COMP 8670 - Take Home Exam

Matthew Belanger

April 4, 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 legitimate 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 legitimate 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 legitimate 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

For reference, the following IP addresses are assigned based on the Hilltop Academy scenario:

Legitimate Gateway : `192.168.50.1`
Attacker (Leo) : `192.168.50.30`
Victim (Teacher) : `192.168.50.40`
Target (Internal Service) : `192.168.70.10`

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?

Since Leo is trying to spoof the router, the IP address would need to be the gateways router so that the teacher's machine will believe the router is sending the information, but since Leo's the machine is physically sending the packet to the teacher, it would need to be Leo's MAC address because ICMP is above the DataLink layer.

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

The teacher will have their table updated such that it will believe that the most efficient route to get to the target machine will be to go to the attackers machine first.

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.

The route will begin at the source, the Teachers IP (192.168.50.40), then the Attackers IP (next hop, 192.168.50.30), then it will be the route to get from the attacker to the legitimate gateway and finally Internal Web Service Server 192.168.70.10.

$$\text{Teacher} \rightarrow \text{Leo} \rightarrow \text{Gateway} \rightarrow \text{Target}$$

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?

Leo wants to just inspect the data and pass it along because Leo is not malicious. The outer message should be an IP message between him and the Teacher, with a redirect ICMP packet at the next layer that claims Leo is the optimal next jump. The next layer should be another IP message with the original information which is between the Teacher and the Target. See the Python implementation.

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.

Eva has not been redirected so she can ping the Teacher the "legitimate" way. Since she is on the same subnet as the Teacher she can monitor the route and see that the optimaml route to the target is:

$$\text{Her} \rightarrow \text{Gateway} \rightarrow \text{Target}$$

Leo's IP does not exist in the route, but the Teachers packet goes through Leo. This is evidence that some tampering has occured.

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.

Any message that will reach router C or E must pass through A. So we only need to consider the sub network formed by A B D.

In the A-B-D triangle network. Initially, router A routes traffic to D via B because the path through L4 and L5 (44) is cheaper than the direct L1 path (50). However, if L5 cost increases to 20, the optimal path switches to the direct L1 route (50) instead of L4 and L5 (53). The oscillation problem arises when these link cost changes occur more rapidly than link-state advertisements can propagate through the network, causing routers to make forwarding decisions based on inconsistent network views. Therefore the loop.

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.

Any message that will reach router C or E must pass through A. So we only need to consider the sub network formed by A B D. A loop can occur because initially, each node computes shortest paths:

- A reaches D via B, cost = 33(L4) + 11(L5) = 44
- B reaches D directly, cost = 11
- D reaches A directly, cost = 50

Now, suppose the L5 link fails. B no longer has a direct route to D but hasn't yet updated its table. A still believes D is reachable via B with cost 44. B queries A and receives this route. Since 44 (A's cost to D) + 33 (L4 link) = 77, B updates its table to route to D via A at cost 77. Then, A queries B and learns of B's new route (via A at 77), so A updates its own route to D as 33 (L4) + 77 = 110 via B. This back-and-forth continues, with each node incrementally increasing the path cost and pointing to the other as the next hop to D, forming a routing loop between A and B despite the triangular structure.

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.

No, in a path graph there is only one route to get to any node. The shortest path algorithm will find this path.

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

No, in a path graph there is only one route to get to any node. The shortest path algorithm will find this path.

