The More Things Change...

Steve Romig
The Ohio State University
July, 2004
Game Plan

• We’ll look at events from the last 20 years
• What have we learned?
• What have we failed to learn?
• I’ll include some commentary about what OSU has done
1978-1983

• I went to college
• I worked as an intern at CompuServe
• Got a job at OSU’s Computer and Information Science Department
• Learning security in the “school of hard knocks”
In 1988...

• One new virus/month reported
• Viruses are “just” a PC thing
  • Unix admins had more serious problems
to worry about!
• The Internet has 60,000 hosts
1988-11-02 - The Morris Worm

- Affected Vax, Sun; through sendmail, fingerd, trusted hosts, passwords
- Early response - patch binaries with adb!
- Much FUD
- Contained within 3 days
- 3000-6000 hosts infected (5-10%)
1988-11-02 - TMVW: Aftermath

• Wakeup call
• Spafford's "Phage" list started
• CERT created
TMW: The Blame Game

- The miscreant
- The vendors
- The programmers
- The users
TMW: The Name Game

- Then: virus, worm, trojan horse
- Now: malware, rootkit, botnet, backdoor
TMW: Homogeneity on the Internet

- Then: 85% Unix (a dozen variants, though)
- Now: 90+% Windows (at least for desktops)
- Geer et al, 2003-09 - warnings about the monoculture
- What to do about it?
TMW: Vulnerabilities

- Buffer overflow in fingerd
- Fingerd runs as root
- "Overlooked" debug option in sendmail
- Password guessing
- Trusted hosts
- All known, fixable problems!
TMW: Vulnerabilities

- Are we better software engineers?
- Are we teaching “secure programming” any differently than we were back then?
- OTOH, more resources, awareness are available
- OTTH, the systems we create are increasingly complicated
1985 - TCP/IP Issues

• "A Weakness in the 4.2BSD UNIX TCP/IP Software", AT&T Bell Laboratories, by Robert Morris

• This describes TCP sequence number prediction

• This could be used to “spoof” trusted hosts

I read it. Though interesting, it seemed fairly obscure and "technical".

Back then, people broke in the old fashioned way: “by hand”.
1992 - Rbone, Neptune

- TCP/IP sequence guessing attacks
- Neptune (1994) has a nice user interface and error checking!
- This is the attack that I thought was too “technical” to be practical
- Writing the code (once) makes the technique widely available to the masses
1989 - Security Workshops

• “Computer Security Incident Handling” Workshops start in Pittsburgh

• Eventually leads (at least indirectly) to the formation of FIRST

• Many incident response teams form over the years

• Are we better at incident response?
1989ish - Mailing Lists Galore

- Full disclosure debates abound, then and now
- alt.security and comp.security created
- 1990-1991 - “Core” mailing list
- 1990 - “vsuite” mailing list
1989-1990

- 1989: Cliff Stoll publishes “The Cuckoo’s Egg”
- 1990: Sun security-alert mailing list begins
1990 Bugs

• Attacks through various “LAN services”:
  • ypserv, portmap, NFS (file handles, device files, general configuration issues)
• Available to the Internet at large
• Insecure default configurations
• Ring any bells?
1995ish - Unix
“Program” Rootkits

- Replaces ls, du, find, ps...
- Pinsh/ponsh backdoor
- Finger daemon backdoor
- Primitive library rootkit components
1995 - Much Password Cracking & Sniffing

• And again in 2004 - deja vu!

• We recognized the need to get away from reusable passwords then (and now)

• Hubs, switches, ssh, VPNs, WEP, dsniff, ettercap, WEP crackers, ssh client trojans...
1995 - OSU SECWOG Starts

- Monthly security awareness and training
- Instrumental in building a community that supports security initiatives at OSU
1995, April - SATAN Released

- Dan Farmer releases SATAN (or Santa, if you prefer)
- *Huge* furor over the release
- Dan loses his job at SGI over it
- Now: everyone has a vulnerability scanner!
1996 - OSU’s Local Miscreants

- They sniff passwords in our labs
- Use our dialup pool for free access
- Break into military and government sites
- No major dialup activity since then (apart from "usual" spam, viruses...)
- We wrote the OSU "review" software
1997 - OSU Starts Scanning

- Started with SATAN
- Purchased ISS Internet Scanner in 1997
- Distributed to departments
- Run centrally
Mid-1990’s

• Netbus, BackOrifice
• First primitive DDOS tools, botnets (via eggdrop, etc)
• Tripwire, Tiger, Cops...
1999 July 4 - DDOS Attacks at OSU

- 250? Unix hosts compromised
- Incoming DOS takes us out for 6 hours
- 50 of the 250 used for outbound DOS, 6 more hours of downtime, 15 buildings shut down on 3 day weekend
- We get more serious about blocking hosts that are compromised
1999 - DDoS Agents

- TFN
- Trinoo
- Stacheldraht...
2000

- OSU firewall project starts
- ILoveYou hits
2001

- Code Red
- NetStumbler
- War Driving
- Remember the 1996 miscreants sniffing passwords? Do you think they’re war driving?
2003 January - Slammer

