# CS628A: Computer Systems Security
# Assignment 3

$8^{th}$ April, 2019

Credits: This assignment and the accompanying material is based on content created by the Arvind Narayanan and his group at Princeton University.

## Getting Started

In this assignment you will learn the basics of network packet analysis. As data streams flow across the network, packet sniffers/analysers captures such traffic and logs it. We have provided you with one such packet capture file assn3.pcap.

You are free to choose any tool that helps you in analysing packet captures including tcpdump, tshark, or wireshark. Install tool of your choice, familiarize yourself with it, and analyze assn3.pcap to answer the following questions.

## Packet Capture Analysis

1. Multiple devices are connected to the local network. What are their MAC and IP addresses ? Who manufactured these devices?
2. What type of network does this appear to be (e.g., a large corporation, an ISP backbone, etc.)? Point to evidence from the trace that supports this.
3. One of the clients connects to an FTP server during the trace.
   a. What is the DNS hostname of the server it connects to?
   b. Is the connection using Active or Passive FTP?
   c. Based on the packet capture, what is one major vulnerability of the FTP protocol?
   d. Name at least two network protocols that can be used in place of FTP to provide secure file transfer.
4. The trace shows that at least one of the clients makes HTTPS connections to sites other than Facebook. Pick one of these connections and answer the following:
   a. What is the domain name of the site the client is connecting to?
   b. Is there any way the HTTPS server can protect against the leak of information in (i.)?
   c. During the TLS handshake, the client provides a list of supported cipher suites. List the first three cipher suites and name the crypto algorithms used in each.

d. Are any of these cipher suites worrisome from a security or privacy perspective? Why?

e. What cipher suite does the server choose for the connection?

5. One of the clients makes a number of requests to Facebook.

   a. Even though logins are processed over HTTPS, what is insecure about the way the browser is authenticated to Facebook?

   b. How would this let an attacker impersonate the user on Facebook?

   c. How can users protect themselves against this type of attack?

   d. What did the user do while on the Facebook site?

# Submission

Fill in *answer.txt* with the answers. The questions are of objective nature, so we are **not** expecting long answers. The moodle submission link will be active soon.