Man-It-The-Middle Attack

Hm… We still have a problem! And it is called Man-In-The-Middle. Obviously, we forgot about it.

So what that means? Say hello to our friends Alice and Bob. As you can remember they fooled Eve, so now they are happy. Not so fast. Do you think they suffered enough? No. That is the real world. Here goes Mallory. She is our man-in-the-middle. And that means she can read all the messages Alice and Bob send. Bad for them, but let`s find out how it works.

Alice and Bob want to talk again. As we remember they use encryption and Diffie-Hellman key-exchange algorithm, we talked earlier. The point is we can`t identify is Alice – real Alice, and not Mallory. The same is thing for Bob. Here goes Mallory, again. Let`s trace them step-by-step:

1. Alice sends a message to Bob, which is intercepted by Mallory
2. Mallory relays this message to Bob; Bob cannot tell it is not really from Alice
3. Bob responds with his encryption key
4. Mallory replaces Bob's key with her own, and relays this to Alice, claiming that it is Bob's key
5. Alice encrypts a message with what she believes to be Bob's key, thinking that only Bob can read it
6. However, because it was actually encrypted with Mallory's key, Mallory can decrypt it, read it, modify it (if desired), re-encrypt with Bob's key, and forward it to Bob
7. Bob thinks that this message is a secure communication from Alice

And as you see everything is bad. We can help them. And we will. Let`s think how. The entry point for Mallory is not intercepting of message. It is the encryption keys exchange. Public keys we talked earlier. The easiest way to help them is to member keys. First time Alice and Bob receive public key they member it. And next time they messaging there is no need to send it again. So nobody can say he is Bob, because Alice can identify Bob now. That is our solution – easy but works.

And now, when I said the problem is solved. Again... Let`s check your memory:

* What is our new problem?
* What is Mallory`s entry point?
* How Alice and Bob deal with is?

Words:

Man-In-The-Middle – Человек посередине

Encryption – шифрование

To identify – идентифицировать

To intercept – вмешиваться/перехватывать

Step-by-step – шаг-за-шагом

Entry point – точка входа