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
1	1
2	2, 3
4	4, 5, 6, 7,
2	5, 8
4	9, 10, 11, 12
2	9, 13
4	14, 15

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

Given that,

$$\text{EstimatedRTT}_n = (1 - \alpha) \times \text{EstimatedRTT}_{n-1} + \alpha \times \text{SampleRTT}_n$$

Setting $\alpha = 0.125$

$$\begin{aligned}
\text{EstimatedRTT}_2 &= (1 - 0.125) \times 20 + 0.125 \times 21 = 20.125 \\
\text{EstimatedRTT}_5 &= (1 - 0.125) \times 20.125 + 0.125 \times 19 = 19.984 \\
\text{EstimatedRTT}_9 &= (1 - 0.125) \times 19.984 + 0.125 \times 24 = 20.483 \\
\text{EstimatedRTT}_{13} &= (1 - 0.125) \times 20.483 + 0.125 \times 22 = 20.676 \\
\hline
\text{EstimatedRTT}_{14} &= (1 - 0.125) \times \text{EstimatedRTT}_{13} + 0.125 \times 22 = 20.841\text{ms}
\end{aligned}$$

I use the same sample value because a new sample had not been measured so I assume the previous one is still valid.

6 Problem 6 - TimeSync Protocol

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

Before presenting a message format I want to present some considerations. A naive solution to this problem would be to create a server that broadcasts the time at regular intervals and if the client sees that it has drifted then it can correct itself.

Problems,

1. Does not take into account message transfer delays.

2. How does client respond when it does not receive messages?

3. What if client receives updates out of order? Which should it trust?

It is better if the client requests the time and provides an incrementing ID of the request.
In this way,

1. Still does not take into account message transfer delays.

2. The client can re transmit the request if it does not hear anything back

3. Reacts to the most recent ID

However, we are still unsure if the message has been significantly delayed. The time server can help us with this. Assuming the time server has accurate knowledge of the time and that the client can accurately measure time durations, we can craft a response message that includes the accurate time along with the clients message ID so the client knows if the response is fresh. The client can retransmit the request if it does not hear back in 30 seconds with the same ID, thus handling time delays and packet loss. This ID is also to help the client ignore old request responses. Server should always respond to requests (Client

is master, server is slave) so it does not need to requests because it will be echod bach in the response.
The request would be (as json),

```
"request": {
        "id": "uint"
}

"response": {
        "id": "uint",
        "current_time": "hh:mm:ss"
}
```

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)

