

# Network attacks

Robert H. Sloan



# Outline

1. Overview of attacks involving network
2. Bots and DoS
3. Then defenses: Firewalls, Logs and auditing logs, IDS, etc.



# Specific network attacks

- Snooping/sniffing: passively reading packets bound for other machines
- IP spoofing: falsify source IP address so it appears to come from different computer
- Man-in-the-middle attacks and replay attacks



# And, DoS

- Denial-of-service (DoS): any attack designed to disrupt availability to authorized users.
- Normally by saturation of something, especially network bandwidth by e.g., via P2P file sharing or IM apps



# Common points of attack

- Web Server
- DNS Server
- Mail server (SMTP)
- Firewall itself; especially DOS
- Test/Development Systems



# Who attacks and why

- The Challenge (So 1999)
- Fame (ditto)
- Industrial Espionage
- **Profit, especially by organized crime**
- Ideology: Hacktivism/Cyberterroism
  - Estonia 2007, Google recently?



# Aside: Estonia 2007

- Botnets heavily used, almost certainly some leased out
- Exact source unknown, but highly organized
- “Patriotic hackers;” involvement of Russian government alleged; cannot be confirmed
- Combined some characteristics of military campaign and covert operation



# DOS/DDoS

- DOS: Attack on availability
- Distributed Denial of Service (DDoS) attack is mounted from multiple platforms
- Successful attacks two pronged:
  1. Attack the protection of computers
  2. Used the compromised systems for DOS attacks on intended victim



# Denial of Service Attacks in general

- Keep the system so busy that it does not have time to respond to legitimate requests
- Exhaust something:
  - Network bandwidth
  - System resources either at transport layer or in some application (e.g., web server)



# For example

- Flooding attacks using the SYN start of TCP connection formerly very popular; still around.
- Floods the buffer that is used in the middle of the 3-way SY handshake
- Various attacks against DNS itself popular



# 2007: DNS Backbone

There are 13 highest-level (*above .com, .org, etc.*)  
DNS *root name servers*. Some are in fact  
distributed. As of March 2007:





# Attack: Feb 6, 2007

- 5 hour attack starting around 11 a.m. Central time by botnet allegedly traced to South Korea against all the root name servers.
- None crashed, but two “suffered badly”; rest had “heavy traffic.”
- At height of attack; 94% of DNS queries answered as opposed to usual near 100%



# Bots, botnets

- **Bot** (robot) or **zombie** or drone is program that secretly takes over another Internet-attached computer and uses it for no good
- Difficult to trace to bot's creator
- In **botnet** of hundreds to (often) 10,000+ to (sometimes) 1.5 million to 10–15 million (Conficker) controlled by **herder**.



# Botnets

- Got started in serious way around 2004; explosive growth since then
- Jan. 2008 estimate: *3.7 million instances per day* of bot doing something no good
- Rental prices dropping; \$200/day for 100,000



# Botnet prognosis

“There's no economic incentive for [a smaller] ISP to sit on the phone for an hour and a half to help a customer get [his or her machine] disinfected. The cost of that is more than the subscription cost,” said Stewart. That fact, coupled with the large percentage of computer users running Windows versions without up-to-date patches, creates an environment that's ripe for abuse.

— “Is the Botnet Battle already Lost?”, *eWeek.com*,  
October 2006



# That was optimistic view....

On a typical day, 40% of the 800 million computers connected to the Internet are bots engaged in distributing e-mail spam, stealing sensitive data typed at banking and shopping websites, bombarding websites as part of extortionist denial-of-service attacks, and spreading fresh infections

—Rick Wesson, CEO of Support Intelligence, quoted in *USA Today*,  
March 2008



# Bot Uses

- DDoS
- Spamming
- Keylogging and packet sniffing
- Spreading new malware
- Installing adware for profit
- Click fraud; manipulating online polls



# What to do about DDoS attacks

- **Protect machines against compromise!**
- Turn off/refuse connections from attacking machines
- First have to identify the attacking machines



# Identification of attacking machines

- Volume protects the attackers
- More machines in attack  $\Rightarrow$  fewer packets per attacking machine suffice
- Really hard to distinguish low-level DOS attack from increase in business
- $\Rightarrow$  Impossible to prevent very large DDoS attacks by detection and countermeasures