The University of North Carolina at Greensboro
CSC 580: Cryptography and Security in Computing
Prof. Stephen R. Tate

Handout 3
January 19, 2017

Homework 1 – Due Tuesday, January 24

Reminder: Homework problems are for you to develop skills and to practice. Once you get a handle on solving these problems, think of generalizations and practice those as well. Clear communication is as important as the right technical idea, and you should write up your solutions clearly so that they can be understood by a non-specialist (and non-mindreader!).

Next Tuesday (Jan 24) students will exchange papers and we will discuss solutions. There will be a quiz on Thursday (Jan 26) consisting of a single problem similar to one of these.

1. Consider a dishonest owner of a coffee shop that provides free WiFi service to its customers. Briefly describe one passive attack and one active attack that the owner could perform on its customers who use WiFi.

2. Draw a system model, identifying data at various parts in the system, for processing a credit card purchase in a store. I'm not expecting you to know or report on how this *actually* works in stores today, but I want you to think, from your own personal experience, about the "pieces" in such a system and how they could work together.

3. Draw an attack tree for stealing a car. Your attack tree should show various attacks, but you do not have to estimate the cost of attacks.