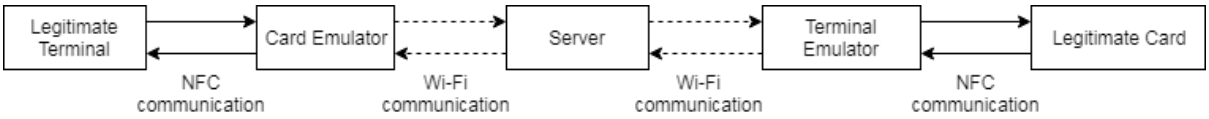
A full relay attack using this method involves 5 entities, one of which is the legitimate card (with contactless payment capabilities), and another the legitimate terminal. In addition to these, there are the terminal emulator, the card emulator and the server which facilitates communication between them. The terminal emulator and the card emulator are both apps that are run on smartphones that have NFC capabilities. The Server is a Python script that is run on some machine. The card emulator, terminal emulator and server communicate over Wi-Fi.



Setup:

- Card Emulator
  Install card emulator apk on a smartphone, ensure that the setting to allow installations from unknown sources is enabled. The apk is signed with a debug key, with an expiry date in 30 years' time.
  - Ensure that the NFC is turned on, on the phone. The phone must be connected to a Wi-Fi network.
  - To enable the app to handle payment commands, go into the Tap and Pay settings of the phone and choose the default payment app as the card emulator. This may not list the name of the app, in which case it will likely be the blank option. Without doing this, by default-app, i.e., Google Pay, will open when the phone receives a payment APDU-command
- Server
  There are a number of scripts in the server file, some of which are utility classes.
  - Terminal.py and Card.py are used to debug the terminal emulator and card emulator, respectively. They require a single parameter (the phone's IP address, which is displayed in the app).
  - Relay.py is the script that facilitates the actual relay and to run it requires two parameters, the IP addresses of the terminal emulator and card emulator. I.e, to launch the relay script with Python 3.7 installed, run a command line in the location of the server files and run the following command:
    python3 relay.py 1.255.255.254 1.255.255.255,
    where the two IP addresses represent the terminal emulator and card emulator, respectively.
  - Make sure that Python 3.7 or later is installed.
  - The device running the terminal script must be connected to the same Wi-Fi network as the card emulator.
- Terminal Emulator
  Install terminal emulator apk on a smartphone in a similar manner to the card emulator. The terminal emulator does not require default payment settings to be changed.
  - As with the Card Emulator, ensure that NFC is activated.
  - The phone running the Terminal Emulator must be connected to the same Wi-Fi network as the Server and the Card Emulator.

Running a relay attack:

To perform an attack, once all the components are set up (assuming the server script is running), first bring a legitimate card within the field of the Terminal Emulator. The Terminal

Emulator should make audio cues that indicate whether it is connected. Then, bring the Card Emulator within range of the legitimate terminal. The relay script waits for the Card Emulator to receive a command, and once the server receives a message from the Card Emulator, it will print out this message. When the Server receives a reply from the Terminal Emulator, it and an explanation of it will be printed also.