Activity: Human Network Map

In this activity, participants are assigned roles as pieces of internet infrastructure, and they then work together to pass messages from one person to another. This activity explains how encrypted messaging increases your security, and the infrastructure that is used every time we send a text message. The activity can also be adapted to explain VPNs and Tor as well.

Adapted from Pitching Packets game. LevelUP has a similar exercise, which we discovered after putting this together, along with a fantastic digital security training curriculum.

Note: We haven't yet tried to do this activity virtually - let us know if you figure out a method to make it work on Zoom!

Materials:

- Cardstock
- Printer or marker
- Envelopes

This activity works best with eight to ten participants. You'll need a minimum of seven participants.

Set aside about 45 minutes to complete the activity and answer questions.

Preparation:

1. Print or write the following labels on whole pieces of cardstock:
    a. Alice's Phone
    b. Bob's Phone
    c. Cell Tower (2)
    d. SMS Center
    e. Signal Server
    f. IMSI Catcher/Stingray

2. On smaller pieces of cardstock that will fit in your envelopes, write the following:
    a. A subpoena from the FBI (2)
        i. “A very official FBI subpoena for all data related to Bob’s phone”
    b. First text message (2) - choose content that will be amusing to your participants, if possible! On the second piece of cardstock with the same message, write “for retention by SMSC”. On both pieces of cardstock, above the message, write: “To: Bob, From: Alice”.
    c. A reply to that text message - again, feel free to write something amusing. Humor helps these concepts stick!

3. On the envelopes, write:
    a. To: Signal From: Bob’s Phone
    b. To: Alice’s Phone From: Signal

Activity:

Step 1 (5 minutes): Assign everyone a role by handing out the large pieces of cardstock. It’s okay if not everyone has a role; some folks can be observers and still participate. People can participate in this activity sitting down, or standing up and moving around.

Accessibility note: If you are going to be standing up and moving around, be sure to offer chairs to participants who may have mobility restrictions. Don’t rely on visual cues to offer chairs - offer them to everyone!

Step 2 (5 minutes): Arrange participants in order of the roles assigned. They should be arranged as follows:

1. Alice’s Phone
2. Cell Tower
3. SMS Center
4. Cell Tower
5. Bob’s Phone

Have the person with the “Signal Server” role stand a few feet away from the person with the SMS Center role.
Have the person with the IMSI Catcher/Stingray role stand off to the side; they will be mobile!
Give two people the FBI subpoenas.

Step 3 (5-10 minutes): Alice sends a text to Bob!

a. Let everyone know that if they receive the message, they should read it aloud.

b. Give Alice the first text message, written on a piece of cardstock (this message is a bundle of two messages). Explain that she is going to send this message to Bob via regular SMS text message.
c. Alice reads the message aloud.
d. Alice passes the message along to the cell tower, who also reads it aloud.
e. The cell tower passes the message to the SMS center, who reads it aloud and keeps a copy.
f. The SMS center passes the message to the other cell tower, who also reads it aloud.
g. Oh no! An IMSI catcher is driving by. Explain that an IMSI catcher is a fake cell phone tower that pretends to be a real cell phone tower. IMSI catchers are often used by state actors to surveil communications in a certain area, such as near a protest. Instruct the IMSI Catcher character to drive by the cell phone tower. The cell phone tower passes the message to the IMSI catcher.
h. The IMSI catcher reads the message.
i. Finally, the IMSI catcher passes the message to Bob, who reads it aloud. It has reached its destination!

