Internet Worms, SYN DOS attack

- Eugene H. Spafford; "The Internet Worm Program: An Analysis"; ACM COMPUTER COMMUNICATION REVIEW; ACM Press, New York,NY; 19(1), pp. 17-57, Jan 1989
- Christoph L. Schuba, Ivan V. Krsul, Markus G. Kuhn, Eugene H. Spafford, Aurobindo Sundaram, Diego Zamboni, "Analysis of a Denial of Service Attack on TCP". Proceedings of the IEEE, 1997
- RFC 2525 - Known TCP Implementation Problems
  - http://www.faqs.org/rfcs/rfc2525.html

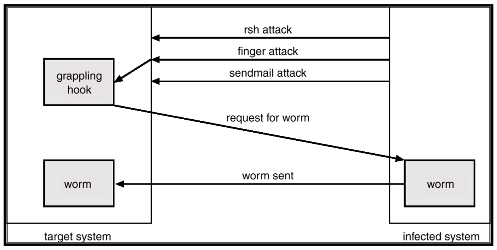
Internet Worm

- November 2, 1988: Robert T. Morris Jr. Internet worm
  - Graduate student at Cornell University. Son of the chief scientist at the National Computer Security Center -- part of the National Security Agency
  - Convicted in 1990: $10,000 fine, 3 yr. Suspended jail sentence, 400 hours of community service
  - Today he’s a professor at MIT

System Threats (from Silberschatz)

- Worms – use spawn mechanism; standalone program
- Internet worm
  - Exploited UNIX networking features (remote access) and bugs in *finger* and *sendmail* programs
  - Grappling hook program uploaded main worm program
- Viruses – fragment of code embedded in a legitimate program
  - Downloading viral programs from public bulletin boards or exchanging floppy disks containing an infection
  - *Safe computing*
- Denial of Service
  - Overload the targeted computer preventing it from doing any useful work

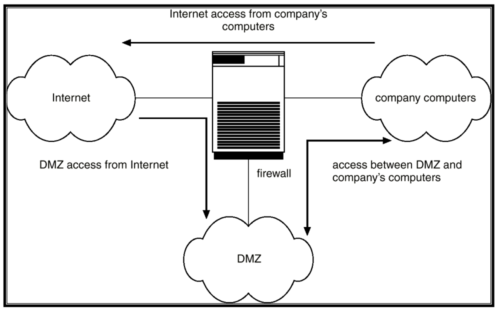
The Morris Internet Worm



FireWall

- A firewall is placed between trusted and untrusted hosts
- The firewall limits network access between these two security domains
  - Prevent internal clients from accessing “forbidden” external nodes (e.g. adult sites)
  - Prevent external nodes from sending malicious objects into protected network
  - SYN flood attacks etc.

Network Security Through Domain Separation Via Firewall


Internet access from company's computers
Internet
company computers
DMZ access from Internet
firewall
access between DMZ and company's computers
DMZ

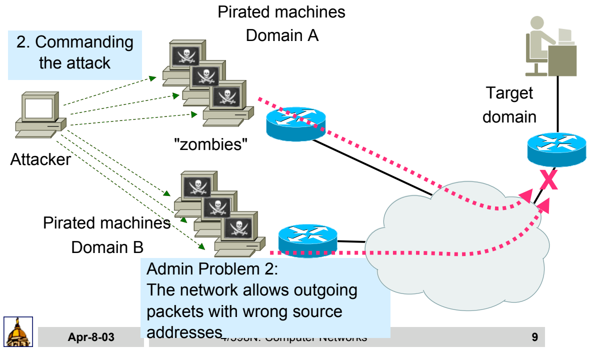
Demilitarized Zone (DMZ)

Intrusion Detection

- Detect attempts to intrude into computer systems.
- Detection methods:
  - Auditing and logging.
  - Tripwire (UNIX software that checks if certain files and directories have been altered – I.e. password files)
- System call monitoring

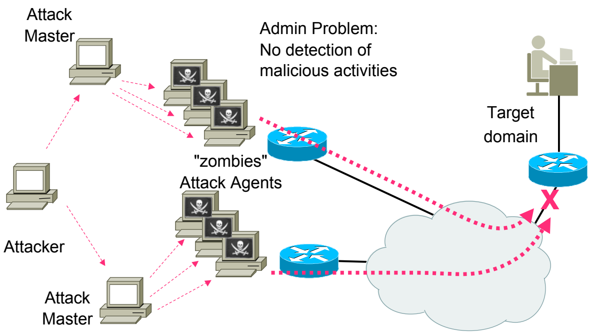
SYN flooding

Network Attacks: Distributed DoS (courtesy Georgios Koutepas)



Admin Problem 2:
The network allows outgoing packets with wrong source addresses

Multi-tier attack



Admin Problem:
No detection of malicious activities

Discussion

- Protocols and components should be designed and evaluated not only on their performance gains, but also on their robustness against implementation flaws