# CSI 4138 / CEG 4394
# Design of Secure Computer Systems

**Assignment #2**
**Due: Friday, November 16, 2018 (before 16:00)**

In class we discussed a botnet that targeted (among other things) DNS servers and used IoT devices in the attack. In the paper "Understanding the Mirai Botnet" [1], the authors do a thorough study of this particular piece of malware.

For this assignment, you must read this paper and provide the following.

- Give a two-page overview of the content of this paper, describing the botnet, its main features, and its evolution over time, in a way that can be understood by non-specialists.

- Identify clearly (separately from the overview) the main vulnerabilities, deficiencies, and weaknesses (in hardware, software, and humans) that contributed to the success of this botnet.

- The authors describe some steps that can be taken to help protect against such botnets in the future. List these and discuss which one(s) you feel is(are) most important or urgent, and why. Are there any additional steps that were not mentioned by the authors, but you feel should be taken? What are they and why would they help?

The assignment should be a maximum of 4 pages in total and need not include any additional references (aside from the paper itself, which of course must be referenced) since you are not being asked to gather, learn, or refer to any material beyond the actual content of the paper. However, note that if you do refer to any other material (papers, articles, websites, etc.), these must also be properly referenced.

[1] M. Antonakakis, *et al*., Understanding the Mirai Botnet, *Proceedings of the 26th Usenix Security Symposium*, Vancouver, Canada, August 16-18, 2017, pp. 1093 – 1110. (https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis)