My Dad's Computer, Microsoft, and the Future of Internet Security

Bill Cheswick

ches@lumeta.com

http://www.lumeta.com


06/22/27
BURGER KING

My Dad's computer

Skinny-dipping with Microsoft

Case study: My Dad's computer

- Windows XP, plenty of horsepower, two screens
- Applications:
  - Email (Outlook)
  - "Bridge:" a fancy stock market monitoring system
  - AIM

Case study: My Dad's computer

- Cable access
- dynamic IP address
- no NAT
- no firewall
- outdated virus software
- no spyware checker

This computer was a software toxic waste dump

- It was burning a quart of oil every 300 miles
- The popups seemed darned distracting to me

My Dad's computer: what the repair geek found

- Everything
- "Viruses I've never heard off"
  - Not surprising: there are 200 new ones each day
- Constant popups
- Frequent blasts of multiple web pages, mostly obscene

Dad's computer: how did he get in this mess?

- He didn't know what the popup security messages mean
- Email-borne viruses
- Unsecured network services
- Executable code in web pages from unworthy sites

Three months after the cleanup

- An alien G-rated screen saver for an X-rated site appeared
- Changing the screen saver worked!
- The screen saver software removed in the correct way!
- Still, this should never have happened

Three months after *that* cleanup

- Windows XP installed, with firewall

This battle was never won

Is this a Bad Thing?

The answer was far from clear to my Dad

He was getting his work done

- Dad: “why do I care? I am getting my work done”
- Didn’t want a system administrator to mess up his user interface settings
- “Dad, hire an administrator to come check weekly.” “Not worth it?”
- Truly destructive attacks are rare
  - They aren’t lucrative or much fun
  - They are self-limiting

This software mess is an extremely common problem

- Technical people spend a lot of family time fixing computers
- This is an ongoing small business opportunity
- College students bring home badly corrupted computers
- Corporate intranets can have similar problems with similar users

```
*** STOP: 0x0000000A (0x802aa502,0x00000002.0x00000000,0xFA84001C)
IRQL_NOT_LESS_OR_EQUAL*** Address fa84001c has base at fa840000 - i8042prt.SYS

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   - ubnb.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

Restart and set the recovery options in the system control panel
or the /CRASHDEBUG system start option. If this message reappears,
contact your system administrator or technical support group.
```

“owned” computer

- The invader potentially has unlimited access to the software on the computer
- In some cases it is even possible to damage hardware
- He can install taps, new programs, delete or corrupt data, at will
- For computer people, this is clearly a Bad Thing
- Speculation: owned computers cost a perceptible fraction of the gross world product.

Botnets: hoards of “owned” computers

- Machines subjugated by worms, viruses, or direct attacks
- A single botnet may have 10,000 slaves and one master
- The “owner” of an “owned” host want to keep others out
  - Some worms and viruses actually patch their entry points, after installing back doors

Phatbot
http://www.lurhq.com/phatbot.html

- 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
- IP laundering stepping stones
- Web servers for phishing
- And, of course, keyboard sniffing on the computer itself
- Criminals and terrorists use these tools to raise money

Recent botnet prices (Stefan Savage)

- Spam forwarding bots: 3-10 cents per week
  - Lower if multiplexed access
  - Reputation counts
  - No command and control over the bots or botnet

Recent botnet prices (Rob Thomas)

- Botnets-to-order, fast connection bots: >= $1 per bot
- Windows-based bots on varied connections, including dialup: 10 cents/host
- Governmental special orders (you name the country) up to $40 per bot
- Sometimes broadband bots are traded for a Gig-Ethernet-connected compromised Sun.

Skinny Dipping on the Internet

Firewall-free access to the Internet

Angst and the Morris Worm

- Did the worm get past my firewall?
- No. Why?
  - Partly smart design
  - Partly luck…removing fingerd
- Peace of mind comes from staying out of the battle altogether

“You’ve got to get out of the game”

-Fred Grampp

“Best block is not be there”

- Mr. Miyagi (Pat Morita)

Karate Kid III

I've been skinny dipping on the Internet since mid-1990s

- FreeBSD and Linux hosts
- Very few, very hardened network services
- Single-user hosts
- Dangerous services placed in sandboxes
- No known break-ins
- No angst

Secure networking components

- Server
- Communications link
- Client
- The bozo in the chair

Secure servers

- Potentially do-able
- The experts run the servers: they are paid to get it right
- You must mistrust all clients, even with strong authentication!
- The database server shouldn’t trust the web server

Secure communications

- Got it! We won the crypto wars
- In June 2003, National Security Agency said that a properly implemented and vetted version of AES is suitable for Type 1 cryptography!
- Ssh is not perfect, but it is holding up pretty well

Secure client

- Few have it, but you can get close
- Almost nobody tries to get it even close
- It might be expensive and inconvenient to have it

The clown in the chair

- He (and us) are always going to be a problem
- Human engineering (i.e. spying) is infinitely varied and clever
- Phishing is currently the most rampant form
- “look for the lock”

A Unix system as a trusted client

“Unix is an administrative nightmare.”

-- Dennis Ritchie

“GUIs don’t fix Unix’s administrative nightmare.”

-- me

How do you measure security? Resistance against attacks

- Fire doors
- Safes
- Nuclear weapons

Rate a Unix systems 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 the weaknesses of a feature you do not use.

-- Microsoft security goal

/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
```

Some should not need root, or shouldn't be setuid

Least privilege

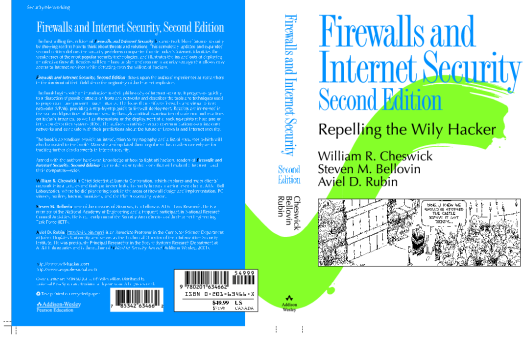
```
/sbin/ping
/sbin/ping6
/usr/X11R6/bin/xterm
/usr/X11R6/bin/Xwrapper-4
/usr/bin/crontab
/usr/bin/su
/usr/bin/lpq
/usr/bin/lpr
/usr/bin/lprm
/usr/bin/login
/usr/bin/passwd
/usr/bin/at
/usr/bin/chsh
/usr/bin/atrm
/usr/bin/atq
/usr/local/bin/sudo
/usr/sbin/traceroute
/usr/sbin/traceroute6
```

```
/usr/X11R6/bin/Xwrapper-4
/usr/bin/su
/usr/bin/passwd
/usr/bin/chsh
/usr/local/bin/sudo
```

Setuid gone on the Mac?

- If so, they have the best host security rating of any Unix-based computer
- But Macs have some new viruses of their own.
- Nobody at Apple is claiming that they are secure
  - My guess is that they are more secure than most

Setuid-root




