COM-301 Computer Security
Exercise 10: Privacy

Privacy

1. Are the following statements True or False:

   (a) Privacy technologies based on using access control to control who access what, protect you from the service provider

   (b) Anonymous communications based on onion routing only protect from adversaries that cannot see both ends of the anonymous communication networks

   (c) Encryption is the only protection needed to ensure privacy online

   (d) Anonymous communications are the only protection needed to ensure privacy online

   (e) An internet without routing security (e.g., enabling BGP hijacking) can break the protection given by low-latency anonymous communication systems

   (f) Using a VPN provides privacy from a local adversary that can only observe the connection from the user to the proxy but not from a global adversary that can observe any link in the network

2. We have seen in the class that a problem with the Tor network, and in general any low-latency anonymous communication systems, is that the shape of the traffic enables an adversary to trace flows through the network. A possible option to fight this type of attacks is to "pad" the connection, i.e., insert enough dummy packets so that all connections look similar. Does this approach make sense to:

   (a) Conceal whether a user is visiting a news website (e.g., CNN, BBC, etc) or a small static web such as http://www.guimp.com/

   (b) Conceal which EPFL employee website a user is visiting (e.g., `https://people.epfl.ch/`)

   (c) Conceal which movie you are downloading from the Pirate Bay.

   (d) Conceal when electronic votes are being sent.

[HINT: think about the bandwidth overhead you would need to protect the traffic]

3. Let us assume that a COM-301 TA decides to invest the money from selling the exam questions into helping the Tor network instead of going to Hawaii. Thus, he buys 1000 machines and sets them up in the basement as onion routers.

   (a) Does this increase the Tor network capabilities to offer anonymity? Against which adversary?

   (b) If instead only one assistant, each of the COM-301 students puts 10 machines in their own basement, would the situation improve?

   [HINT: think about who could see the traffic going through the new machines should they be incorporated to the Tor network.]

4. We have seen in the class that anonymous credentials enable users to prove possession of an attribute (e.g., Bob is subscribed to the newspaper, Thomas is older than 18, etc.), and also that they are unlinkable across uses (e.g., Bob's visits to the newspaper cannot be linked to each other).

   Compare the privacy that Bob has when he visits CNN over Tor, and when he visits CNN without Tor.