Homework 5 (Updated)

Due: December 2, 2016 **Points:** 100

Questions

Remember to justify your answers where appropriate.

1. (*25 points*) Please complete the post-class survey at

   `https://purdue.qualtrics.com/jfe/form/SV_0fvNeirjntAILCl`

   This survey asks you questions about robust coding. Please answer the questions as best you can. The answers will *not* be graded! Also, the teacher will not be told individuals' scores; he will simply be told whether you took the survey. So, where the survey says " the course ID assigned to you by your instructor," please enter your UC Davis student ID. The teacher will also be told the overall results, but not any individual results.

   Thus, you will either receive full credit for this question, or no credit.

2. (*30 points*) The Mysterious Mortgage Company announced it has upgraded the authentication required of its website users to two-factor authentication. Amy, a mortgagee, wants to log into her account on the web site. She enters her login name and password. Instead of showing her a screen with her account information, the next screen asked her to re-enter her login name and password. After she does so, she is then given the account page. Is this two-fsctor authentication? Why or why not?

3. (*45 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*) A vendor advertises that its system was connected to the Internet for 3 months, and no one was able to break into it. It claims that this means the system cannot be broken into from any network.

   (a) Do you share the vendor's confidence? Why or why not?

   (b) If a commercial evaluation service had monitored the testing of this system and confirmed that, despite numerous attempts, no attacker had succeeded in breaking into it, would your confidence in the vendor's claim be increased, decreased, or unchanged?