COSC 434/534: Network Security

Exercise Set 1  Due: January 31, 2018

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. Threat Models and Risk Assessment. Suppose the course instructor has created a database of all information for this course: homeworks, exams, handouts, and grades. Create a detailed threat model for this database: what should the security goals be? What are reasonable attacks, and who are the potential attackers? What threats should we explicitly exclude from consideration?

Now assume that the database is stored on the instructor's personal laptop, with no network card and no floppy disk drive. Propose at least two security mechanisms that would help counter your threat model (e.g. file or disk encryption, a laptop lock, a safe to store the laptop, a Kevlar laptop sleeve, relocation to Fort Knox . . . ), and analyze the net risk reduction of both. You should justify your estimates for the various incidence rates and costs. While we do want to see numbers for this part, don’t worry about figuring out exact costs or risk reductions, guess at some reasonable numbers but don’t spend very long at this part of the assignment.

2. How the Internet Is Glued Together. What are the five layers in the Internet protocol stack? What are the principal responsibilities of each of these layers?

3. ARP By Other Means. There are alternative ways we could execute ARP over the simply query-response method we use now. One method could focus on the use of a trusted authority, the other could rely on distributed consensus.

(a) The trusted authority solution would work as follows. A single, well known, host operated by the local network owner is the only host that is allowed to respond to ARP queries. It maintains its own ARP cache either through out of band means (e.g. a static config file) or by assigning hosts IP addresses to hosts itself. All hosts in the network will only transmit ARP queries directly to that host (i.e. they know the MAC address of this trusted host), and only accept ARP responses from that host. Analyze the security of this system compared to how ARP is currently done. You should think about each of the four security properties (confidentiality, integrity, availability, and accountability).

(b) The distributed consensus approach works like this. ARP queries are broadcast like they are now, but rather than only the host which has the IP address responding, all hosts respond with what they think is the correct answer. The host which sent the ARP query will in turn accept the most common response. Again, analyze the security of this system in the same manner you did for part a.

1 n.b.: this database does not exist; don’t waste your time trying to attack it!
**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 “Addressing” or “Routing”.