40 Years of Internet Security, and the Future for Firewalls

Bill Cheswick

ches@research.att.com

Outline

- **The presenters will describe their views on the directions and trends that they anticipate tomorrow's security products and solutions will take to enable secure, de-perimeterized, global working across all organizations. They will welcome your feedback throughout this conference.**

Internet Security: history

- The third packet transmitted in 1969 crashed the server
- We have been making a lot of the same mistakes ever since
- Basically, the Internet is currently working fine, warts and all

Perimeters: A Brief History

- Before 1987: wide open, end-to-end principle
- Jeffrey C. Mogul, Richard F. Rashid, Michael J. Accetta. *The Packet Filter: An Efficient Mechanism for User-level Network Code*. *Proceedings of the 11th Symposium on Operating Systems Principles*, ACM SIGOPS, Austin, Texas, November 1987.
- November 1988: Morris Worm
- 1989: *Screend* paper
- Packet filtering widely available in routers

Other work from DEC

- Fred Avolio and Marcus Ranum
- Brian Reid and Paul Vixie
- DEC Gatekeeper, DEC SEAL
- Application level gateways

At Bell Labs

- Bill Cheswick, *The Design of a Secure Internet Gateway*. *Proceedings of the Usenix Summer Conference* (Anaheim), June 1990.
  - Described work by Dave Presotto, Howard Trickey, and then me

“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”

Also coined the word “proxy”

Described first circuit gateway (a la SOCKS)

Key Points

- With application level gateways, end-to-end is gone
- With circuit gateways, end-to-end intercepted at TCP level
- gateway designers got in the game of protocol-catchup

Key questions

- With the end-to-end paradigm somewhat broken (client/server still allowed in one direction), does that end research on the Internet?
  - Well, no. The web came out afterwards.
  - And many attempts to subvert firewalls
    - tunnels through port 80
- Can one live on the Internet without a firewall?

“You’ve got to get out of the game”

-Fred Grampp

“Best block is not be there”

- Mr. Miyagi (Pat Morita)

Karate Kid III

Skinny Dipping on the Internet

Secure networking components

Secure networking components

- Server

Secure networking components

- Server
- Communications link

Secure networking components

- Server
- Communications link
- Client

Secure networking components

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

Secure servers

Secure servers

- Potentially do-able

Secure servers

- Potentially do-able
- The experts run the servers: they are paid to get it right

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!

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, NSA 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 bozo 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”

The Secure Client is where we

- Windows clients?
- Unix clients?
- Macintosh clients?
- Thin clients?

Internet skinny dipping for me,

Internet skinny dipping for me,

- FreeBSD and Linux hosts

Internet skinny dipping for me,

- FreeBSD and Linux hosts
- Very few, very hardened network services

Internet skinny dipping for me,

- FreeBSD and Linux hosts
- Very few, very hardened network services
- Single-user hosts

Internet skinny dipping for me,

- FreeBSD and Linux hosts
- Very few, very hardened network services
- Single-user hosts
- Dangerous services placed in sandboxes

Internet skinny dipping for me,

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

Internet skinny dipping for me,

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

A Unix system as a trusted client

“Unix is an administrative nightmare.”

-- Dennis Ritchie

GUIs don’t fix administrative nightmares

How do you measure security? Resistance against attacks

How do you measure security? Resistance against attacks

- Fire doors

How do you measure security? Resistance against attacks

- Fire doors
- Safes

How do you measure security? Resistance against attacks

- Fire doors
- Safes
- Nuclear weapons

Crude host security metric

Crude host security metric

- Count the number of setuid-root programs

Crude host security metric

- Count the number of setuid-root programs
- Each is a potential door into privilege

Crude host security metric

- Count the number of setuid-root programs
- Each is a potential door into privilege
- Smaller numbers are more secure

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
```

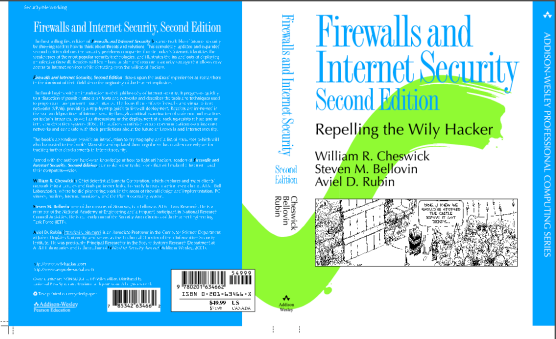
Some should not need root, or

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-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    & \\
```

Skinny dipping with the Mac?

