COMP 8670 - Take Home Exam

Matthew Belanger

March 31, 2025

1 Problem 1 - Printer Attack

1.1 Can Attila arrange to learn the contents of Vicky's document without physically accessing any of the printers?

Yes Attila can learn the contents of Vicky's documents using a man in the middle attack (assuming they are on the same network). This is possible due to two features of the protocol.

1. Attila can learn the IP addresses of all the printers on the network and forward any packets recieved to the victim's requested printer. This is possible due to the **Printer Discovery packets** and the **Printer Announcement packets**.

2. Attila can recieve Vicky's print requests due to how the non-priter machines handle **Printer Announcement packets**. Since **Printer Discovery packets** are broadcasted to the entire network, Attila will know when Vicky is looking for printers. Attila knows all the printers on the network and is able to wait a short while so the Vicky will recieve the legitiment printer data and then Attila can spoof additional **Printer Discovery packets** by claiming to be a printer with the same name as the actual printer, and when Vicky receives this new data her machine will override the entry due to the protocol specification.

Due to these two possibillities, Attila can itercept Vicky's packets by pretending to be the printer and forward them to the printer and Vicky will not know the difference but Attila can save a copy of the sensitive data. In short, Attila learns all the names of the printers on the network, waits for discovery requests and then retransmits **Printer Announcement packets** with her IP addresses but the requested printers names so that the host machines log her IP as each printer on the network.

1.2 Describe two distinct Denial-of-Service (DoS) attacks that Attila could execute against the Printer Discovery Protocol.

Attila can,

1. send high volumes of **Printer Discovery packets**, so that the printers will be unable to service legitiment discovery requests due to being overloaded with Attila's bogus requests.

2. send high volumes of **Printer Announcement packets**, so that the client machines will unable to register legitiment printers requests due to being overloaded with Attila's bogus announcements.

1.3 Can Attila modify what is printed on the printer?

Yes Attila can. See my response in section 1.1. Note that in the method I described, the original document Vicky sends will never reach the destination printer, it is a copy that Attila forwards than reaches the printer. Attila can very easily swap out the document instead of forwarding a copy.

2 Problem 2 - Hilltop Academy IT Security

2.1 What would be the source IP address and the MAC address in the ICMP Redirect message sent by Leo's Laptop to the Teacher's Workstation?

2.2 After receiving the ICMP Redirect message, what changes occur in the routing table of the Teacher's Workstation?

2.3 Indicate the new route (including the next-hop IP address) that the Teacher's Workstation will use to send packets intended for the Internal Web Service Server after the ICMP Redirect attack is successful.

2.4 What should be the content of the ICMP Redirect message to make sure the Teacher's Workstation routes the traffic as intended by Leo?

2.5 If Eva notices unusual network activity and investigates the traffic coming to and from the Teacher's Workstation, identify the signs that would indicate an ICMP Redirect attack is taking place.

3 Problem 3 - Python From Section 2

See Python Implementation.

4 Problem 4 - Link-State and Distance-Vector Routing

4.1 Assume we are using Link-State routing for the network in figure "Network Topology A". Is it possible to for oscillation problem to occur.

4.2 Assume we are using Distance-Vector routing for the network in figure "Net- work Topology A". Is it possible to for a routing loop problem to occur.

4.3 Assume we are using Link-State routing for the network in figure "Network Topology B". Is it possible to for oscillation problem to occur.

4.4 Assume we are using Distance-Vector routing for the network in figure "Net- work Topology B".

5 Problem 5 - Congestion Control

5.1 Show for sending 15 different packets (duplicate packets do not count), how the window size will change, and the packets sent in each window.

Window Size	Packets Sent
-	-
-	-
-	-
-	-
-	-
-	-
-	-
-	-
-	-
-	-
-	-
-	-
-	-
-	-
-	-

Table 1: Window Size vs. Packets Sent

5.2 **Assume that we set the initial estimated RTT to 20 ms and we measured the actual RTT for packets 2, 5, 9, 13 as shown in table 2. Calculate the estimated RTT for packet number 14.**

Packet #	2	5	9	13
RTT (ms)	21	19	24	22

Table 2: Round-Trip Time (RTT) for Different Packets

6 Problem 6 - TimeSync Protocol

6.1 **Define the message format for both time synchronization requests and responses in your protocol.**

6.2 **Sketch a timeline for the operation of your protocol in case of a simple time synchronization request and response with no error, and in case there is one error (e.g. time drift greater than 30 seconds)**

7 Problem 7 - RDT Protocol

7.1 **Draw a time chart for the packets between A and B, showing the number of data and acknowledgment packets exchanged between A and B. When B received the message "CAT" correctly, there was no crash or time failure.**

7.2 **Draw a time chart for the packets between A and B, showing the number of data and acknowledgment packets between A and B. When B only receives the message "CA" and not "CAT" due to time failure. A and B will fail to detect that the message was sent incorrectly and terminate the connection.**

7.3 **Draw a time chart for the packets between A and B, showing the number of data and acknowledgment packets between A and B. B only receives the message "CATC" and not "CAT" due to time failure. A and B will fail to detect that the message was sent incorrectly and terminate the connection.**