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

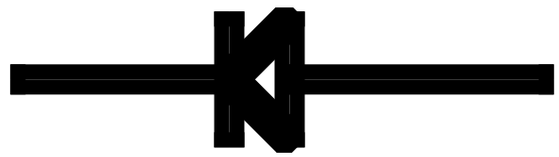
- Dave Presotto at Bell Labs rewrote mailer because he didn't trust *sendmail*

- 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

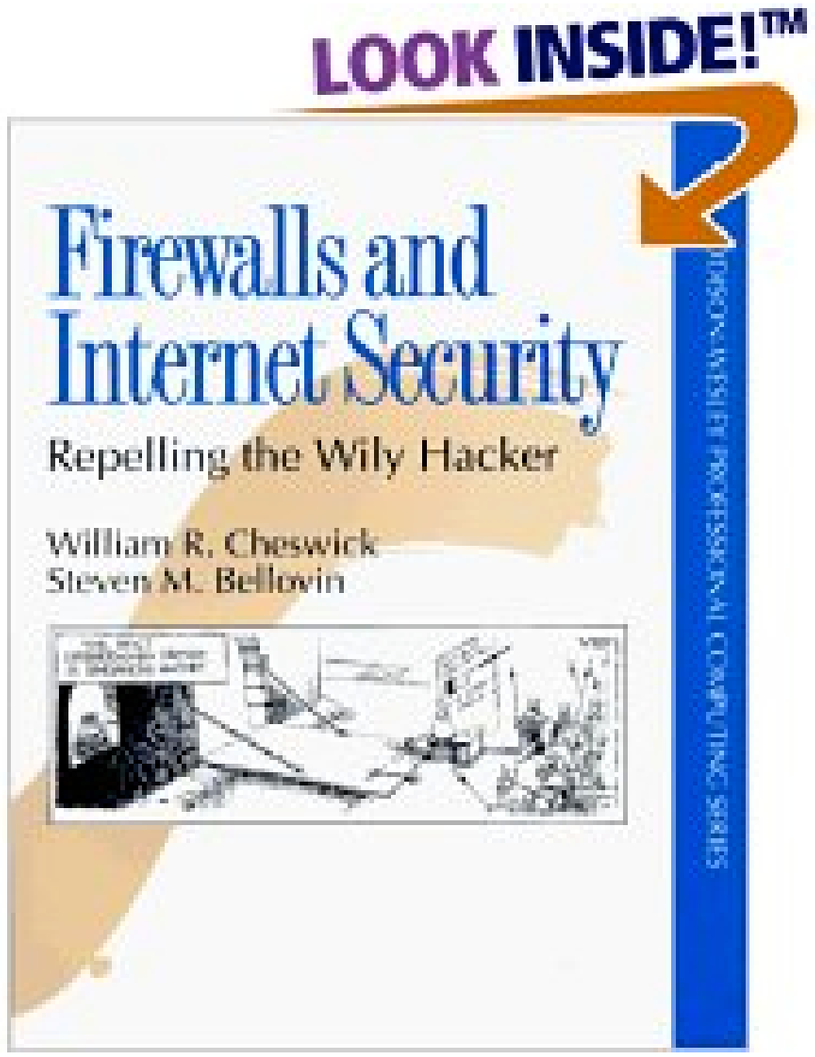
- Standard servers are too dangerous to expose to outside access
- TCP/IP packets are too dangerous
  - No IP connectivity to outside