Step 4 (5-10 minutes): Bob sends a message back to Alice! Explain that Bob is worried about security, and so he chooses to send his message using an end-to-end encrypted messaging application called Signal. Alice also has Signal downloaded on her phone. End-to-end encryption means that only Bob and Alice can unlock the message. To symbolize end-to-end encryption, we'll put Bob's message in one envelope (the one labeled from: Bob to: Signal) and then put that envelope inside the other envelope (the one labeled from: Signal to: Alice). Explain that envelopes can only be opened by those who they are addressed to - this corresponds to encryption, which can only be decrypted by those who have the encryption key.

a. Bob passes the message (in its envelopes) to…
b. Oh no! The IMSI catcher is still in the area. Instruct the IMSI catcher to "drive by" Bob. The IMSI catcher takes the envelope and reads it aloud, and then passes it to the cell tower.
c. The cell tower reads the envelope.
d. The IMSI catcher passes it to the Signal server.
e. The Signal server reads the envelope, and since it's addressed to them, opens the envelope. They read the envelope inside and pass it along.
f. The Signal server passes the envelope to the cell tower.
g. The cell tower reads the envelope, and passes it to Alice.
h. Alice receives the envelope. Since the envelope is addressed to her, she can "decrypt" it by opening it, and reads the message aloud.

Step 5 (5-10 minutes): Subpoenas are served. Explain that because Bob was near a protest, the FBI was able to get a subpoena for his data on the day of the protest. Whether or not he was involved in the protest, it doesn't matter. The FBI has the subpoenas and is going to serve them.

a. The first subpoena is served to the SMS Center. They share what they have that matches the subpoena (the copy of the text message), and the FBI reads it aloud.
b. The second subpoena is served to the Signal server. The Signal server shares what they have that matches the subpoena (the envelope, which shows that Bob has an account with Signal), and the FBI reads it aloud.

Step 6 (10 minutes): Discussion. Lead discussion by asking the following questions:
a. What's the difference in security between sending a message via SMS versus Signal?
b. What threats does using Signal protect you from?
c. What threads does Signal *not* protect you from?

Adaptations:

You can use a similar activity to illustrate how VPNs encrypt network traffic and hide your IP address. You'll have to prepare different materials for this. The roles you'll want to prepare (on larger pieces of cardstock) are:

- Alice's Computer
- Wifi Router
- ISP-owned DNS
- ISP Server
- VPN-owned DNS
- VPN Server
- Google.com Server

Prepare three smaller pieces of cardstock, each with a silly Google search.

You'll want to label envelopes as follows:

- Envelope 1:
    - HTTPS
      To: Google - 74.125.224.72
      From: Alice's Computer - 29.765.11.35
- Envelope 2:
      To: VPN - 74.81.88.74
      From: Alice's Computer - 29.765.11.35
- Envelope 3:
      To: Google - 74.125.224.72
      From: VPN - 74.81.88.74

And finally, prepare two subpoenas:

- Very Official Subpoena for Google
    - All records related to Alice or IP address 29.765.11.35 from Google.com.
- Very Official Subpoena for VPN
    - All records related to Alice or IP address 29.765.11.35 from Private Internet Access.

If you'd also like to illustrate Tor, you'll want to prepare cardstock for:

- Tor Entry Node
- Tor Middle Node
- Tor Exit Node

And for Tor, you'll need the following envelopes:

- Tor Envelope 1:
  To: Tor Entry Node
  From: Alice - 29.765.11.35
- Tor Envelope 2:
  To: Tor Middle Node
  From: Tor Entry Node
- Tor Envelope 3:
  To: Tor Exit Node
  From: Tor Middle Node
- Tor Envelope 4:
  To: Google - 74.125.224.72
  From: Tor Exit Node

You'll run the activity the same as above, with the roles aligned such that the first message goes from Alice → Wifi Router → ISP-owned DNS → ISP Server → Google.com Server.

The second message will be placed inside Envelope 3, which will be placed inside Envelope 2, and will go from Alice → Wifi Router → VPN-owned DNS → VPN Server → Google.com Server.

If you illustrate Tor, a third message will be placed inside Tor Envelope 4, inside 3, inside 2, inside 1, and passed from Alice → Wifi Router → Tor Entry Node → Tor Middle Node → Tor Exit Node → Google.com Server.

In the discussion questions, discuss how using a VPN or Tor can protect you, and what its limits are.