replay attack defense (WEP)

Advanced Computer Security (CS-558-01)

ADITYA NIKHIL – A20493729
KULADEEP MANTRI – A20498452

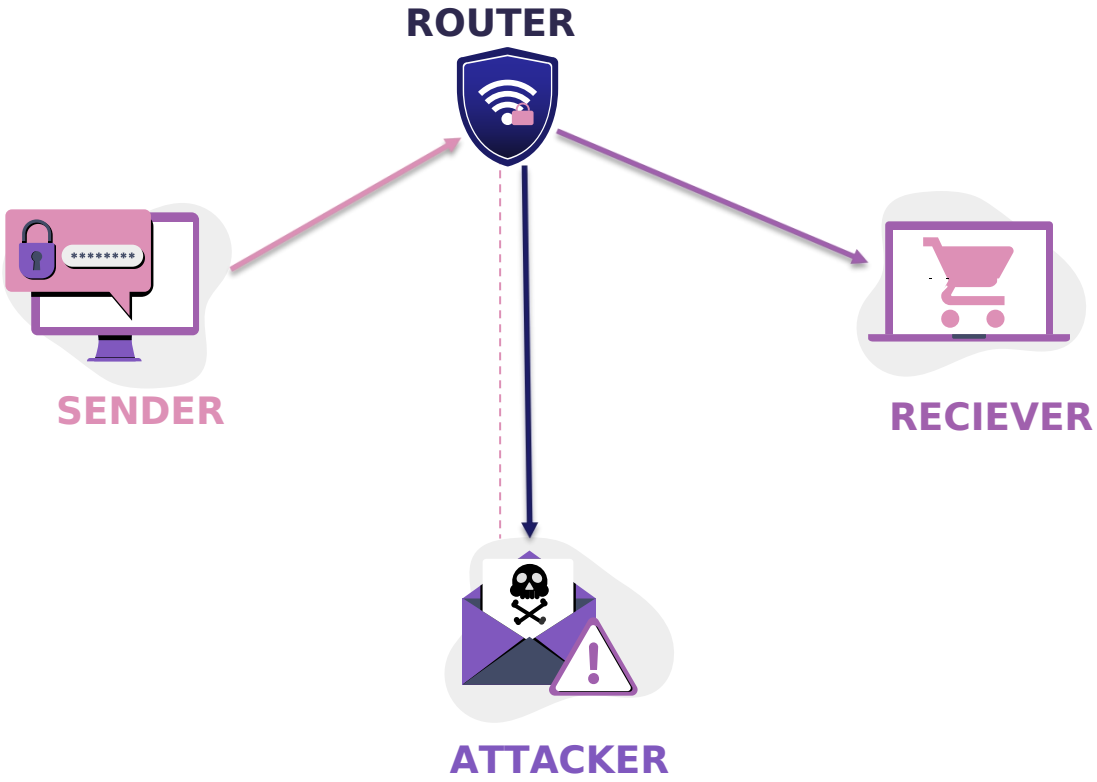
Abstract

In this project, we will look at the issue of intrusion detection in wireless networks. There are two types of defenses we will elaborate in this project :