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

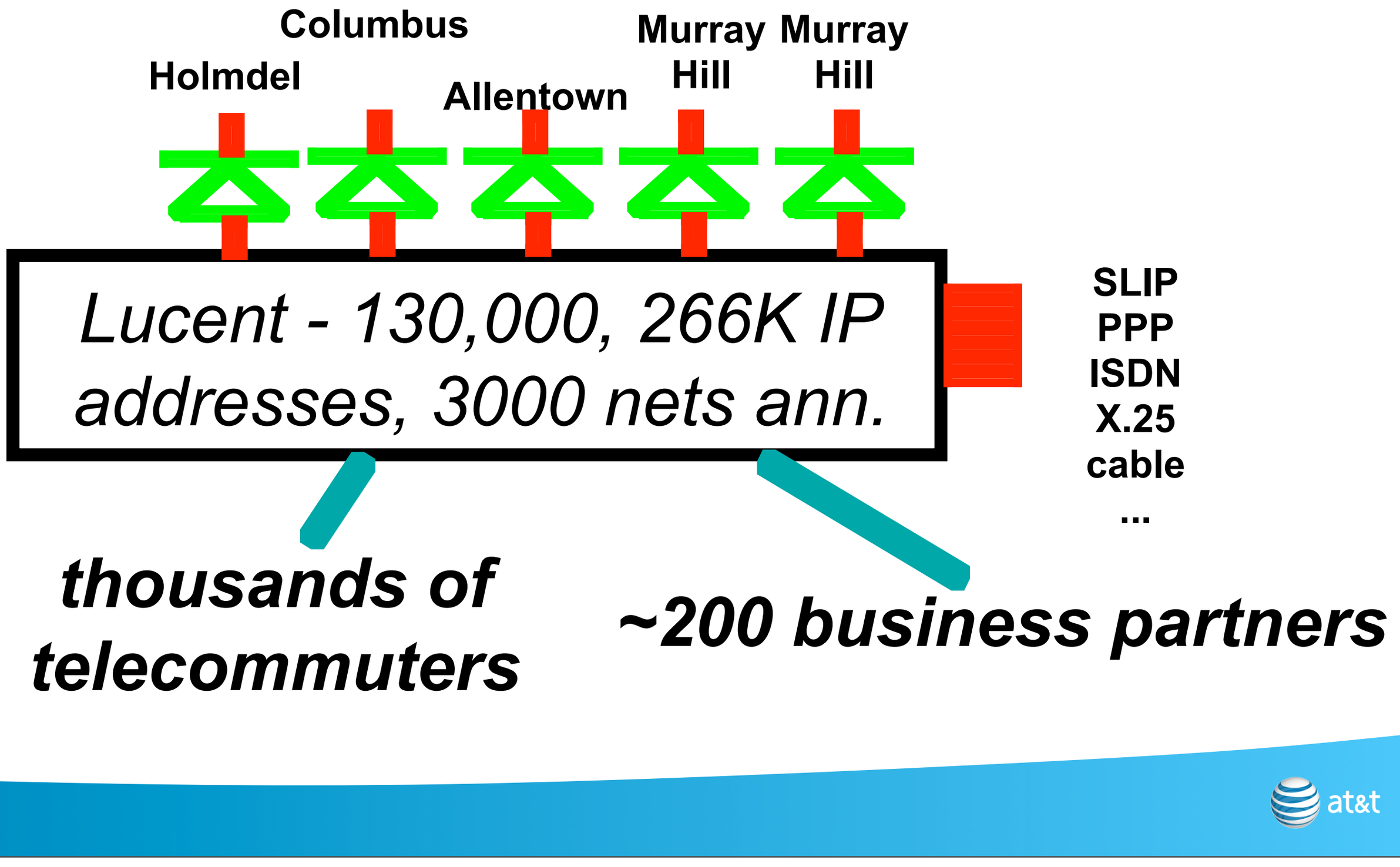
Disadvantages of perimeter defenses

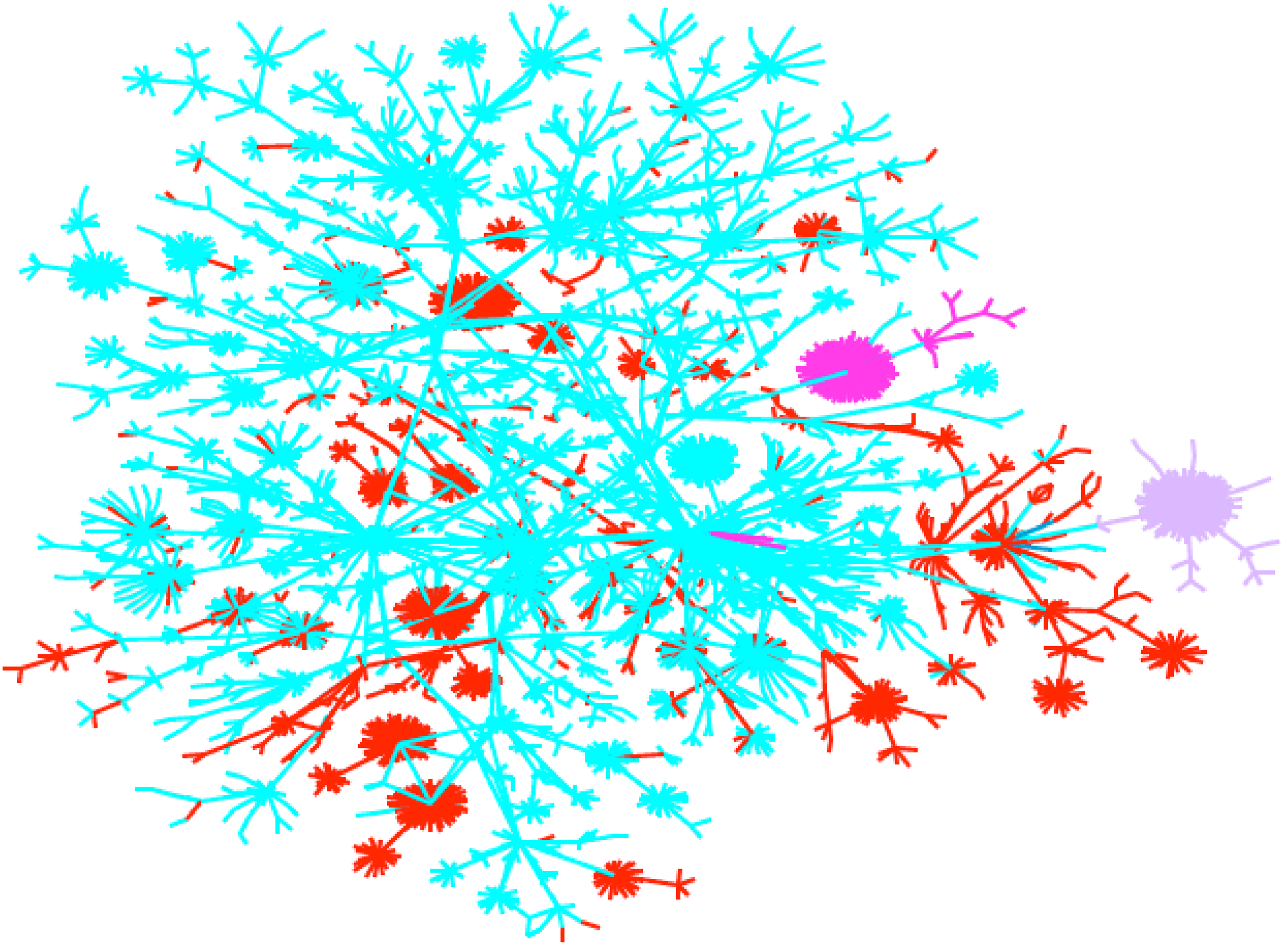
- Lose much of the innovation potential of the end-to-end principle
- Hard to keep up with new desired services
- Mechanism for outgoing TCP connections very helpful
  - reflected in modern NAT security