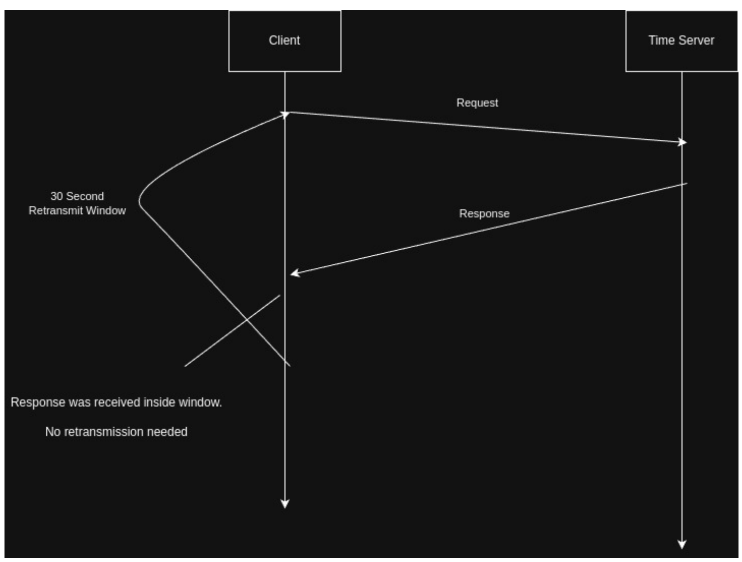

Figure 1: No Errors Diagram

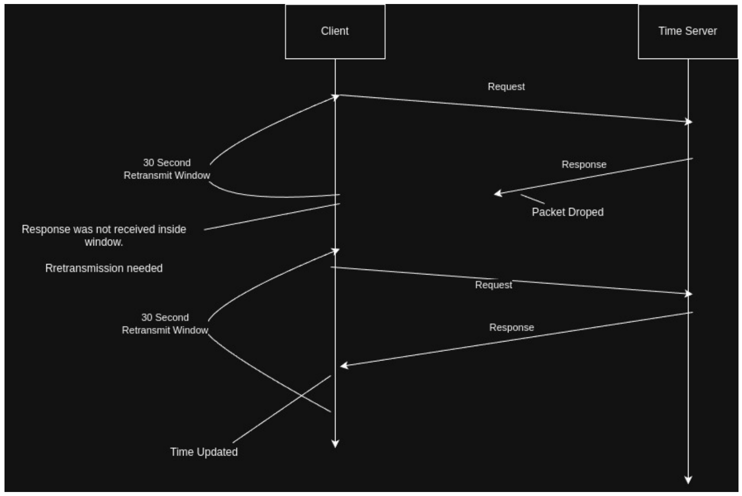

Figure 2: One Error Diagram

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.

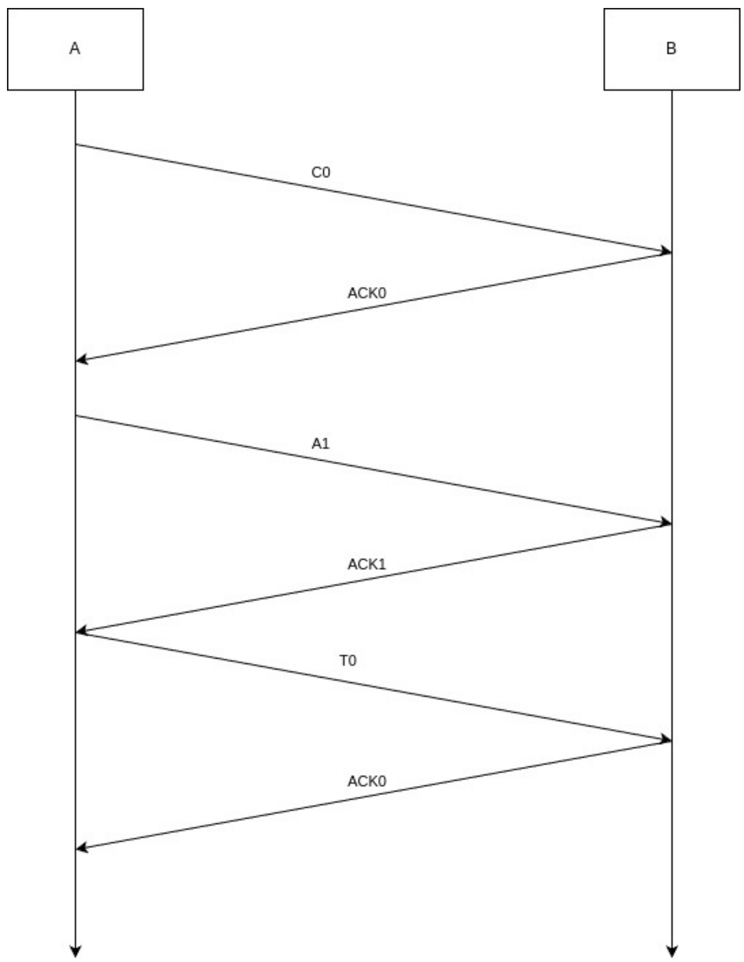

Figure 3: CAT sent and Recieved

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.