```
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     & \\
```

A B1-rated system would help

- But administration makes a Unix system look easy
- CWTG

Client concerns, even on Unix

- The browser
  - They really need a lot of functions to use the Internet well these days
- Email clients
  - HTML content? It's hard to live without
- I see jails, sandboxes, and VM as solutions

Can my Dad (and millions like him) get out of the game?

Arms races

Virus arms race

- Early on, detectors used viral signatures
- Virus encryption and recompilation (!) has thwarted this
- Virus detectors now simulate the code, looking for signature actions
- Virus writers now detect emulation and behave differently
- Virus emulators are slowing down, even with Moore's Law.

Virus arms race

- I suspect that virus writers are going to win the detection battle, if they haven't already
  - Emulation may become too slow
  - Even though we have the home-field advantage
  - Will we know if an undetectable virus is released?
- Best defense is to get out of the game.
  - Don't run portable programs, or
  - Improve our sandbox technology
- People who really care about this worry about Ken Thompson's attack
  - Read and understand "On Trusting Trust"

Getting out of the virus game

- Don’t execute roving programs of unknown provenance
- Trusted Computing can fix the problem, in theory
- Why can’t we load the software into Dad’s computer, and just say “stay!” in a firm voice?
  - I’d let duly-signed agents, like Microsoft, change the code base

Arms Race Games

Password sniffing and cracking

Password sniffing and cracking arms race

- Ethernet has always been sniffable
- WiFi is actually *very thin* Ethernet
- Keystrokes can be logged if the client software (or hardware) is compromised.

Password sniffing and cracking arms race

- Password cracking works 3% to 60% of the time using offline dictionary attacks
  - More, if the hashing is misdesigned (*c.f.* Microsoft)
- This will never get better, so…
- We have to get out of the game

It is simply poor engineering to expect a human to choose and remember passwords that are not susceptible to dictionary attacks

Users are not going to pick passwords that are resistant to dictionary attacks. Period.

- Either don't let them pick passwords
  - Inconvenient for the users
  - Not a panacea (see below)
- Or don't give the bad guys a chance to run dictionary attacks---get out of the game
  - That means passwords are validated on the server, not the client
  - Ssh agent keys get this wrong
  - Bank ATM cards get this right

Password sniffing and cracking arms race

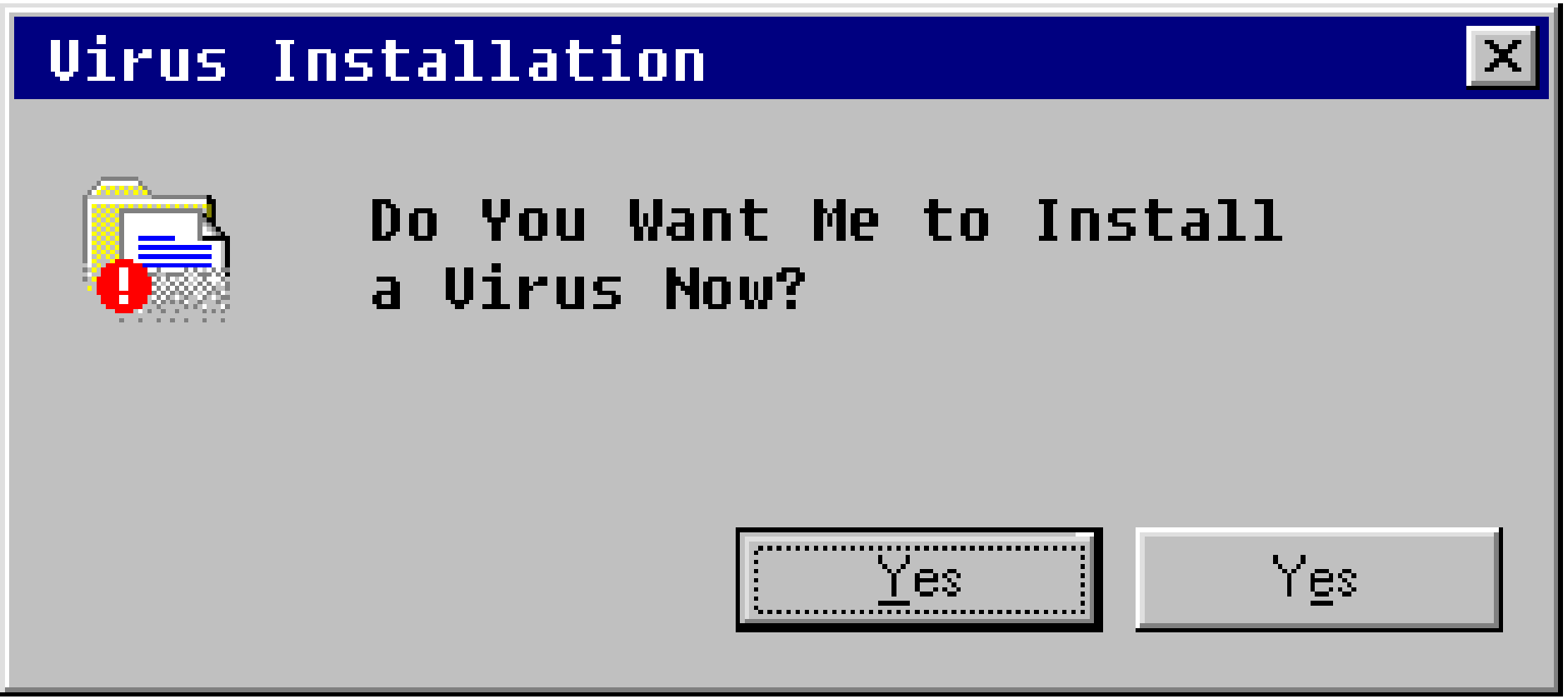
- This battle is mostly won, thanks to SSL, IP/SEC, and VPNs.
- There are many successful businesses using these techniques nicely.
- Current clear text services:
  - SNMP
  - POP3
  - AIM

Password sniffing was not a problem for Dad

- He had no important passwords to sniff
- AIM is interceptible
  - Fixable…will it be?
  - GAIM has a crypto module now

Authentication/Identification Arms races

- Password/PIN selection vs. cracking
- Human-chosen passwords and PINs can be OK if guessing is limited, and obvious choices are suppressed
- Password cracking is getting better, thanks to Moore's Law and perhaps even botnets


Virus Installation
Do You Want Me to Install a Virus Now?
Yes
Yes

Hardware tokens

- It would be nice if the server end is open source
- The business model has never been one for global adoption
- Challenge/response form factor is the safest, but not accepted

One-Time-Passwords are not perfect

- I installed these at Bell Labs in the early 1990s
- "We never had an undetected break-in" – me
- "Yes, you did." – Steve Branigan
  - Insecure client allowed session capture via Sun kernel module TAP

Arms Races: User deception

User education vs. user deception

- Phishing, spam offers, etc.
- We will continue losing this one
- Even experts sometimes don't understand the ramifications of choices they are offered

Authentication arms race: predictions

- I don't see this improving much, but a global USB dongle would do it
- Don't wait for world-wide PKI.

Arms Races: Hardware destruction

Arms race (sort of) hardware destruction

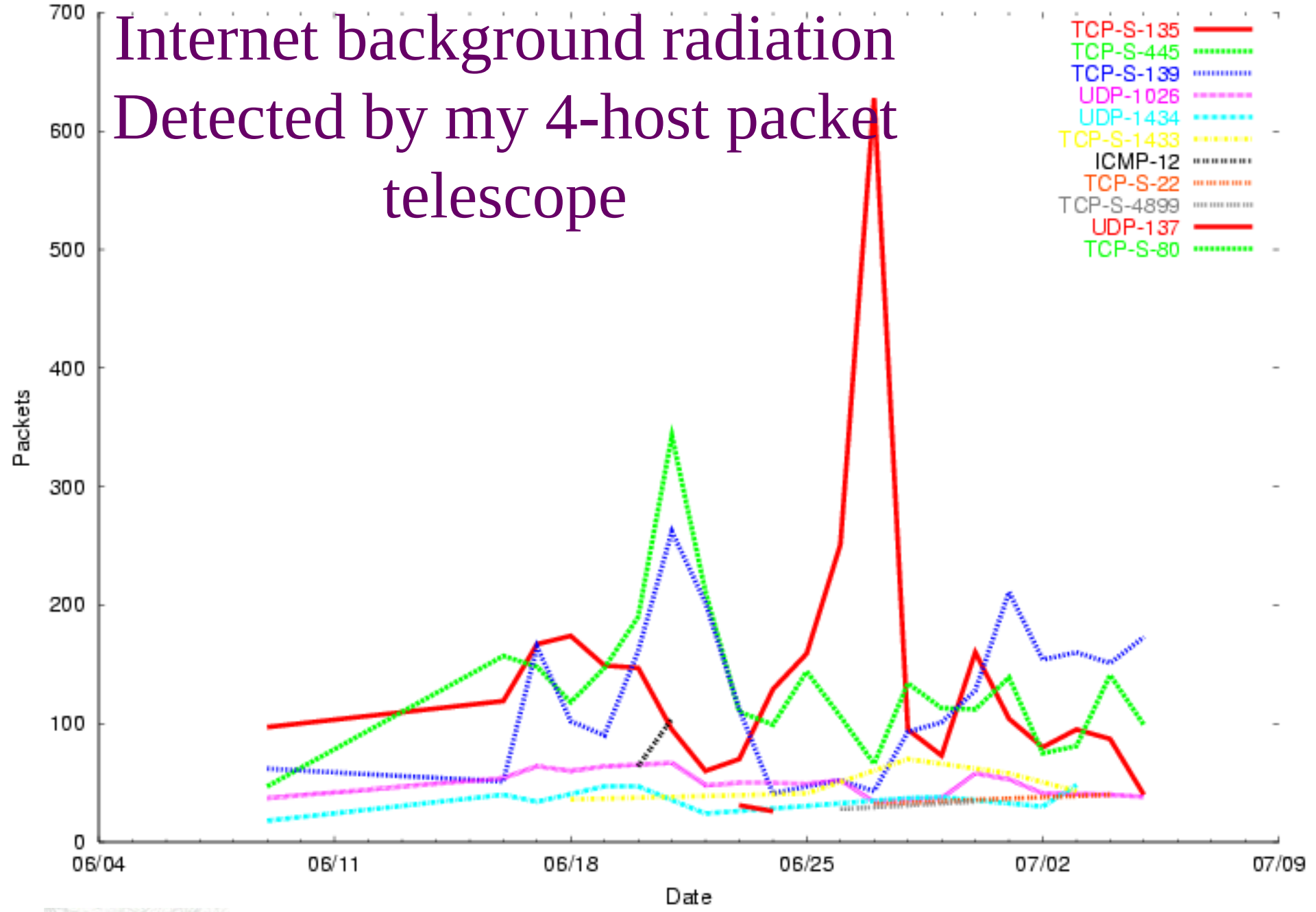
- IBM monochrome monitor
- Some more recent monitors
  - Current ones?
- Hard drives? Beat the heads up?
- EEPROM write limits
  - Viral attack on .cn and .kr PC motherboards
  - Other equipment
- Anything that requires a hardware on-site service call

Arms race (sort of) hardware destruction

- Rendering the firmware useless
  - This can be fixed (mostly) with a secure trusted computing base.

Arms Races: software updates

Internet background radiation Detected by my 4-host packet telescope



Software upgrade race: literally a race

- Patches are analyzed to determine the weakness
- Patch-to-exploit time is now down below 10 hours
  - NB: spammers have incentive to do this work
- Now the good guys are trying to obfuscate code!
- Future difficult to say: dark side obscures everything.

Arms Races: simulation/emulation

- Jails
  - Cliff Stoll and SDInet
- Honeypots
  - Honeynet
  - honeyd
- The deception toolkit---Fred Cohen
- Much recent work on detecting and hiding honeypots. The detectors will win.

Microsoft client security

It has been getting worse: can they skinny-dip safely?

Rate a computer's network security?