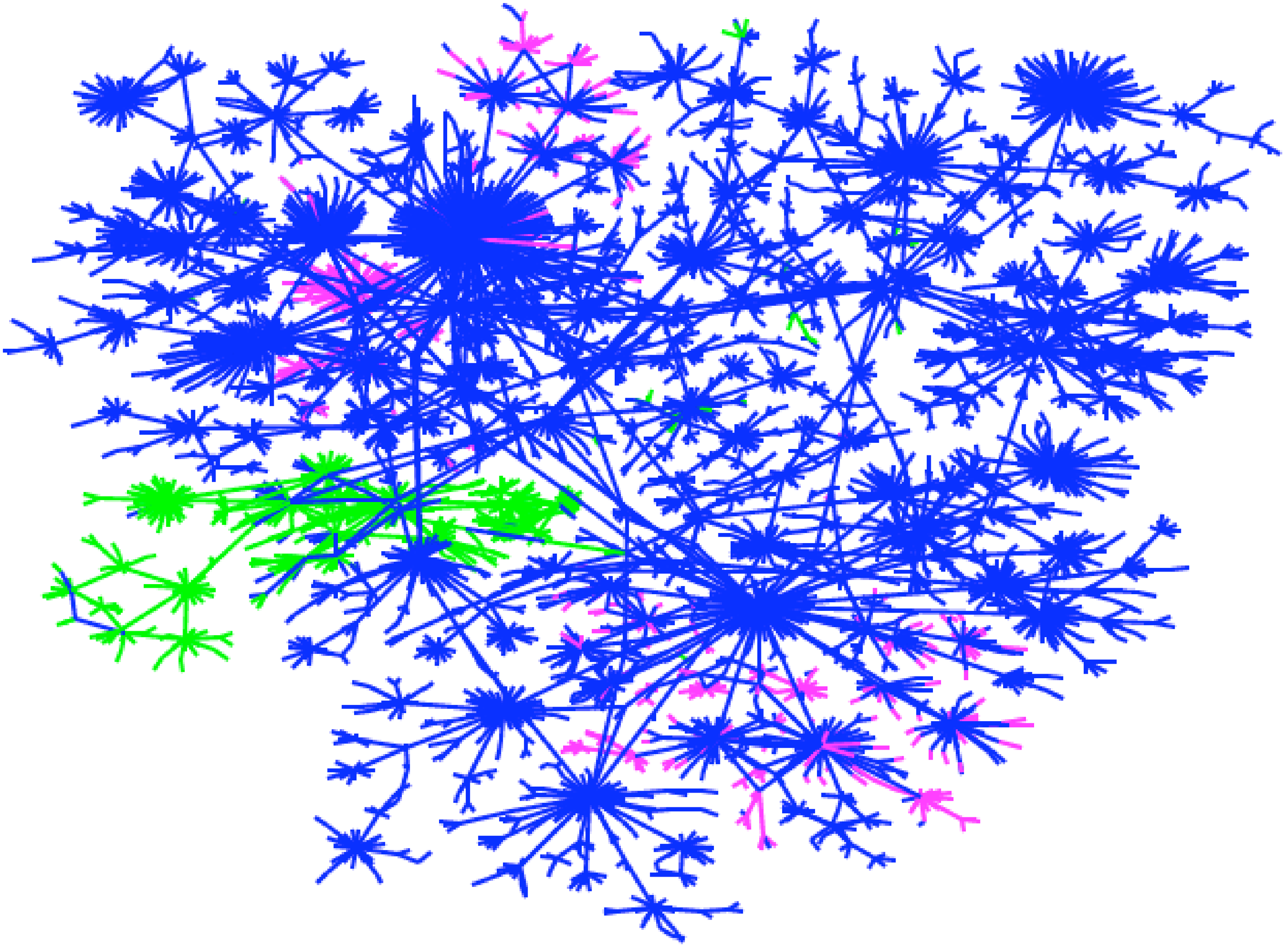
Chewy Center is a problem

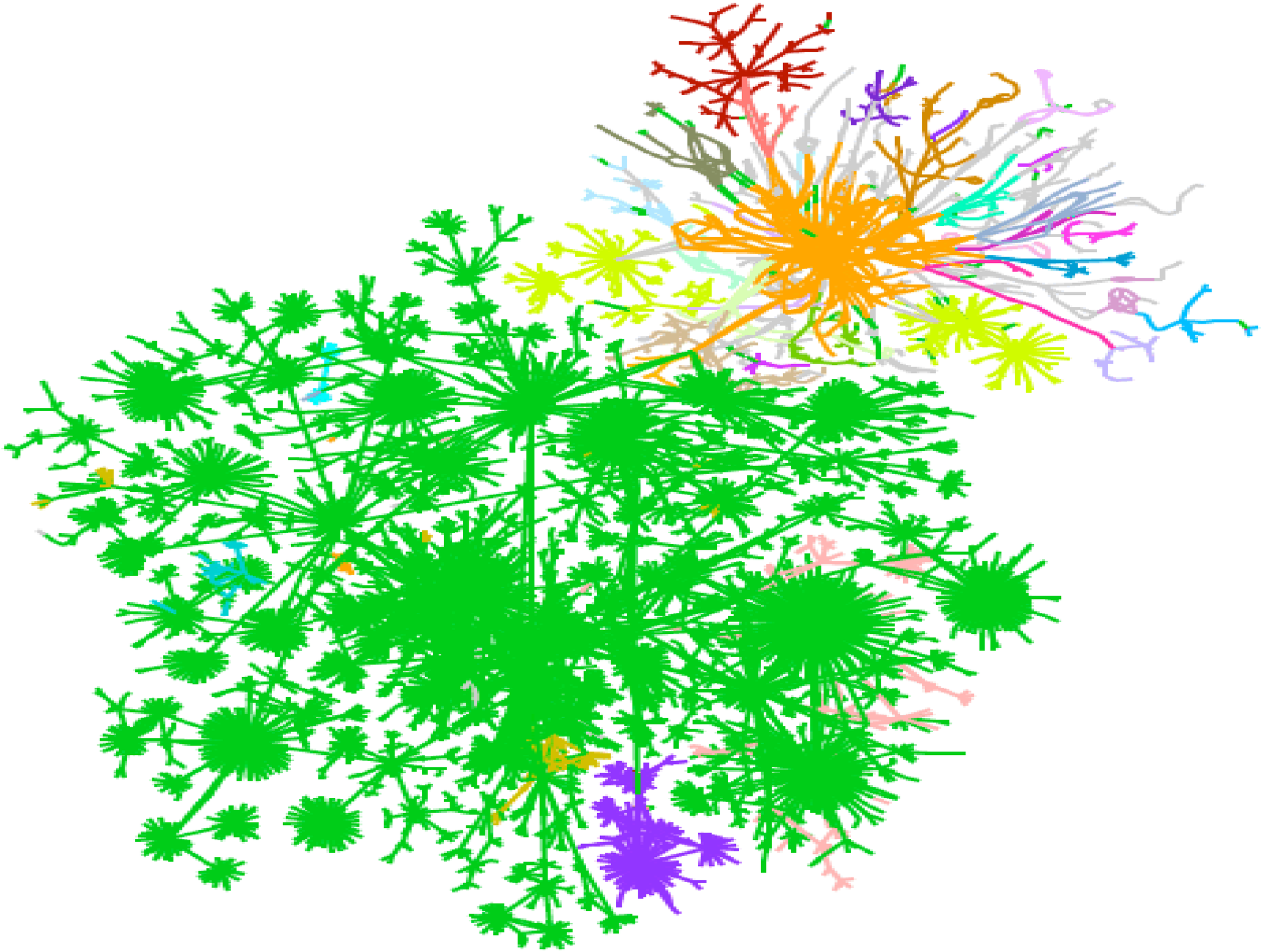
- Host weakness "OK" if firewall is present, but isn't really
- By 1996, AT&T/Lucent had 130,000 hosts "inside" the perimeter

