COSC 434/534: Network Security

Homework 1 Extra Credit Due: March 31, 2017

Ground Rules. You may choose to work with up to two other students if you wish. Only one submission is required per group, please ensure that all group members names are on the submitted copy. Work must be submitted electronically via email. You will use your Homework 1 login for these homeworks, they are already installed.

More “Complicated” Passwords, I Swear. [20 points]

Part 4 and 5 use an identical protocol to parts 2 and 3, so your offline dictionary attack is a good starting place. The Part 4 and Part 5 clients are “more secure” with their passwords. They use some common tactics that normal people utilize to pass password strengtheners. There are several pieces of research and software that address how easy it is to break passwords, even when users are applying “good” policies. Some links to two of the most relevant ones are on the course web page where you found this writeup. Sadly, my protocol does not exactly match a common authentication scheme, so this is not as simple as directly using John the Ripper, but you can either call into John the Ripper’s code base, or at the very least, you should examine the search techniques of John the Ripper and integrate them into your own offline attack. I will point out two hints. One, the search space is larger, so you might want to decompose this into a parallel task. Two, you’ll notice that you still need cracklib-small, that should give you a hint on what the passwords are based on. For every password you recover you will receive a bonus 10% towards you Homework 1 score.

Usage follows the same for as the other three parts of the homework.
The cracklib-small dictionary must still be in the directory you run the jar from.