

University Of Washington, CSE 590P – Computer Security - Homework 8  
Tadayoshi Kohno, John Manferdelli

Due: 4:30pm March 8, 2007. This homework is worth 18 points.

See the course website (<http://www.cs.washington.edu/education/courses/csep590b/07wi/>) for instructions on how to submit your homework. For this assignment, you should submit a PDF file named 'YourLastName-YourFirstInitial-HW8.pdf'. Please type your name on the first page of your assignment.

1. (6 points total.) Look at the information about intrusion detection systems here <http://snort.org/docs/faq/3Q06/faq.html> and, in particular, here <http://snort.org/docs/faq/3Q06/node18.html>.
  - 1.1. (3 points) Give one key advantage and one key disadvantage with placing an IDS system on the *inside* of a firewall.
  - 1.2. (3 points) Give one key advantage and one key disadvantage with placing an IDS system on the *outside* of a firewall.
2. (6 points total.) Consider slide 108 on honeypots in the lecture's slide deck, as well as slide 6 in <http://www.cs.ucsd.edu/~mvrable/papers/2005-sosp-potemkin-presentation.pdf>.
  - 2.1. (2 points.) Give one key advantage and one key disadvantage with *low involvement* honeypots (like network telescopes which passively listen for network activity).
  - 2.2. (2 points.) Give one key advantage and one key disadvantage with *medium involvement* honeypots (like honeyd).
  - 2.3. (2 points.) Give one key advantage and one key disadvantage with *high involvement* honeypots (real machines).
3. (6 points total.) Describe three challenges (at most one paragraph each) with providing ubiquitous low-latency anonymous communications. You may find this paper helpful: <http://tor.eff.org/svn/trunk/doc/design-paper/challenges.pdf>. You may also think back to all the other issues we discussed in class, from usability and social issues to technical issues.
4. (7 points total extra credit.) Read the paper on Tor: <http://tor.eff.org/svn/trunk/doc/design-paper/tor-design.pdf>. Then answer the following questions
  - 4.1. (1 point.) Short summary of the paper.
  - 4.2. (2 points.) Two most important new ideas in this paper, and why (at the time the paper was written).
  - 4.3. (2 points.) Two biggest weaknesses with the paper, and why.
  - 4.4. (2 points.) Two important open research questions on the topic, and why the questions matter.

Reading:

Gollmann, Chapter 13.