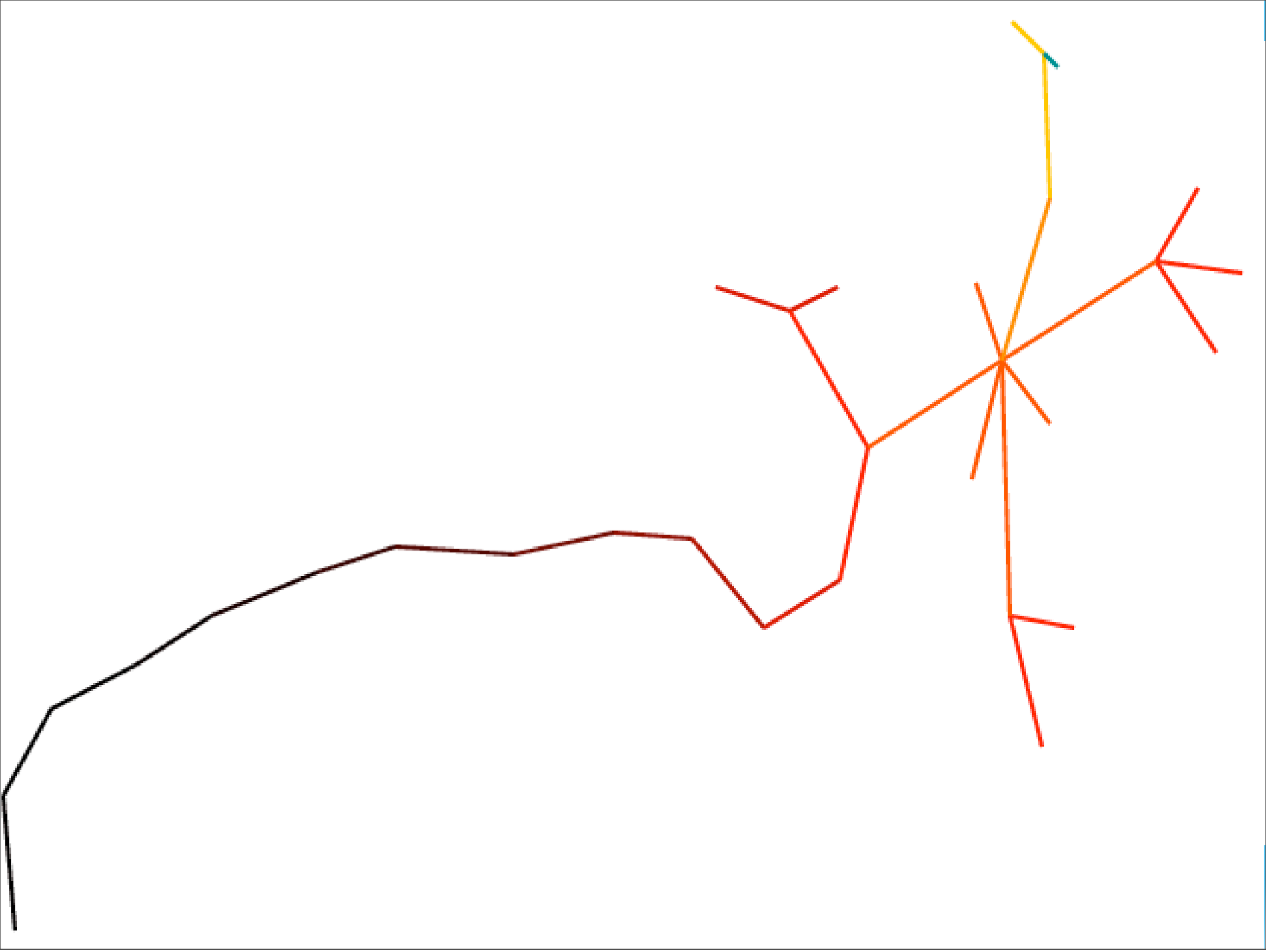
The Internet











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

Win ME

```
Active Connections - Win ME

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:1032         0.0.0.0:0              LISTENING
  TCP    223.223.223.10:139     0.0.0.0:0              LISTENING
  UDP    0.0.0.0:1025           *:*
  UDP    0.0.0.0:1026           *:*
  UDP    0.0.0.0:31337          *:*
  UDP    0.0.0.0:162            *:*
  UDP    223.223.223.10:137     *:*
  UDP    223.223.223.10:138     *:*
```

Win 2K

```
Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1029         0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1036         0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1078         0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1080         0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1086         0.0.0.0:0              LISTENING
  TCP    0.0.0.0:6515         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:139        0.0.0.0:0              LISTENING
  UDP    0.0.0.0:445          *:*
  UDP    0.0.0.0:1038         *:*
  UDP    0.0.0.0:6514         *:*
  UDP    0.0.0.0:6515         *:*
  UDP    127.0.0.1:1108       *:*
  UDP    223.223.223.96:500   *:*
  UDP    223.223.223.96:4500  *:*
```

Win XP pre-SP2

```
Proto  Local Address          Foreign Address        State
 TCP    ches-pc:epmap          ches-pc:0              LISTENING
 TCP    ches-pc:microsoft-ds   ches-pc:0              LISTENING
 TCP    ches-pc:1025           ches-pc:0              LISTENING
 TCP    ches-pc:1036           ches-pc:0              LISTENING
 TCP    ches-pc:3115           ches-pc:0              LISTENING
 TCP    ches-pc:3118           ches-pc:0              LISTENING
 TCP    ches-pc:3470           ches-pc:0              LISTENING
 TCP    ches-pc:3477           ches-pc:0              LISTENING
 TCP    ches-pc:5000           ches-pc:0              LISTENING
 TCP    ches-pc:6515           ches-pc:0              LISTENING
