Song
Spring 2015

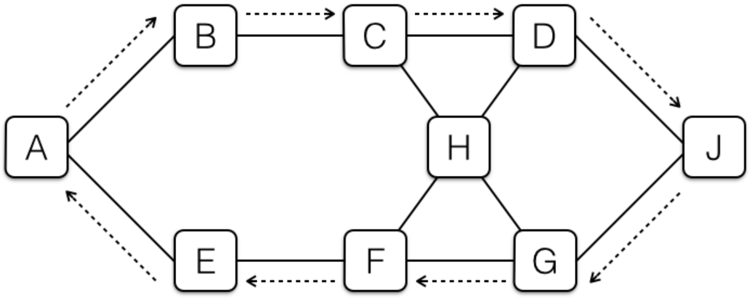
CS 161
Computer Security

Discussion 11

April 7 & April 8, 2015

Question 1 ***TCP*** **(25 min)**

Consider the following network topology:



The machine A has initiated a TCP connection to machine J. As it turns out, all packets from A to J happen to follow the path indicated by the right-facing dotted arrows, and all packets from J to A happen to follow the path indicated by the left-facing dotted arrows. Machines A and J use modern TCP software and do not have any special defenses against attack.

(a) Suppose that Mallory controls (only) machine C. Can she inject RST packets destined for machine J into this TCP connection, such that they will be accepted by machine J? Why or why not?

(b) Suppose that Mallory controls (only) machine C. Can she inject spoofed data into this TCP connection, so machine J will accept the spoofed data thinking that it came from machine A? Why or why not?

(c) Suppose that Mallory controls (only) machine H. Can she inject spoofed data into this TCP connection, so machine J will accept the spoofed data thinking that it came from machine A? Why or why not?

(d) Suppose that Mallory can eavesdrop on all packets that go through machine C (but cannot inject forged packets from C). Also Mallory can run software on machine F that lets her inject forged packets from F (but cannot eavesdrop on packets going through F). Can Mallory injected spoofed data into the TCP connection, so that it will be accepted by machine J as though it came from A? Why or why not?

(e) Suppose that Mallory can eavesdrop on all packets that go through machine F (but cannot inject forged packets from F). Also Mallory can run software on machine F that lets her inject forged packets from C (but cannot eavesdrop on packets going through C). Can Mallory injected spoofed data into the TCP connection, so that it will be accepted by machine J as though it came from A? Why or why not?

Question 2 ***Denial-of-service*** (25 min)

An anti-spam company, GreenMail, uses a vigilante approach to fighting spam.[1] GreenMail's customers report their spam to GreenMail, and the company then automatically visits the websites advertised by the URLs in the spam messages and leaves complaints on those websites. For each spam that a user reports, GreenMail leaves a generic complaint. GreenMail operates on the assumption that as the community grows, the flow of complaints from hundreds of thousands of computers will apply enough pressure on spammers and their clients to convince them to stop spamming.

After a short while of operation, GreenMail's public web site comes under a massive DDoS attack that uses SYN flooding.

(a) Briefly describe the type of traffic that an attacker sends to launch a SYN flooding attack.

(b) Briefly describe how the attack can cause a denial-of-service.

(c) Can GreenMail use a packet-filter firewall to defend itself against the DDoS that uses SYN flooding?

If so, describe what sort of rule or rules the firewall would need to apply, and what "collateral damage" the rules would incur.

If not, explain why not.

(d) Explain how the GreenMail service could itself be used to mount a DoS attack.

(e) Briefly describe one approach that victims could use to defend themselves against the attack you sketched.

[1] FYI, this is based on an actual company and its experiences.