```
netstat -an | wc -l
```

Windows 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	223.223.223.10:137	*:*	
UDP	223.223.223.10:138	*:*	

Windows 2000

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	*:*	

Windows XP: this laptop, 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	*:*	

FreeBSD partition, this laptop (getting out of the game)

```
Active Internet connections (including servers)
Proto Recv-Q Send-Q  Local Address
tcp4       0      0  *.22
tcp6       0      0  *.22
```

It is easy to dump on Microsoft, but many others have made the same mistakes before

Default services SGI workstation

```
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
```

More default services

```
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 and David Wagner, *Usenix Security, 2004*
- Unchecked user-space pointers in system calls in Linux
- Mostly in device drivers
- New bugs appearing in new releases
- *BSD maybe no better

Firewalls and intranets try to get us out of the network services vulnerability game

What everyday computer users really need

Most of my Dad's problems were caused by weaknesses in features he never used or needed.

A proposal: Windows OK

Windows OK

- Thin client implemented with Windows
- It would be fine for maybe half the Windows users
  - Students, consumers, many corporate and government users
- It would be reasonable to skinny dip with this client
  - Without firewall or virus checking software

Windows OK

- No network listeners
  - *None* of those services are needed, except admin access for centrally-administered hosts
- Default security settings
- All security controls in one or two places
- Security settings and installed software can be locked

Windows OK (cont)

- There should be nothing you can click on, in email or a web page, that can hurt your computer
  - No portable programs are executed ever, except…
- ActiveX from approved parties
  - MSFT and one or two others. List is lockable

Windows OK

- Reduce privileges in servers and all programs
- Sandbox programs
  - Belt and suspenders

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.