 TCP    ches-pc:netbios-ssn    ches-pc:0              LISTENING
 TCP    ches-pc:3001           ches-pc:0              LISTENING
 TCP    ches-pc:3002           ches-pc:0              LISTENING
 TCP    ches-pc:3003           ches-pc:0              LISTENING
 TCP    ches-pc:5180           ches-pc:0              LISTENING
 UDP    ches-pc:microsoft-ds   *:*
 UDP    ches-pc:isakmp         *:*
 UDP    ches-pc:1027           *:*
 UDP    ches-pc:3008           *:*
 UDP    ches-pc:3473           *:*
 UDP    ches-pc:6514           *:*
 UDP    ches-pc:6515           *:*
 UDP    ches-pc:netbios-ns     *:*
 UDP    ches-pc:netbios-dgm    *:*
 UDP    ches-pc:1900           *:*
 UDP    ches-pc:ntp            *:*
 UDP    ches-pc:1900           *:*
 UDP    ches-pc:3471           *:*
```

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

SGI Irix

```
ftp      stream  tcp     nowait  root    /v/gate/ftpd
telnet   stream  tcp     nowait  root    /usr/etc/telnetd
shell    stream  tcp     nowait  root    /usr/etc/rshd
login    stream  tcp     nowait  root    /usr/etc/rlogind
exec     stream  tcp     nowait  root    /usr/etc/rexecd
finger   stream  tcp     nowait  guest   /usr/etc/fingerd
bootp    dgram   udp     wait    root    /usr/etc/bootp
tftp     dgram   udp     wait    guest   /usr/etc/tftpd
ntalk    dgram   udp     wait    root    /usr/etc/talkd
tcpmux   stream  tcp     nowait  root    internal
echo     stream  tcp     nowait  root    internal
discard  stream  tcp     nowait  root    internal
chargen  stream  tcp     nowait  root    internal
daytime  stream  tcp     nowait  root    internal
time     stream  tcp     nowait  root    internal
echo     dgram   udp     wait    root    internal
discard  dgram   udp     wait    root    internal
chargen  dgram   udp     wait    root    internal
daytime  dgram   udp     wait    root    internal
time     dgram   udp     wait    root    internal
sgi-dgl  stream  tcp     nowait  root/rcv dgld
uucp     stream  tcp     nowait  root    /usr/lib/uucp/uucpd
```

