Homework 4

Due: June 3, 2015 **Points:** 100

Questions

Remember to justify your answers. If you do not, then you will receive no credit for them, even if your (unjustified) answer is correct.

1. (*40 points*) The Tor protocol, as discussed in class, is intended to prevent an attacker who can observe a fraction of the links involved from tracing a message. Consider the situation in which an attacker can observe the *entire* Tor network, including entry and exit relays.

   (a) If only one client uses that Tor network to contact a server, how can the attacke determine the source and destination of the circuit?

   (b) Devise a way to prevent this. You may assume multiple clients have Tor proxies, but *not* that more than one client is connecting to a server. Why do you think Tor does not use your method?

2. (*30 points*) Consider a ring-based access control system with rings numbered from 0 (high) to 9 (low). A procedure segment with bracket (2, 5, 6) is executing on this system in ring 5. Assume the discretionary access controls allow all accesses to data and segments.

   (a) The procedure tries to write to two data segments with access brackets $(2,3)$ and $(4,8)$, and read data from a data segment with access bracket $(3,4)$. Which of these accesses succeeds?

   (b) It tries to call a segment with bracket (0, 1, 7) that resides in ring 4. Does the call succeed? If so, does a ring-crossing fault occur?

   (c) Unfortunately, the segment in (b) has a Trojan horse. When the original process calls that segment, it tries to append bogus information to a log with access bracket $(4,7)$ and erase data in a second log with access bracket $(0,1)$. Do either of these succeed?

3. (*30 points*) Consider how a system with capabilities as its access control mechanism could deal with Trojan horses.

   (a) In general, do capabilities offer more or less protection against Trojan horses than do access control lists? Justify your answer in light of the theoretical equivalence of ACLs and C-Lists.

   (b) Consider now the inheritance properties of new processes. If the creator controls which capabilities the created process is given initially, how could the creator limit the damage that a Trojan horse could do?

   (c) Can capabilities protect against all Trojan horses? Either show that they can or describe a Trojan horse process that C-Lists cannot protect against.

Extra Credit

4. (*20 points*) How can a system use originator-controlled access control to implement Cohen's information flow metrics as a defense against malware?