- 10 minutes to infect most hosts
- 34 OSU computers infected
- Infection rates: 1.4m/hr inbound, 26.6m/hr outbound
- Patching becomes a "big deal"
2003 January - Slammer

- We used ISS' scanslam to ID vulnerable computers
- We used Cisco netflow logs to ID infected computers
- Infected, vulnerable computers are blocked automatically
2003 June - Adware and Spyware

- Largely ignored (by us) until then
- Finally receiving attention now
  - Good free software
  - Commercial products
- How did this stuff get into our computers without an uproar?
2003 August - Blaster

• Hard on the heels of password guessing attacks, many systems locked down

• MS03-039 patch released. Looks “important”, we see manual exploits

• More blocking of vulnerable, infected computers

• More incentive to patch things
2004 February - Bagle, MyDoom, Netsky, etc.

- Lots of email!
- Many, many variants
- Bounce email from A-V software on mail servers is almost as bad as the virus email itself!
2004 - We Come Full Circle

- Intruders sniffing, cracking passwords
- Local exploits to gain root, set up shop
- By hand - little/no automation
2004 - Viruses

- OSU finally gets anti-virus on the central email system
- 1.5m messages/day
- 100,000 viruses
<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>SomeFool</td>
<td>66,885</td>
</tr>
<tr>
<td>Bagle</td>
<td>17,633</td>
</tr>
<tr>
<td>MyDoom</td>
<td>8,598</td>
</tr>
<tr>
<td>Zafi</td>
<td>1,542</td>
</tr>
<tr>
<td>Lovgate</td>
<td>1,020</td>
</tr>
<tr>
<td>Damaru</td>
<td>940</td>
</tr>
<tr>
<td>Gibe</td>
<td>118</td>
</tr>
<tr>
<td>Sircam</td>
<td>41</td>
</tr>
</tbody>
</table>
Things That Haven't Changed

- Bugs, design flaws in software
- The full-disclosure debate
- Default installs are (largely) insecure
Things That Are Better

- More incident response teams, abuse contacts
- Vendors seem responsive, sort of, after the fact
- More awareness
Things That Are Worse
## Increasing Incidents

<table>
<thead>
<tr>
<th>Year</th>
<th>Incidents</th>
</tr>
</thead>
<tbody>
<tr>
<td>1994</td>
<td>2</td>
</tr>
<tr>
<td>1995</td>
<td>11</td>
</tr>
<tr>
<td>1996</td>
<td>102</td>
</tr>
<tr>
<td>1997</td>
<td>308</td>
</tr>
<tr>
<td>1998</td>
<td>348</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>2002</td>
<td>1145</td>
</tr>
<tr>
<td>2003</td>
<td>786/4039</td>
</tr>
</tbody>
</table>
Increasing Automation

- Easy for them to infect 100's of thousands of hosts
- 200,000 hosts picking up agobot from OSU in 3 days...
- On the other hand, we’re more automated also
Increasing Sophistication

- Better rootkits (HackerDefender)
- Encryption
- Agobot
Increasing Variations

- Agobot - hard to analyze them all
- If you don’t have time to really analyze them, how do you know what they do, how to clean it up, etc?
Increased Economic Incentives

- Spam
- Industrial espionage
- Identity theft
- Extortion
The Stakes Are Higher

- The Internet isn't just a "cool toy" any more
- Our y2k survival plan: use paper forms
- In 2004, the paper forms don't exist
- The Internet is a must-have: distance education, business processes, communication...
Worm Futures

- Fast spreading (through early recon)
- Multi-vector, multi-platform
- Field upgradable
- Better communications - firewall/proxy savvy, crypto, multiple methods
- Stealthier (rootkits, smarter scanning)
Books

- 1985 - Unix System Security
- 1991 - Practical Unix Security
- 1994 - Firewalls and Internet Security
- 1999 - First of the “Hacking Exposed” books
More Books

- 2002, 2003 - Honeypots and Honeynets; Snort; Intrusion Detection
- 2003, 2004 - Malware; Exploiting Software; Hacker Disassembling Uncovered; Shellcoder’s Handbook; more in the works...
Critical Things

- Lots of information (netflow, logs, etc.)
- Organized incident response
- Ability to block vulnerable, infected hosts
- Awareness, education, training
- Community
Challenges

- 10,000+ user-owned machines
- Network registration, vetting, self-remediation
- Awareness, training
- Remote access and reusable passwords
Summary

• (Almost) nothing new under the sun - learn from the past!

• Read some old security papers, especially Spaf’s on TMW and Thomson’s “On Trusting Trust”

• If you don’t secure it, it will get hacked

• Go read phrack, blackhat.org
References

• securitydigest.org - old security mailing lists


• csrc.nist.gov/publications/history - a collection of old security papers

• www.net.ohio-state.edu/security/talks.shtml - slides for this talk, other talks at OSU