Network-Role-Play

> [!toc] Table of Contents

This game aims to illustrate the process, but not the functionality, of network communication using the example of emails without encryption, with transport encryption, and with end-to-end encryption. It is not really a game that is meant to be fun, but rather a means of explaining the topic without having to use a network diagram, thus making it more accessible to less technical people.

Roles

- 2x servers (systemli.org & gmail.com)
- 2x communication parties (Alice & Bob)
- 1x (or more) police officers (Eve)
- 3x "The Internet" (optional)

Materials

- 1x sheet of paper for text
- 1x sheet of paper with email metadata
- 3x sheets of paper with IP metadata for the routes between the nodes
- 2x signs with the names of the servers
- 2x signs with the email and IP addresses of the communication parties
- 1x small box that can be locked with a padlock (large enough to hold the sheet of paper with the text)
- 3x large boxes with lids (large enough to hold the other box)
- 2x padlocks
- 3x chairs

Ideally, the sheets should be laminated and written on with whiteboard markers. This way, they can be easily reused.

Procedure

In preparation, the Internet metadata information is stuck on each of the large boxes.

Then the roles are assigned. The role of the police should preferably be played by someone without much technical knowledge, so that creativity is required for the attacks. The rest of the people watch.

The two servers and two communication parties stand in a square. The servers and communication parties are given the signs with their information.

One chair is placed between each of the four people, on which one person playing the internet sits. They are also given the box with the corresponding internet metadata.

Alice writes a message to Bob on the sheet for the text and fills in the metadata that is not already filled in on the sheet with the metadata.

Now the various scenarios are played out. Each scenario is shown once without MITM and once with MITM (in our case by the police). The role of the police is to come up with their own ideas on how to attack the scenario. The only exceptions are attacks on Alice and Bob, which are not the aim of this game. Furthermore, the legality of the attacks or whether the parties would hand over the data to the authorities is not discussed; all technically possible attacks can be considered. The police can only attack the internet and the servers.

If the police cannot think of any way to attack, the audience can help. If they also have no ideas, the moderator can help.

The audience should then explain what happened, whether the attack worked, and what data the police obtained.

Unencrypted

Anna gives the sheets with the text and the email metadata to the Internet, which gives them to the first server, which sends them back to the Internet, which sends them to the second server, which sends them back to the Internet, which finally sends them to Bob. At each node, the sheets are placed in the box with the corresponding IP metadata.

Unencrypted - MITM

Possible targets of attack are:

- The internet
- The servers

All data can be intercepted at both points.

Transport encrypted

This time, the boxes are “locked” with lids. Although these boxes are not locked in the game, it is pointed out that they should still be considered secure. However, they only provide protection during transport; the nodes must be able to open the corresponding boxes.

Otherwise, it works the same as in the unencrypted scenario. It is important to ensure that both sheets are taken out of the box at each node and then placed in the appropriate other box. This is necessary because the servers need the metadata to know where to forward the mail.

Transport encrypted - MITM

Possible targets for attack are:

- The servers

All data can be intercepted there.

End-to-end encryption

First, it is explained that end-to-end encryption involves a public key and a private key. We represent the public key as a padlock and the private key as the key for the lock. It is briefly pointed out that this public key must be exchanged in such a way that it is certain that it belongs to the person. For this scenario, we do this by having Bob go to Alice in person and give her the padlock.

Alice puts the piece of paper with the text in the small box, locks it with the padlock, and puts this box together with the sheet containing the metadata in the large box. She then sends it to the Internet. After that, the process is the same as before: the large box is unpacked and repacked at each node, and the small box is finally opened at Bob's end.

End-to-end encryption - MITM

Possible targets for attack are:

- The servers

Only the metadata can be accessed there.

End-to-end encryption with TOFU

This time, the public key is exchanged as usual by email without being verified.

1. Alice writes to Bob, “Send me the key.”
2. Bob sends the key.
3. Alice writes end-to-end encrypted as above.

End-to-end encryption with TOFU - MITM

Possible targets of attack are:

- The servers

All data can be intercepted there.

The attack proceeds as follows:

1. Alice writes to Bob, “Send me the key.”
2. Bob sends Alice the key.
3. The police intercept the key and replace it with their own.
4. Alice encrypts the message with the police key.
5. The police intercept the message and read it.
6. The police re-encrypt the message with Bob's actual key and send it on.

Neither Alice nor Bob are aware of the attack, but the police can read everything. Because the key was replaced by the police, a second padlock is required here.

Version #2
Erstellt: 2026-02-15 16:16:46 UTC von ESC-IT Migration Bot
Zuletzt aktualisiert: 2026-03-18 13:28:30 UTC von ESC-IT Migration Bot