Song
Spring 2015

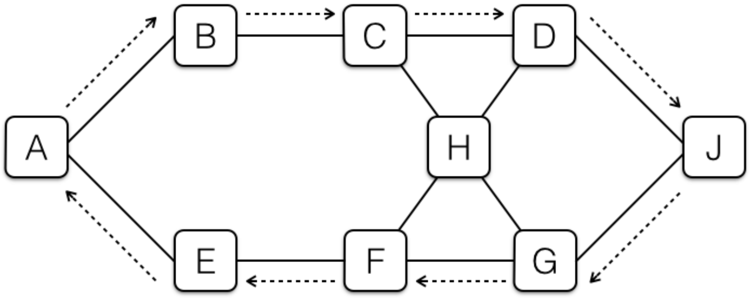
CS 161
Computer Security

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?

> **Solution:** Yes. She is on-path and can see the sequence numbers, so she can inject a forged RST packet with the right sequence number.

(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?

> **Solution:** Yes. She is on-path and can see the sequence numbers for both directions, so she can inject a forged data packet with the right sequence numbers.

(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?

Solution: No. She is off-path and cannot observe the sequence numbers.

(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?

Solution: Yes. She is on-path, so by observing packets traversing machine C, she can observe the sequence numbers. Then, she can inject a spoofed packet from machine F.

(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?

Solution: Alas, this question had a typo: it should have said "Mallory can run software on machine C that lets her inject forged packets from C (but cannot eavesdrop on packets going through C)." To be fair and avoid penalizing people who were misled by the typo, we decided to grade only your answers to parts (a)–(d), but not your answer to part (e).

For those curious, with the correction, the correct answer is: Yes. She can see the sequence numbers for both directions (since they're contained in the handshake, and also every packet from J to A contains an acknowledgement that mentions the sequence number of the last packet that J received from A). This is enough that she can inject a forged packet that J will accept. Note that TCP connections have two independent sequence number spaces: the data from A to J is labelled with one range of sequence numbers, and the data from J to A uses another unrelated range of sequence numbers. It might be tempting to think that Mallory can see only the latter sequence numbers but not the former, and so won't know what sequence number to put into the forged packet destined for J. However, in fact, acknowledgements from J to A mention the sequence number of the last packet from A to J that was received by J, so the acknowledgements will reveal the sequence number that Mallory needs to make the attack work.

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

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

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.

> **Solution:** A SYN flooding attack sends a stream of TCP "initial SYN" packets to the targeted server. Each packet appears to represent a request to establish a new connection.
>
> Note that the attacker *may* spoof the source addresses of such SYNs to make them harder for the defender to filter them out, but this is not required. An attack that employs a large botnet, for example, might not use spoofing.

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

> **Solution:** For each incoming SYN packet, the server both responds and consumes memory because it records information (state) associated with the impending new connection. The attack primarily aims to exhaust the server's available memory for keeping this state.

(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.

> **Solution:** Here are two possible answers:
>
> (1) If the flood uses a fixed number (not too large) of IP source addresses in its packets, then the target could install a number of firewall rules that deny traffic from those addresses. In this case, the collateral damage depends on how much legitimate traffic also comes from those addresses.
>
> (2) If the flood uses a very large number of IP source addresses, either by employing a large number of different systems ("bots") to send the traffic, or by spoofing the IP source address in each SYN packet, then the target will not be able to specify enough firewall rules to defend against the attack. Note that the

target cannot use a rule such as "drop any incoming TCP SYN sent to our web server" without enabling the attack to fully succeed, i.e., the collateral damage would be that no legitimate traffic can reach the server.

It's also possible that the SYN flood traffic would have fields in its packet headers *other* than the source IP address that do not appear in legitimate traffic to the site. If so (and this in fact occurs in practice), then the target can set up their firewall to filter on those header fields, rather than the source IP addresses.

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

Solution: An attacker could send a large number of bogus spam reports to GreenMail, falsely indicating some victim site V has been sending spam. GreenMail's servers will then visit V to lodge complaints, overwhelming V in the process if the volume of visits is high enough.

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

Solution: V could refuse to accept incoming connections from GreenMail in order to avoid the load from GreenMail's servers registering complaints.

A final note: do not hesitate to ask for help! Our office hours exist to help you. Please visit us if you have any questions or doubts about the material.