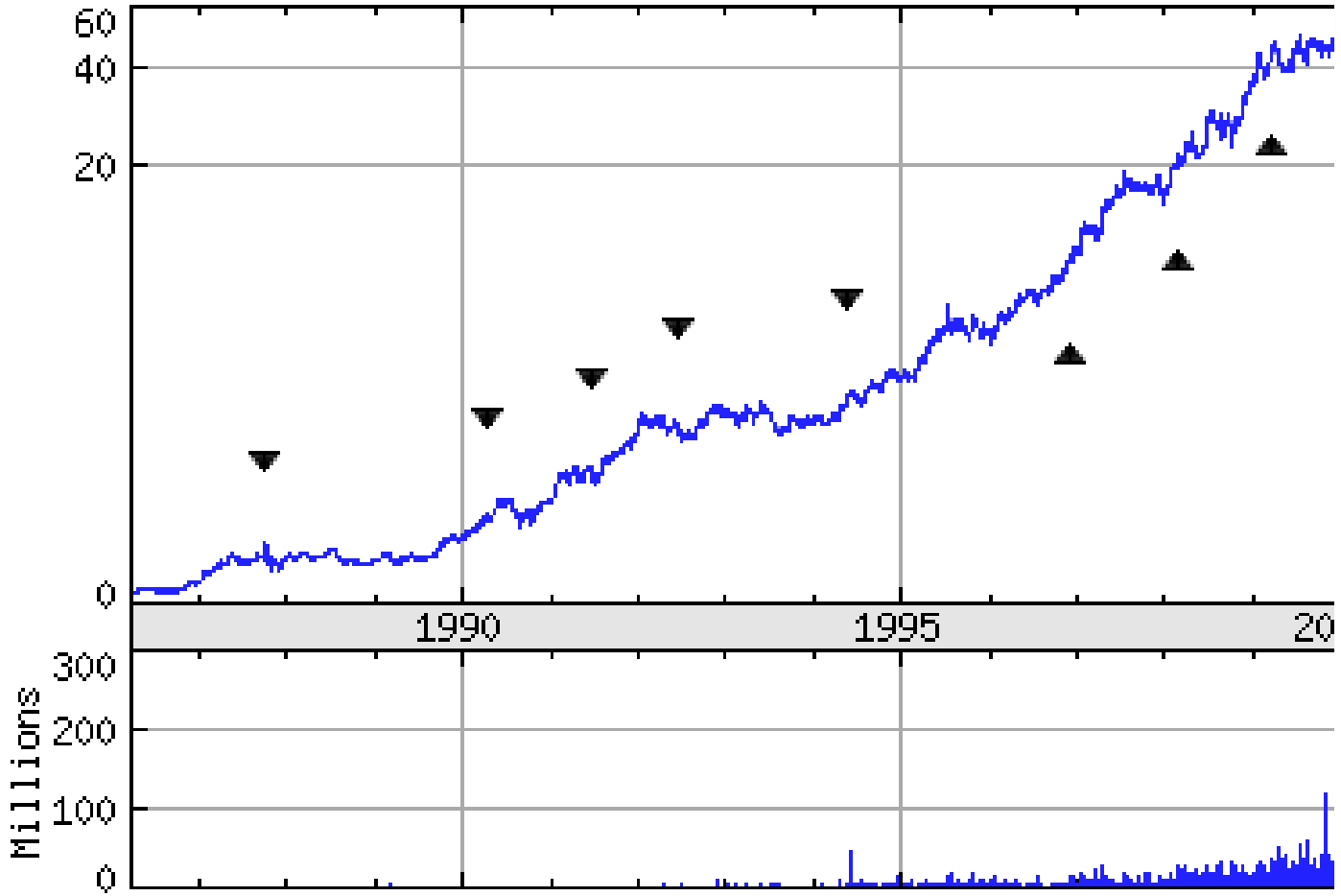
Vulnerabilities in OK: it wouldn't be perfect

- Buffer overflows in processing of data (not from the network)
- Stop adding new features and focus on bug fixes
- Programmers can clean up bugs, if they don't have a moving target
  - It converges, to some extent

Spooks and Tippy Top Secret Networks

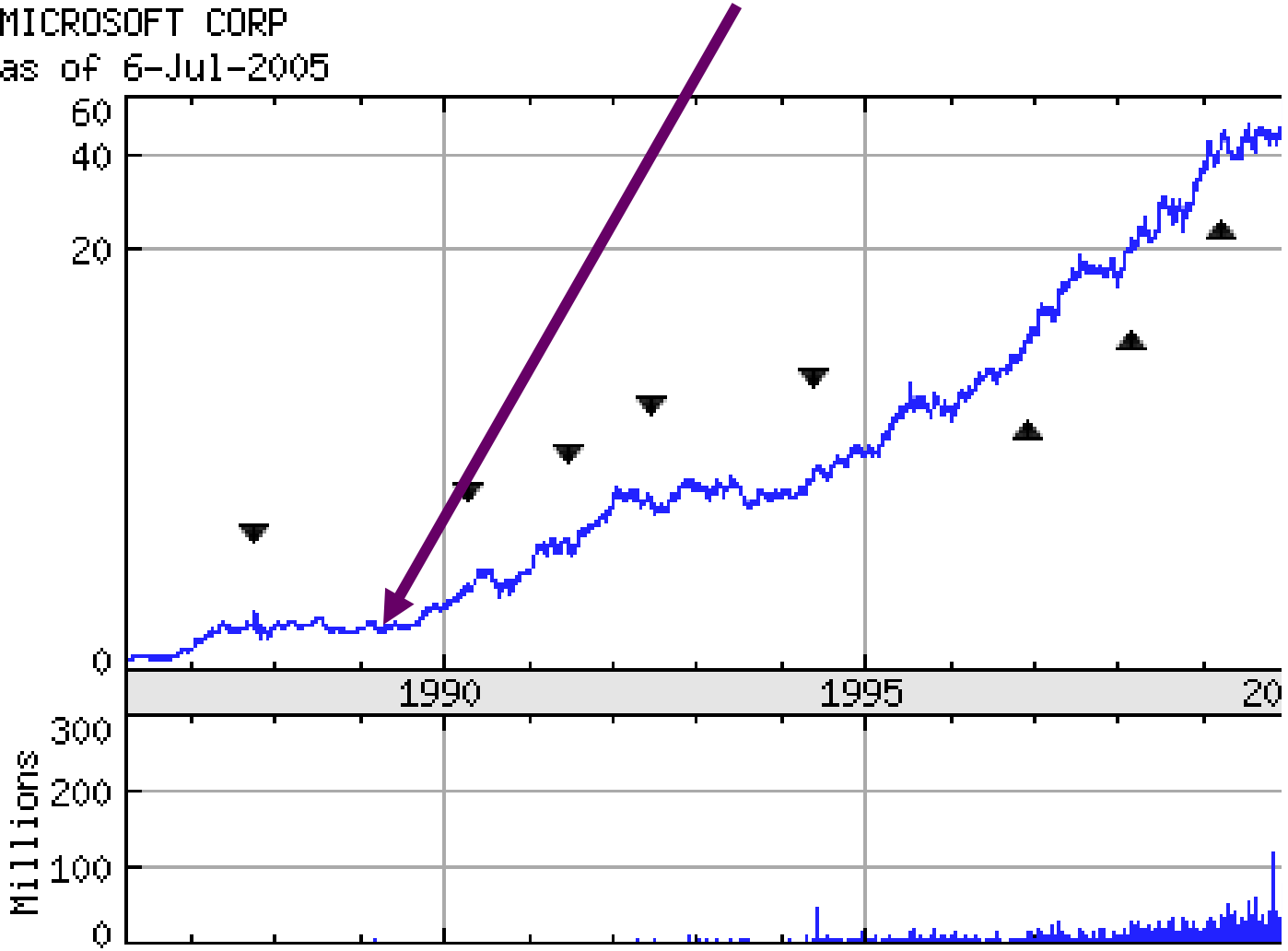
- Think about the requirements you would have on software and hardware on a network carrying mixed levels of top secret data
  - c.f. *Body of Secrets* (Banford) and his description of Intellink
- Trusted hardware
- Compartmentalized software (a VM for each level)
- Carefully-chosen COTS software, with $0.5MM spent on vetting it