SGI Irix (cont.)

```
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)

http://www.matasano.com/log/611/gunar-petersons-os-security-features-chart/

		Windows Vista	Windows XP SP2	RHEL 4	OpenBSD 3.x	Mac OS X
images	Section Reordering			■	■	
	EXE Randomization	■		□		
	DLL Randomization	■		■	■	
stack	Frame Protection	■	□	□	□	
	Exception Protection	■	□			
	Local Variable Protection	■	□	□	□	
	Randomization	■		■	■	
	Non-Executable	■		■	■	
heap	Metadata Protection	■	■			
	Randomization	■		■	■	
	Non-Executable	■	□	■	■	

■ 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 machne
- 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

```
CPUID: GenuineIntel 5.2.c irql:1f    SYSVER 0xF0000565

Dll Base  Date Stamp  - Name                  Dll Base  Date Stamp  - Name
80100000  2be154c9    - ntoskrnl.exe          80400000  2bc153b0    - hal.dll
80200000  2bd49628    - ncrc710.sys           8025c000  2bd49688    - SCSIPORT.SYS
80267000  2bd49683    - scsidisk.sys          802a6000  2bd496b9    - Fastfat.sys
fa800000  2bd49666    - Floppy.SYS            fa810000  2bd496db    - Hpfs_Rec.SYS
fa820000  2bd49676    - Null.SYS              fa830000  2bd4965a    - Beep.SYS
fa840000  2bdaab00    - i8042prt.SYS          fa850000  2bd5a020    - SERMOUSE.SYS
fa860000  2bd4966f    - kbdclass.SYS          fa870000  2bd49671    - MOUCLASS.SYS
fa880000  2bd9c0be    - Videoprt.SYS          fa890000  2bd49638    - NCR77C22.SYS
fa0a0000  2bd4a4ce      Vga.SYS               fa0b0000  2bd496d0      Msfs.SYS
fa8c0000  2bd496c3    - Npfs.SYS              fa8e0000  2bd496c9    - Ntfs.SYS
fa940000  2bd496df    - NDIS.SYS              fa930000  2bd49707    - wdlan.sys
fa970000  2bd49712    - TDI.SYS               fa950000  2bd5a7fb    - nbf.sys
fa980000  2bd72406    - streams.sys           fa9b0000  2bd4975f    - whnh.sys
fa9c0000  2bd5bfd7    - mcsxns.sys            fa9d0000  2bd4971d    - netbios.sys
fa9e0000  2bd49678    - Parallel.sys          fa9f0000  2bd4969f    - serial.SYS
faa00000  2bd49739    - mup.sys               faa40000  2bd4971f    - SMBTRSUP.SYS
faa10000  2bd6f2a2    - srv.sys               faa50000  2bd4971a    - afd.sys
faa60000  2bd6fd80    - rdr.sys               faaa0000  2bd49735    - bowser.sys

Address   dword dump   Build [1381]                                  - Name
fe9cdaec  fa84003c fa84003c 00000000 00000000 80149905                - i8042prt.SYS
fe9cdaf8  8025dfe0 8025dfe0 ff8e6b8c 80129c2c ff8e6b94                - SCSIPORT.SYS
fe9cdb10  8013e53a 8013e53a ff8e6b94 00000000 ff8e6b94                - ntoskrnl.exe
fe9cdb18  8010a373 8010a373 ff8e6df4 ff8e6f60 ff8e6c58                - ntoskrnl.exe
fe9cdb38  80105683 80105683 ff8e6f60 ff8e6c3c 8015ac7e                - ntoskrnl.exe
fe9cdb44  80104722 80104722 ff8e6df4 ff8e6f60 ff8e6c58                - ntoskrnl.exe
fe9cdb4c  8012034c 8012034c 00000000 80088000 80106fc0                - ntoskrnl.exe
```

Unix Host Security

```
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

/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

```
/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
```