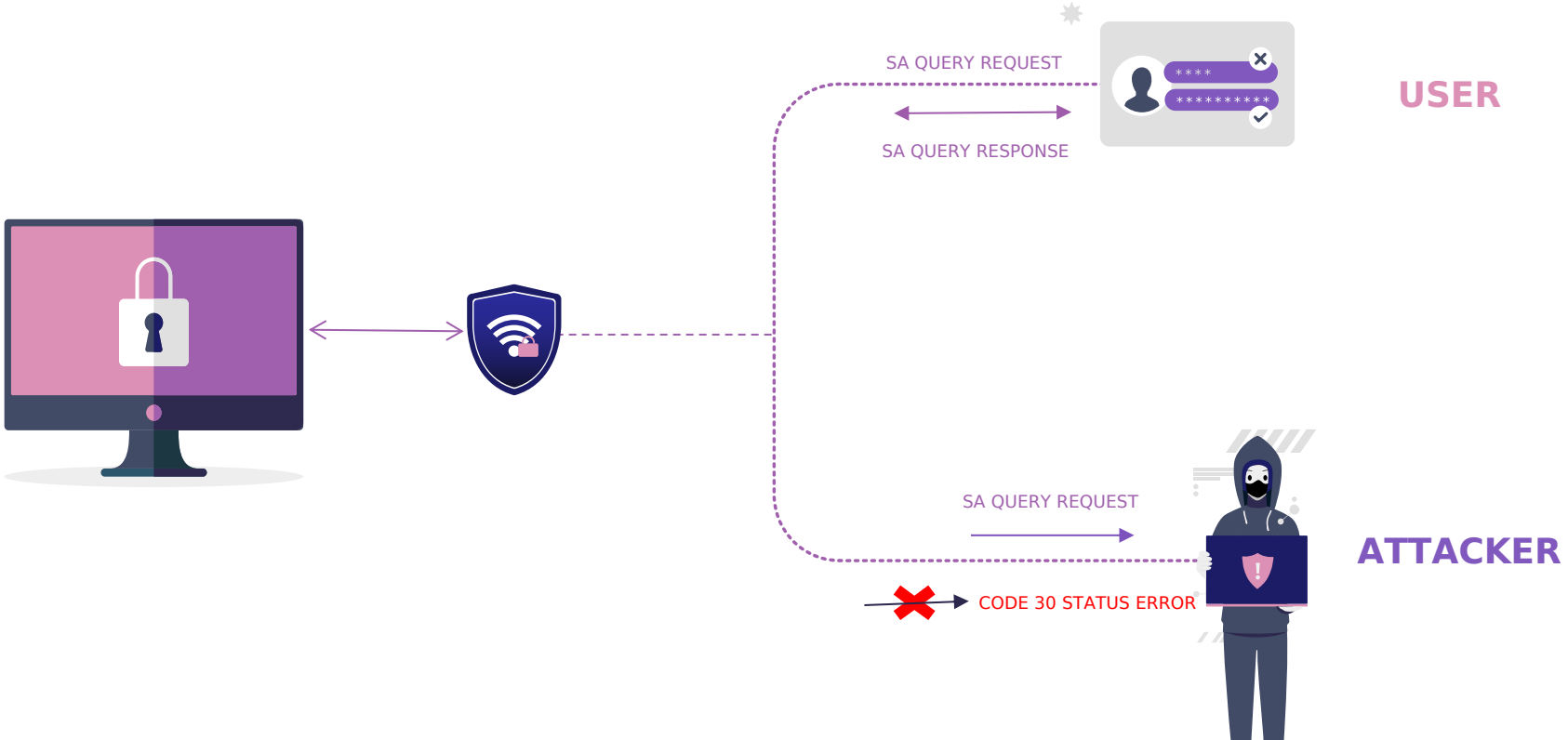
1. The 802.11w standard introduces a cryptographic message integrity check to the Wi-Fi protocol to validate the authenticity of wireless control frames, which will allow you to validate the frames from your infrastructure using an external cryptographic library and identify rogue device imposing your network.

2. Defense can also take a proactive approach and actively inject frames to prevent the rogue network from ensnaring your clients.

ARP–request replay attack



802.11W STANDARD (1ST DEFENSE)



802.11W Working process (1st DEFENSE)

SA QUERY REQUEST

A Request is sent to the client

Client must respond within a given time period

SA QUERY RESPONSE

CODE 30 ERROR

If the response is not reported on time code 30 error will occur

CONNECTED

PRO–Active Approach (2nd DEFENSE)

- We take a proactive approach and actively inject frames to prevent the rogue network from ensnaring the clients. While there are possibilities for actively defending your network and prevent a network attack from succeeding.

- Not all strategies that are technically possible are legally allowed. In the last part, you will further investigate this tension and develop a mitigation plan compliant with the legislation in your area.