Man-in-the-Middle Demo

About

This is a demo of a Man-in-the-Middle attack, as shown in lecture. It is not a graded lab, and is only meant to be used as a fun exercise to get you familiar with the concept of these kinds of attacks.

Keep in mind, this is for learning purposes only: using this maliciously is against the Student Code of Conduct and the Computer Fraud and Abuse Act.

The example code here will attack any webpage by causing it to be flipped upside-down, and by printing out any message to a website which contains the text "password".

How to run

Note: I've only tested this using Python 3.10 on Windows 11, and Firefox. I find Firefox much easier to use for this, and the directions below only apply to that browser. You may have to take different steps if you are using a different browser.

Part 1: Running the Man-in-the-Middle attack code:

1. Install Python from https://www.python.org/, if you haven't already.
2. Open a terminal in the same directory as mitm.py.
3. Install the required library with `python -m pip install mitmproxy`
4. Run the program with `mitmproxy -s mitm.py`
5. The mitmproxy library should open a command line tool. Press `shift + E` to see the event log.
   Note: On my machine, the CLI seems to get stuck and stop receiving input sometimes. I don't know what causes this or how to fix it, other than restarting the program.

Part 2: Getting your browser to send traffic to the attacker

You should now have the MitM program set up, but your browser is not sending messages through it. It is not, in fact, in the middle of anything. In a real attack scenario, this code would run on a router that is actually between you and the target website. For this demo however, we need to force the local browser to send traffic through it. How you do this depends on the browser and OS: I've listed the steps I use for Firefox below, but here's an article that should help for other systems: https://www.avast.com/c-how-to-set-up-a-proxy. The proxy server you want is "localhost" with a port of "8080" (the default values used by mitmproxy). *Note: this will redirect all of your network traffic, so be sure to undo any changes after the demo is over! You may be unable to access the internet if you close the mitmproxy Python script without reverting your proxy settings.*

Here are the steps I used for Firefox:

1. Go to about:preferences
2. Scroll down to "Network Settings" and click "Settings"

3. Choose "Manual proxy configuration" and set HTTP to "localhost" with a port of "8080". Select "Also use this proxy for HTTPs".

After configuring the proxy, you should be performing a Man-in-the-Middle attack on any insecure website you visit. Try going to http://neverssl.com, which does not provide any kind of safeguards against this kind of attack. If everything is working correctly, it should appear upside-down!

Part 3: Getting around safeguards

Most websites implement protections against this kind of attack. These websites will send you an error message, warning you of a security risk. To view the page anyway, select "Advanced", then "Accept the Risk and Continue" (this process might be slightly different on non-Firefox browsers). Some websites go a step further and prevent you from viewing the page at all- you may have to clear all site data by clicking the lock icon in the URL bar and selecting "Clear cookies and site data". *Note: This will clear any saved passwords or logins you have on the site!*

At this point, you should be able to perform a Man-in-the-Middle attack on yourself! You can play around with the Python code to do different things: the example code shows you how to read and replace text. The `flow.request.content` variable stores messages from you to the server, while `flow.response.content` stores messages from the server to you.