrnl.exe
- ntoskrnl.exe
- ntoskrnl.exe
- ntoskrnl.exe
- ntoskrnl.exe
Unix Host Security

```bash
find / -perm -4000 -user root -print | wc -l
```
/bin/rcp
/sbin/ping
/sbin/ping6
/sbin/shutdown
/usr/X11R6/bin/Xwrapper
/usr/X11R6/bin/xterm
/usr/X11R6/bin/Xwrapper-4
/usr/bin/keyinfo
/usr/bin/keyinit
/usr/bin/lock
/usr/bin/crontab
/usr/bin/opieinfo
/usr/bin/opiepasswd
/usr/bin/rlogin
/usr/bin/quota
/usr/bin/rsh
/usr/bin/su
/usr/bin/lpq
/usr/bin/lpr
/usr/bin/lprm
/usr/bin/chpass
/usr/bin/login
/usr/bin/passwd
/usr/bin/at
/usr/bin/ypchsh
/usr/bin/ypchfn
/usr/bin/ypchpass
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/yppasswd
/usr/bin/batch
/usr/bin/atrm
/usr/bin/atq
/usr/local/bin/screen
/usr/local/bin/sudo
/usr/local/bin/lppasswd
/usr/sbin/mrinfo
/usr/sbin/mtrace
/usr/sbin/ppp
/usr/sbin/pppd
/usr/sbin/sliplogin
/usr/sbin/timedc
/usr/sbin/traceroute
/usr/sbin/traceroute6
Remove the ones I never Use

“You should never be vulnerable to a weakness of a feature you do not use” - Microsoft security directive
/sbin/ping
/sbin/ping6
/usr/X11R6/bin/xterm
/usr/X11R6/bin/Xwrapper-4
/usr/bin/crontab
/usr/bin/su
/usr/bin/lpq
/usr/bin/lpr
/usr/bin/lprm
/usr/bin/login
/usr/bin/passwd
/usr/bin/at
/usr/bin/chsh
/usr/bin/atrm
/usr/bin/atq
/usr/local/bin/sudo
/usr/sbin/traceroute
/usr/sbin/traceroute6
Least Privilege
/sbin/ping
/sbin/ping6
/usr/X11R6/bin/xterm
/usr/X11R6/bin/Xwrapper-4
/usr/bin/crontab
/usr/bin/su
/usr/bin/lpq
/usr/bin/lpr
/usr/bin/lprm
/usr/bin/login
/usr/bin/passwd
/usr/bin/at
/usr/bin/chsh
/usr/bin/atrm
/usr/bin/atq
/usr/local/bin/sudo
/usr/sbin/traceroute
/usr/sbin/traceroute6
/usr/X11R6/bin/Xwrapper-4
/usr/bin/su
/usr/bin/passwd
/usr/bin/chsh
/usr/local/bin/sudo
<table>
<thead>
<tr>
<th>OS</th>
<th>&amp;</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIX 4.2</td>
<td>242</td>
<td>&amp; a staggering number</td>
</tr>
<tr>
<td>BSD/OS 3.0</td>
<td>78</td>
<td>&amp; someone's guard machine</td>
</tr>
<tr>
<td>FreeBSD 4.3</td>
<td>42</td>
<td>&amp; 2 appear to be third-party</td>
</tr>
<tr>
<td>FreeBSD 4.3</td>
<td>47</td>
<td>&amp; see text for closer analysis</td>
</tr>
<tr>
<td>FreeBSD 4.5</td>
<td>43</td>
<td>&amp; about half may be special for this host</td>
</tr>
<tr>
<td>HPUX A.09.07</td>
<td>227</td>
<td>&amp; 3 appear to be third-party</td>
</tr>
<tr>
<td>Linux (Mandrake 8.1)</td>
<td>39</td>
<td>&amp; 2 third-party programs</td>
</tr>
<tr>
<td>Linux (Red Hat 2.4.2-2)</td>
<td>39</td>
<td>&amp; 31 &amp; 2 third-party programs</td>
</tr>
<tr>
<td>Linux (Red Hat 2.4.7-10)</td>
<td>39</td>
<td>&amp; 2--4 third-party</td>
</tr>
<tr>
<td>Linux (Red Hat 5.0)</td>
<td>59</td>
<td>&amp; approved distribution for one university</td>
</tr>
<tr>
<td>Linux (Red Hat 6.0)</td>
<td>38</td>
<td>&amp; 34 may be special to this host</td>
</tr>
<tr>
<td>Linux 2.0.36</td>
<td>26</td>
<td>&amp; 2 third-party programs</td>
</tr>
<tr>
<td>Linux 2.2.16-3</td>
<td>47</td>
<td>&amp; 6 third-party programs</td>
</tr>
<tr>
<td>Linux 7.2</td>
<td>42</td>
<td>&amp; 6 third-party programs</td>
</tr>
<tr>
<td>NCR Intel 4.0v3.0</td>
<td>113</td>
<td>&amp; 6 third-party programs</td>
</tr>
<tr>
<td>NetBSD 1.6</td>
<td>35</td>
<td>&amp; 11 third-party programs</td>
</tr>
<tr>
<td>SGI Irix 5.3</td>
<td>83</td>
<td>&amp; 6 third-party programs</td>
</tr>
<tr>
<td>SGI Irix 5.3</td>
<td>102</td>
<td>&amp; 6 third-party programs</td>
</tr>
<tr>
<td>Sinux 5.42c1002</td>
<td>60</td>
<td>&amp; 2 third-party programs</td>
</tr>
<tr>
<td>Sun Solaris 5.4</td>
<td>52</td>
<td>&amp; 6 third-party programs</td>
</tr>
<tr>
<td>Sun Solaris 5.6</td>
<td>74</td>
<td>&amp; 11 third-party programs</td>
</tr>
<tr>
<td>Sun Solaris 5.8</td>
<td>70</td>
<td>&amp; 6 third-party programs</td>
</tr>
<tr>
<td>Sun Solaris 5.8</td>
<td>82</td>
<td>&amp; 6 third-party programs</td>
</tr>
<tr>
<td>Tru64 4.0r878</td>
<td>72</td>
<td>&amp; \</td>
</tr>
</tbody>
</table>
Measuring security