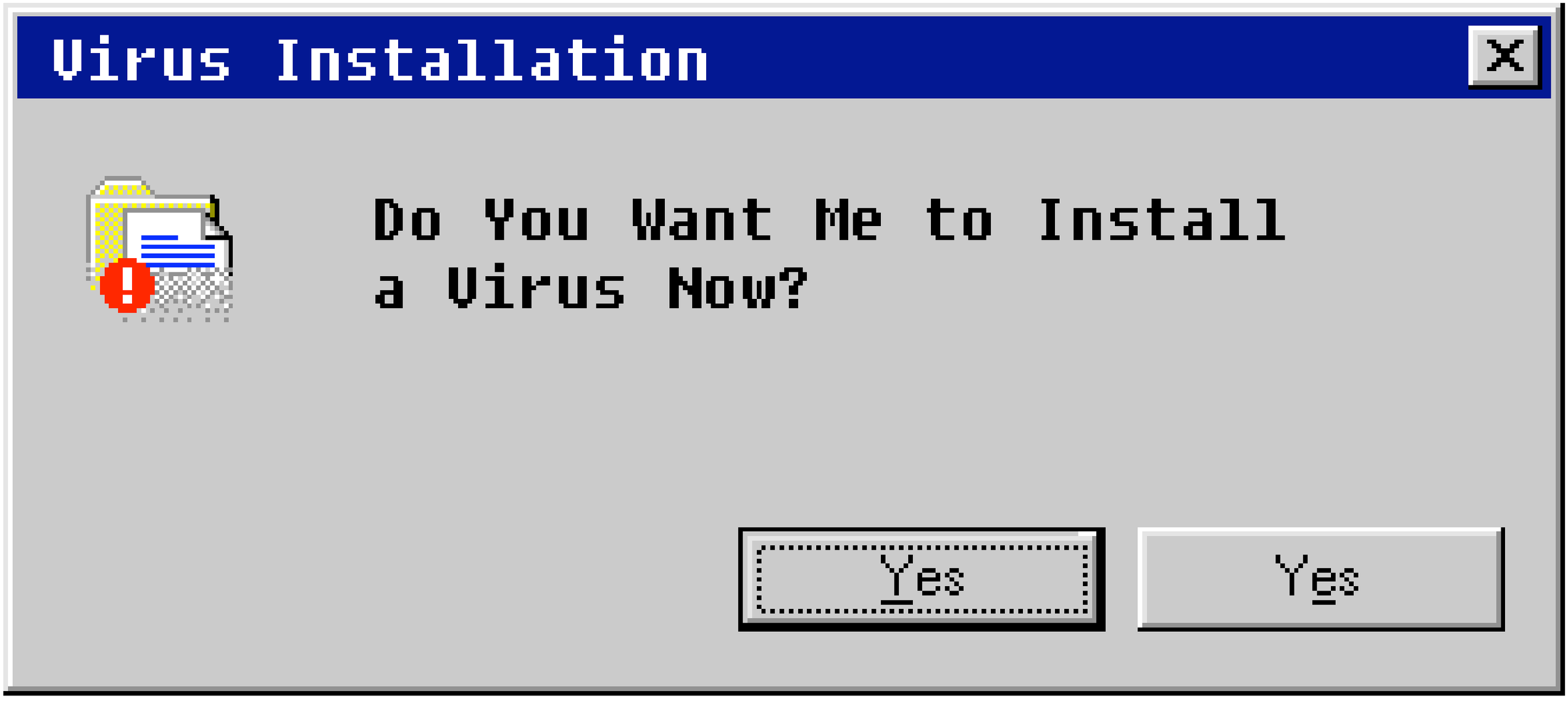
```
AIX 4.2                  & 242    & a staggering number \\
BSD/OS 3.0               & 78                \\
FreeBSD 4.3              & 42     & someone's guard machine\\
FreeBSD 4.3              & 47     & 2 appear to be third-party\\
FreeBSD 4.5              & 43     & see text for closer analysis \\
HPUX A.09.07             & 227    & about half may be special for this host
Linux (Mandrake 8.1)     & 39     & 3 appear to be third-party \\
Linux (Red Hat 2.4.2-2)  & 39     & 2 third-party programs \\
Linux (Red Hat 2.4.7-10)         & 31     & 2 third-party programs\\
Linux (Red Hat 5.0)      & 59           \\
Linux (Red Hat 6.0)      & 38     & 2--4 third-party \\
Linux 2.0.36             & 26     & approved distribution for one university
Linux 2.2.16-3           & 47           \\
Linux 7.2                & 42           \\
NCR Intel 4.0v3.0        & 113    & 34 may be special to this host \\
NetBSD 1.6               & 35           \\
SGI Irix 5.3             & 83           \\
SGI Irix 5.3             & 102          \\
Sinux 5.42c1002          & 60     & 2 third-party programs\\
Sun Solaris 5.4          & 52     & 6 third-party programs\\
Sun Solaris 5.6          & 74     & 11 third-party programs\\
Sun Solaris 5.8          & 70     & 6 third-party programs\\
Sun Solaris 5.8          & 82     & 6 third-party programs\\
Tru64 4.0r878            & 72     & \\
```

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 beautify
- 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