Ground Rules. You may choose to work with one other student if you wish. Only one submission is required per group, please ensure that both group members names are on the submitted copy. Work must be submitted in hard copy by the start of class.

1) False Positive Answer. Anderson’s chapter 10 details several ways to defeat physical intrusion detection systems (a.k.a. “burglar alarms”). One of the common ones is to artificially create “false” alarms so that the true alarm is ignored. Let’s investigate this idea with respect to logical intrusion detection systems.

(a - 2 pts) An old Snort rule says that any HTTP packet that includes “/..%c0%af../” should trigger an alarm, as an attempted IIS exploit. Explain why in “normal” usage this rule would have a low false positive rate.

(b - 5 pts) Suppose Eve discovers a web server, vulnerable.org that is vulnerable to the IIS unicode exploit and she wants to exploit the hole without having it noticed. What are a few ways Eve can temporarily increase the false positive rate at vulnerable.org for the rule, without getting her IP address noticed?

(c - 3 pts) What can you conclude about “advertised” false positive and false negative rates?

2) Shuffle Issues.

Pretend I have an email anonymizer based around a Chaum mix. In order to do timely delivery, theChaum mix receives messages, waiting until the anonymity set size reaches a certain fixed value, and then flushes, sending the emails.

• A (5 pts) - Pretend you are an adversary watching the network traffic of the mix. How can that adversary launch an attack which de-anonymizes a single user?

• B (5 pts) - Adjust the design of this chaum mix in order to mitigate this attack.

Paper Review If you are a graduate student, you are expected to also include with this exercise set a paper review of one of the papers posted as graduate reading over these two weeks. Your paper review is not supposed to be a full paper in and of itself, but rather a summary in your own words and some evidence that you’ve thought about what the paper is trying to do, if they achieve their goals, how useful their goals are, and how it could be improved. Your paper review should have the following components.

• A brief summary in your own words about what the paper was about. You should cover what problem the paper was trying to solve or highlight, how the authors proposed achieving their goals, and how the authors evaluated their success. This should NOT simply be a re-statement of the abstract hit with a thesaurus until un-recognizable, I do not mind if you did not fully understand the paper, if something was confusing, or you did not understand a concept, feel free to state that. (1-2 paragraphs)
• State one problem with the paper. Every paper has a problem, be it an evaluation that does not actually measure what it should, a poor assumption, an incorrect threat model, an obvious attack/defense, etc. Find one thing that you think is a flaw in the paper, and briefly explain why you think it is a flaw. (2-3 sentences)

• State two possible things that could be done for future work. This could be expanding the attack/defense to work under different assumptions or in different deployments. It could be a different set of evaluations. It could be an improvement to how the system is constructed. Try to be specific. (1-2 sentences each)

Choose a paper from the weeks listed as “Peer to Peer Systems” or “Privacy and Anonymity”.