

Lesson 1

Man-In-the-Middle Simulation

Goal: This lesson, played as a game, explores the idea of what a “man in the middle” can do in a Wi-Fi network.

Setup: As there are two things (i.e., request forging and response forging) that a man in the middle can do, there will be two versions of this game. Before you start, form groups of 3 or 4 (preferably 4) and assign each member a role.

Team Role:	Group Member Name:
Sender (group member 1): creates a message to be sent to the validator. In the attack, you are the victim of the keylogging attack.	
Interceptor (man in the middle) (group member 2): intercepts the message from the receiver and can read or change the original message sent. In the attack, you are considered the attacker.	
Validator (group member 3): receives the message from the interceptor and ensures it is a valid message before sending it to the receiver. In the attack, you are the local Wi-Fi.	
Receiver (group member 4): receives the message from the validator and responds with an answer before passing it back to the validator. In the attack, you are the online server that the sender is trying to reach.	

Things to consider:

1. When writing your question and answer, write lightly with a pencil so the interceptor can modify the message without the recipient seeing pencil marks that couldn't be fully erased.
2. As all these interactions are invisible to the other parties, you should not watch what the other parties are writing, especially not what the "man in the middle" is writing as in a real attack you don't know that they are there.
3. Determine a prompt that the questions and answers will fall under. Examples: "What is your favorite type of food?", "Who is your best friend?", etc.

Steps:

1. The sender (group member 1) should write (lightly) a question that fits with the prompt and then send the message to the interceptor (member 2).
2. The interceptor (member 2) should then receive the message from the sender and make changes to the original message if they wish. After they discreetly have made their changes, they should then pass the message on to the validator (member 3).
3. The validator (member 3) should receive the message and ensure that it is still a valid message and does not appear to be tampered with too much. They will then send this message to the receiver (member 4).
4. The receiver (member 4) then opens the message sent to them and responds (lightly) on the back of the paper with their answer. They then pass this response on to the validator (member 3).
5. The validator (member 3) receives this response and again checks to make sure that it is a valid response and passes this response back to the interceptor (member 2).
6. The interceptor (member 2) receives the response and again can discreetly make changes to the response before passing the response on to the original sender (member 1).
7. The original sender (member 1) then opens the response and tries to understand the response.

Post Activity Discussion:

1. Did the response make sense in terms of the question that was originally asked?
2. Validator: ask the sender (member 1) and the receiver (member 2) what messages they sent and received.
3. Without knowing that changes were made by the interceptor, would you have been able to tell that the response or question had been tampered with?
4. What are the key takeaways from this activity?