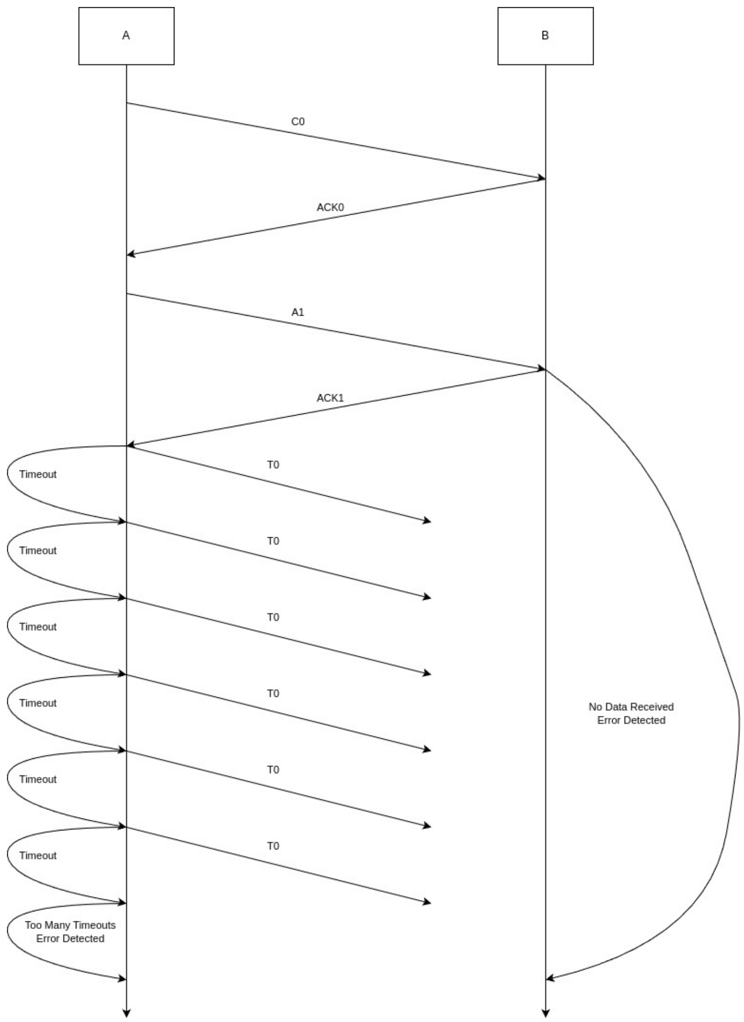

Figure 4: CAT sent and CA Recieved

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.

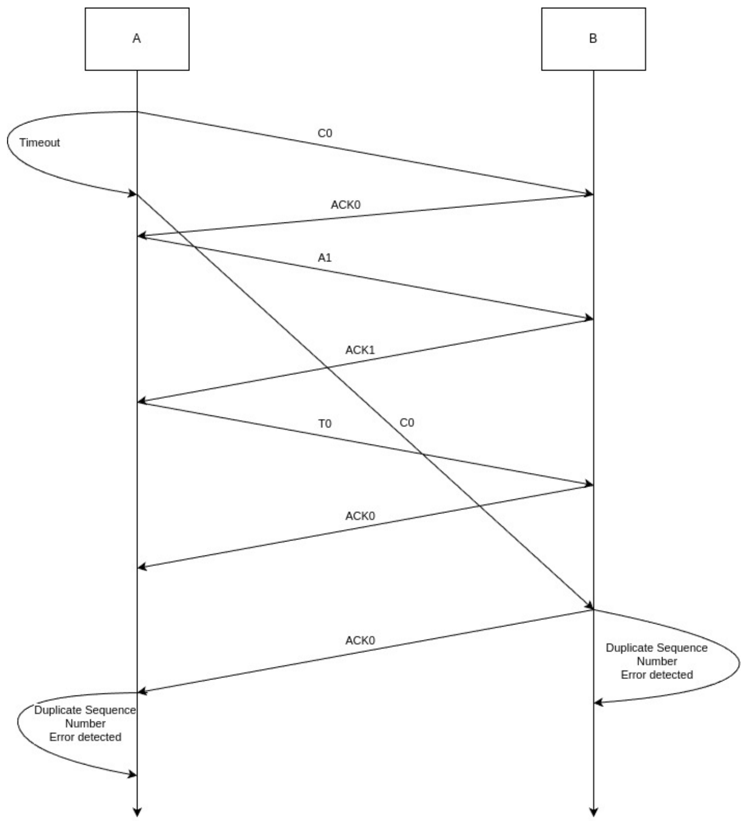

Figure 5: CAT sent and CATC Recieved