Each question is worth 10 points. The total assignment is worth 170 points.

1. Online tracking and fingerprinting

   (a) One of the hotly contested issues in online tracking is whether tracking should be opt-out or opt-in, i.e., whether the default should be tracking or non-tracking. Does this actually matter, since both provide the same choice?

   (b) For "Do Not Track" to be meaningful, there has to be some way of detecting trackers that are not in compliance. What are some ways of doing so?

   (c) Experiment with Panopticlick. Try to minimize the identifiability of your usual browser or another browser. What’s the most anonymous you were able to get? With what settings?

   (d) Are there tools you can download that are specifically intended to resist fingerprinting?

   (e) Are there applications of fingerprinting for fraud prevention?

   (f) Neither self-regulation in the U.S. nor Government regulation in the EU (e.g., "the cookie law") has worked particularly well. What are some reasons that these attempts have run into problems?

   (g) Speculate on what the state of online tracking might look like in 5 years.
2. Tor

(a) Install and use the Tor browser. What privacy properties do you think Tor is providing? Against what adversary?

(b) Pick any Tor hidden service and use it. Record all IP addresses seen by your browser as you are using the service. Do all of them belong to Tor relays? Write down the name of the service, names of the relays, and any non-relay IP addresses you see.

3. Mobile security

(a) Name one way that malware writers deliver apps to iOS devices without use of the Apple app store.

(b) Describe a common man-in-the-middle attack against mobile (and other) devices that involves physical proximity.

(c) What does “dual persona” mean in mobile management? How can it be implemented?

(d) Why have “dual persona” approaches to security not succeeded?

4. Cybercrime and cyberwarfare

(a) What is an “air gap” and why did it pose a challenge to the writers of Stuxnet? How did Stuxnet jump the air gap at the Natanz Nuclear Facility?

(b) The Stuxnet worm represented several firsts in the evolution of malware. Name one.

(c) Visit the Digital Attack Map at http://www.digitalattackmap.com. What is the highest-volume single DDoS attack you can find? Given typical upload speeds for home broadband, approximately how big a network of bots would be required to mount this attack via direct transmission of (TCP/IP or UDP) traffic?

(d) How could a much smaller botnet be used to generate an attack with similar volume? How small?