What was Microsoft doing wrong? Nothing.



What was Microsoft doing wrong? Nothing.

Good time to sell stock and buy $16MM Porsche



XP SP2

Bill Gets It

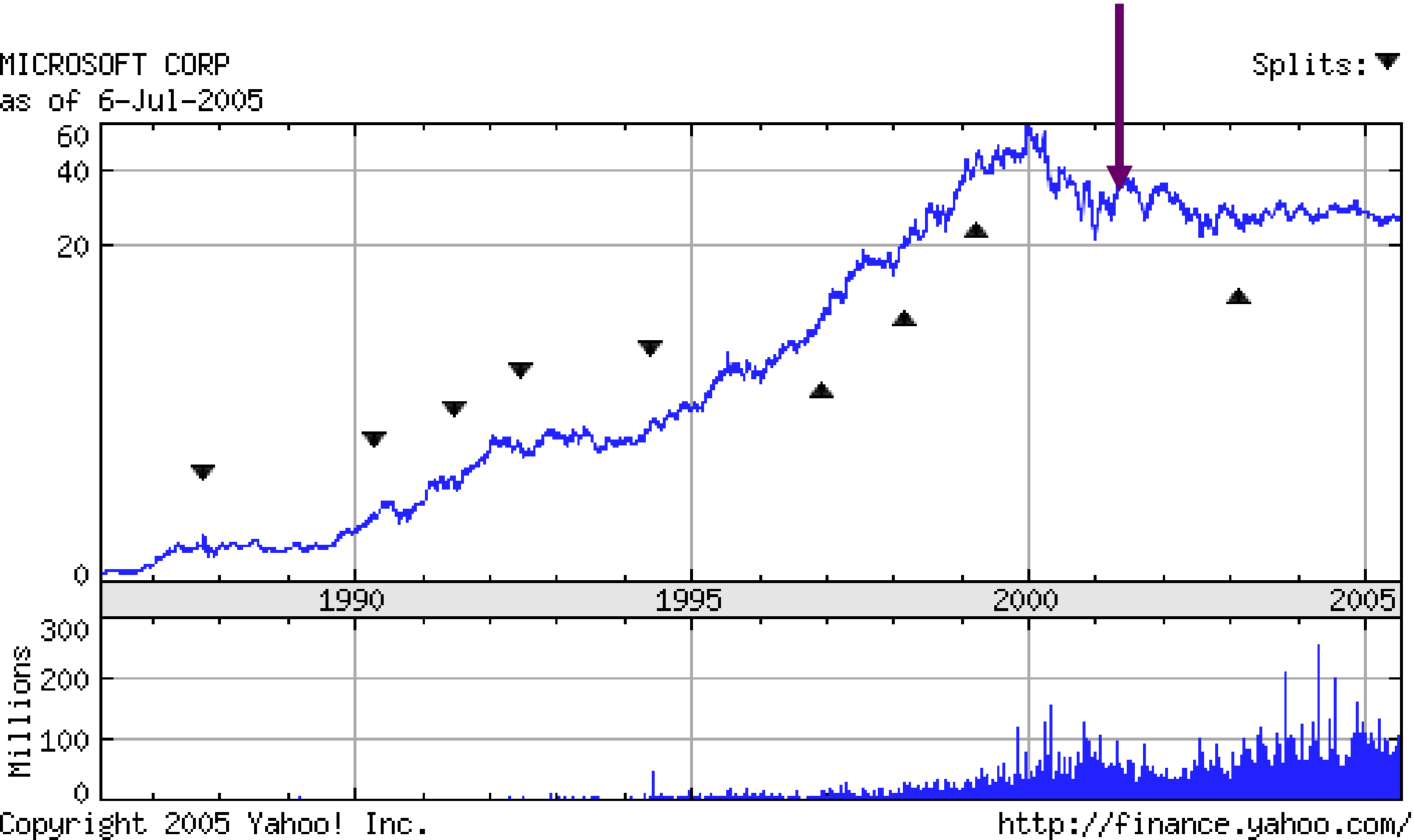
XP SP2: Bill gets it

- "a feature you don't use should not be a security problem for you."
- "Security by design"
  - Too late for that, its all retrofitting now. ***Longhorn!***
- "Security by default"
  - No network services on by default
- Security control panel
  - Many things missing from it
  - *Speaker could not find ActiveX security settings*
- There are a lot of details that remain to be seen.

Microsoft really means it about improving their security

- Their security commitment appears to be real
- It is a huge job
- Opposing forces are unclear to me
  - Marketing?
  - More demand for features? What about my number of slides?
- It's been a long time coming, and frustrating

Bill Gets It


MICROSOFT CORP
as of 6-Jul-2005
Splits:
60
40
20
0
1990
1995
2000
2005
300
200
100
0
Millions
Copyright 2005 Yahoo! Inc.
http://finance.yahoo.com/

Microsoft secure client arms race

- They have fixed a lot of low-hanging fruit
- But they have added new branches
- Longhorn/Vista is a rewrite
- Microsoft might win, but it is going to be a while
- This endeavor has no parallel that I can think of

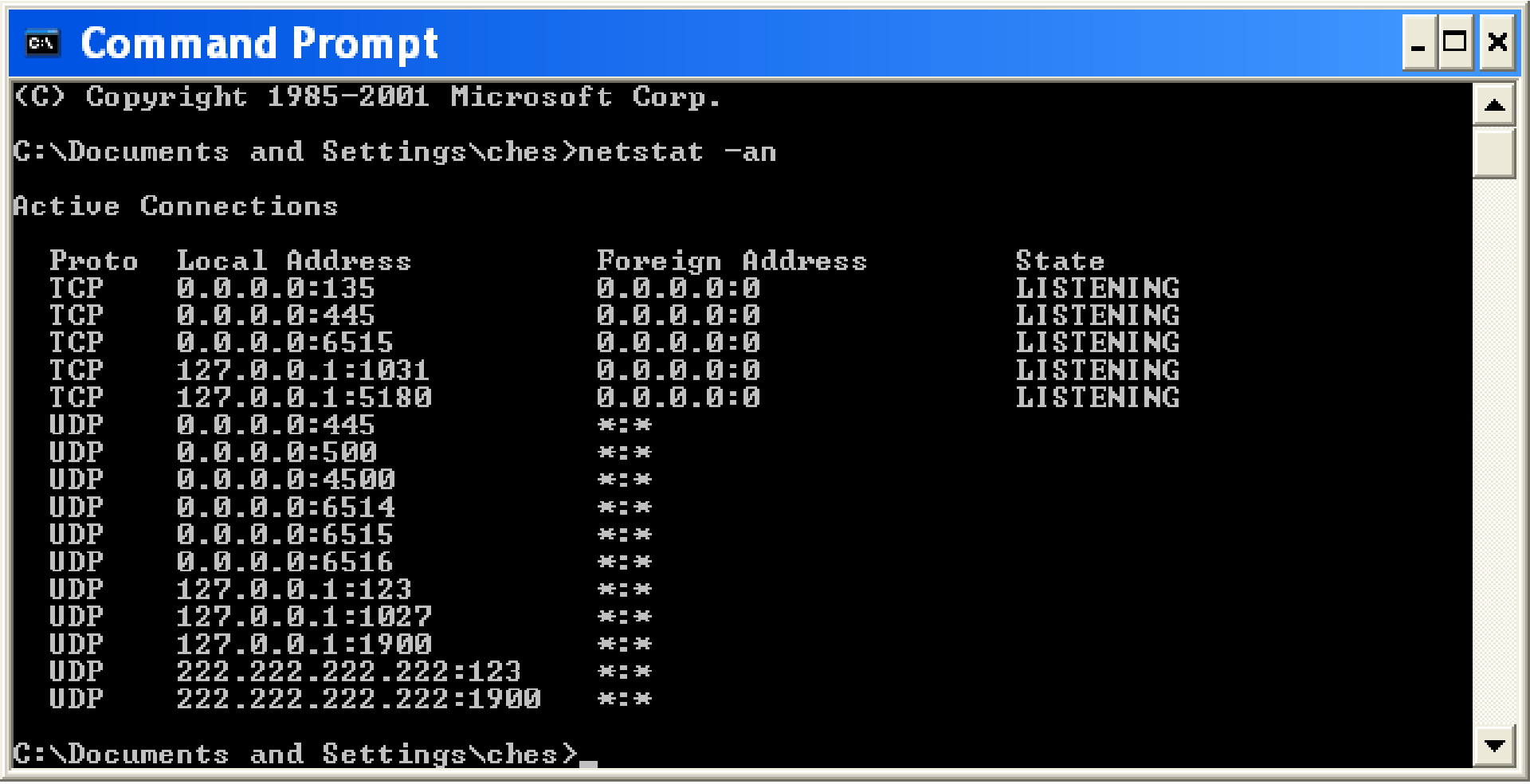
Microsoft's Augean Stables: a task for Hercules

- 3000 oxen
- 30 years
- (that's roughly one oxen-day per line of code in Windows)
- It's been getting worse since Windows 95


Windows Security Center
Security Center
Help protect your PC
Resources
Get the latest security and virus information from Microsoft
Check for the latest updates from Windows Update
Get support for security-related issues
Get help about Security Center
Change the way Security Center alerts me
Security essentials
Security Center helps you manage your Windows security settings. To help protect your computer, make sure the three security essentials are marked ON. If the settings are not ON, follow the recommendations. To return to the Security Center later, open Control Panel.
What's new in Windows to help protect my computer?
Firewall
ON
Automatic Updates
CHECK SETTINGS
Automatic Updates is set up to download and install updates only after checking with you. Click Turn on Automatic Updates to have Windows automatically keep your computer current with important updates (recommended). How does Automatic Updates help protect my computer?
Turn on Automatic Updates
Virus Protection
NOT MONITORED
You've told us you're using antivirus software that you will monitor yourself. To help protect your computer against viruses and other security threats, make sure that your antivirus software is turned on and is up to date. How does antivirus software help protect my computer?
Recommendations...
Manage security settings for:
Automatic Updates
Internet Options
Windows Firewall
At Microsoft, we care about your privacy. Please read our privacy statement.


Windows Security Center
Security Center
Help protect your PC
Resources
Get the latest security and virus information from Microsoft
Check for the latest updates from Windows Update
Get support for security-related issues
Get help about Security Center
Change the way Security Center alerts me
Security essentials
Security Center helps you manage your Windows security settings. To help protect your computer, make sure the three security essentials are marked ON. If the settings are not ON, follow the recommendations. To return to the Security Center later, open Control Panel.
What's new in Windows to help protect my computer?
Firewall
ON
Automatic Updates
ON
Virus Protection
ON
McAfee Managed VirusScan reports that it is up to date and virus scanning is on. Antivirus software helps protect your computer against viruses and other security threats. How does antivirus software help protect my computer?
Note: You now have antivirus software that Windows can monitor. Click Recommendations to find out how.
Recommendations...
Manage security settings for:
At Microsoft, we care about your privacy. Please read our privacy statement.

Windows XP: this laptop, with SP 2



SP2 was just a start: more work is needed

- Security panel and ActiveX permissions
  - Also, list of trusted signers needed
- Still too many network services
  - They may not be reachable from outside the box

SP2 wasn't easy to deploy in a big site

- Many people rely on unsafe configurations, even if they don't realize it
- Future SPs won't be easy either, especially if they follow my advice
- *It is a good sign that these installations are hard*
  - Visiting the dentist after 20 years of neglect
- Company deployments have trouble with version skew
- Use a Big Mallet

Windows Vista Home Basic

- For consumers that want to simply use the PC to browse the Internet, correspond with friends and family over email or perform basic document creation and editing tasks
- This ought to be Windows OK

Windows Vista Home Premium

- Everything in Windows Vista Home Basic, plus the Windows Vista Aero and Media Center and Tablet PC capabilities
- This is the Tivo/MythTV/home entertainment play

Windows Vista Business

- For small to medium size businesses
- Less reliant on dedicated IT support
- Better support for IT

Windows Vista Enterprise

- Windows Vista Business plus hardware encryption

Windows Vista Ultimate

- Windows Vista Home plus Business
- The works

Windows Vista Starter

- Cheap, emerging world version
- Can this be Windows OK?

Vista

- Clicking may still be dangerous
- Vista embodies a lot of these suggestions
  - There is a lot of work, which is certainly why it is behind schedule
- Lots of versions: all of the above, in 32 and 64-bit versions
- Hard to cut through the marketing words at this point
- Still touts firewalls and virus protection

Other Solutions for computer users like my Dad

Lindows/OpenOffice/vmware

- Tastes almost, but not quite, unlike tea.
- Ubuntu: still a memory hog
  - Gnome + evolution
- Vmware? Xen?
- Lumeta's choice…
  - There really isn't much of a plan B for most companies
  - (I used to have a secretary who knew troff)

Build an OS from scratch

- Not as hard as you might think
- "I couldn't sleep this weekend, so I rewrote the TCP/IP stack"
- Plan 9
- Various other research operating systems
- Has to keep up with current WinTel hardware
  - Centrino is a step backward for me
  - Drivers are a source of MSFT's security problems

Build an OS from scratch

- Start from scratch, with audibility as the principal goal
  - Like the old A1 systems
- The goal might be to run IE with demonstrable safety
- IBM's virus labs did this
  - VM with logging file system
  - Reset file system to pre-boot position post infection

Software scales

- Linus can write a kernel
- Don Knuth can write a kernel
  - Or inetd. Or a TCP/IP stack…
  - He gave his book *Literate Programming* to Bill Gates
- Profit is not necessarily required to obtain the software we need
- LinuxSE
  - More stuff from spooks?

Lot's of ideas out there

“It’s like thinking about your grandparents having sex: we wouldn’t be here if they hadn’t”

-Earl Bobert

Some ideas

- "we have a big problem supporting all those drivers" – Microsoft
  - Put them in a Multics-style "ring", confining them to least privilege?

Some ideas: hardware protection

- Stack smashing
  - Memory tagged with execute bits, a la Burroughs 5500
- Gcc support for hardware protections in X86 segments?
- Apparently, Win 2003 has this turned on, and it can be turned on on XP, though it breaks things.

Various ideas: software tools to clean up programs

- Automated privilege separation
- Software tools to detect unchecked user-supplied addresses in system calls
- Software checks for dangerous code
  - Microsoft has generated some of these programs internally
- "Setuid Demystified"
  - Get the semantics of system calls right
- How about a system call regression test suite?

Summary: we ought to win these battles

- We control the playing field
- DOS is the worse they can do, in theory
- We can replicate our successes
- We can converge on a secure-enough environment

Conclusions

- We've actually gotten noticeably better at Internet security in the past decade
  - Strong encryption is easy and can be ubiquitous
  - Robust clients are increasingly possible
  - Much server software is stronger now
  - Microsoft is trying to clean up their act
- None of this is easy to explain to non-technical users

My Dad's Computer, Microsoft, and the Future of Internet Security

Bill Cheswick

ches@lumeta.com

http://www.lumeta.com