- Safes: withstand 30 minutes of prying
- Nuclear weapons: resistance to misuse
- Computers: withstands $x$ hours of attack by $y$ people of $z$ capability
Bozo in the Chair

- These attacks will continue indefinitely
- Attackers’ ingenuity is endless
Virus Installation

Do You Want Me to Install a Virus Now?

Yes

Yes
Bozo in the Chair

• Unreasonable to expect users to understand security implications of most computer decisions

• Experts can easily lack enough data

• It is poor engineering to expect humans to choose and remember passwords that are resistant to dictionary attacks
Resistance to Secure Clients

- Many clients haven’t demanded secure host
- Naive users have high tolerance for infection
- Lost weekends for techies
Is Secure Software Really That Hard?

- Yes
- People don’t want to pay for it
- Still in the “good enough” stage
  - especially grandma
Secure software

- Security has to be designed in at the beginning, no retrofits
- Attitude of the designer is key
- Small is beautiful
- Converge on a version, and stop changing it
Successes?

• TeX.

• Postfix (Unix mailer)
  • even sendmail, scourge of the past, is getting better

• dockmaster?
Can we Skinny Dip Safely with Windows?

- I ran XP SP2 on my laptop for several years without problems
- Use mostly for slide presentations, not day-to-day
- 20,000 BP employees are skinny dipping with Windows
Skinny Dipping with Windows? No...

- Students
- Teenage gamers
- Grandma
How has skinny dipping worked for me?

• FreeBSD and Linux hosts
• Very few, very hardened network services
• Single-user hosts
• Dangerous services placed in sandboxes
  • Much too hard to do
How has skinny dipping worked for me?

- Quite well, but I give up services
- No undetected break-ins
- Not all my hosts and services are skinny dipped
Windows OK

What Grandma really needs
Windows OK

- Think client implemented with Windows
- It would be fine for maybe half the Windows users
  - students, consumers, many corp. and gov. users
- Reasonable to skinny dip with it
Windows OK

- No network listeners
- Default secure settings
- All security controls in one or two places
- Security settings can be locked after installation
Windows OK

• There should be nothing that you can click on, in email or on the web, that will hurt your software

• No portable programs executed, except special signed ones

• Reduce privileges of all user programs

• Sandbox dangerous programs
Office OK

- No macros in Word or PowerPoint. No executable code in PowerPoint files
- The only macros allowed in Excel perform arithmetic. They cannot create files, etc.
Limitations to host-level security

- Cannot stop DDoS attacks
  - so we are still going to need walled gardens
- Giving up a layer is an important security decision, once the inside is toughened
Can we skinny dip with Windows?

- Many do it now, usually carefully
- BP put more than 10,000 hosts outside their perimeter
- This will get more plausible soon
What about invited threats?

- Thin clients could help
- Virtualization will help
- Some browsers and mail readers are safer than others
Future technologies

• Looking for virtualization of client software, in all operating systems
• Virtualization will help servers, nicely
• Beyond the DMZ: a quasi-walled garden?
End-to-end opportunities?

- P2P is what we call it these days
- I hear Microsoft is developing more of these
Internet Irregulars

• Serbian web pages
• Solar storm
• Israeli/Palestinian
• Bin Laden’s latest, by “Laura Mansfield”
IPv6

- Three years away since 1993
- Some day, we *are* going to run out of addresses
- I see no migration drivers for intranets
Internet Security in a Nutshell

- The third character on the Internet crashed the server (1969)
- The same problems have been repeated repeatedly ever since
- Still, we are getting our work done
The Internet: we Are there yet

• Spectacular technology that scaled better than we have any right to expect.

• Software could be much cheaper to maintain, and much safer

• We ought to win: its our own hardware, dammit!
40 Years of Internet Security: Are we There Yet?

Bill Cheswick
AT&T Research
ches@research.att.com