- Has not been a target, to date
- Legacy software is a problem (old servers)
- Firewall seems effective
- Trouble can be invited in
- Has a lot of technical promise

Skinny-dipping with Microsoft:

Skinny-dipping with Microsoft:

- One hour of catching up

Skinny-dipping with Microsoft:

- One hour of catching up
- Four hours of cleaning up his Windows box

Skinny-dipping with Microsoft:

- One hour of catching up
- Four hours of cleaning up his Windows box
- Security measure: 1/(1+4) = .2
  - 1.0 is top security

Skinny-dipping with Microsoft:

- One hour of catching up
- Four hours of cleaning up his Windows box
- Security measure: 1/(1+4) = .2
  - 1.0 is top security
- Denial-of-free-time attacks

Skinny-dipping with Microsoft:

- One hour of catching up
- Four hours of cleaning up his Windows box
- Security measure: 1/(1+4) = .2
  - 1.0 is top security
- Denial-of-free-time attacks
- How much technical free time is eaten by these sorts of system administration demands?

These computers are software

These computers are software

- Burning a quart of oil every 300 miles

These computers are software

- Burning a quart of oil every 300 miles
- The popups seemed darned distracting to me

These computers are software

- Burning a quart of oil every 300 miles
- The popups seemed darned distracting to me
- We could not keep the machine clean

Is this a Bad Thing?

The answer was far from clear to my Dad

He is getting his work done

He is getting his work done

- Dad: “why do I care? I am getting my work done”

He is 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

He is 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?”

He is 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

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.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 C&C over the bots or botnet

Recent botnet prices (Rob Thomas, Team Cymru)

- 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 countries) up to $40 per bot
- Sometimes broadband bots are traded for a Gig-Ethernet-connected compromised Sun.

Microsoft client security

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

Measure of network security

- Number of network servers accessible from the outside
- The “surface area” of a system
  - (what are the units, bits^2)?)

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	0.0.0.0:31337	*:*	
UDP	0.0.0.0:162	*:*	
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-

```
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

```
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

```
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

What my dad, and many (most?) computer users really need

Most of my Dad's problems are caused by weaknesses in features he never uses or needs.

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.

Microsoft's Augean Stables:

Microsoft's Augean Stables:

- 3000 oxen

Microsoft's Augean Stables:

- 3000 oxen
- 30 years

Microsoft's Augean Stables:

- 3000 oxen
- 30 years
- (that's roughly one oxen-day per line of code in Windows)

Microsoft's Augean Stables:

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

XP SP2: Bill gets it

XP SP2: Bill gets it

- “a feature you don’t use should not be a security problem for you.”

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

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
- "Security by default"
  - No network services on by default

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
- "Security by default"
  - No network services on by default
- Security control panel
  - Many things missing from it
  - *Speaker could not find ActiveX security settings*

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
- "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

- 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

Microsoft secure client arms

- Microsoft might win, but it is going to be a while
- This endeavor has no parallel that I can think of

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.

Vista

Reading the tea leaves

Good signs

- It took longer than they expected
  - 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 may be painful
- Security training seems to be ongoing at MSFT
- New software analysis tools have appeared in their literature
- Spider honeymonkeys paper

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

Bad signs

- Last I knew, they were still using blacklisting, not whitelisting, of file types
  - Dangerous stance
- DRM requirements have required widespread modifications to break functionality when software is amiss
  - It is hard enough to make unbroken software without such foolishness

2007 Prediction:

2007 Prediction:

Vista is going to make Microsoft clients much better, but it will take a little while

Predictions about Vista

- Vista is going to be a success
  - Financial
    - Homes will get it because it's there
    - Industry will adopt it. Those running Win2K will have a harsher upgrade experience than those on XP SP2
  - Security
    - After the low hanging fruit is fixed
  - Investors need some patience
- The new look is nice, but mostly irrelevant

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 (does) this
  - Vmware 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

Some ideas

- "we have a big problem supporting all those drivers" – Microsoft
  - Put them in a Multics-style "ring", confining them to least privilege?
- Linux has the same problem, and is more brittle
- *nix has the same problem, and doesn't drive as much hardware

Some ideas: hardware protection

- Vista may be a leader now
- Intel finally has good support for virtualization
  - This is the belt-and-suspenders that large, dangerous software like browsers and mail readers need.

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?

IPv6

- Government: yes, definitely
- China: yes, definitely
- Cell networks: yes, definitely
- Overseas: mostly yes
- Corporate intranets: I don’t see the driver

IPv6 on intranets

- Double all the firewall rules (and some companies have thousands of firewalls) (and many have thousands of rules on a given firewall)
- Routers need to handle it, at least in slow path
- Address space will make asset control harder
  - Solution: insist that your routers know who is on their local networks, and insist that you have access to that information

Summary: we ought to win

- 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

40 Years of Internet Security, and the Future for Firewalls

Bill Cheswick

ches@research.att.com