**Paper Reading Questions**

For each paper, your assignment is two-fold. By 10PM the evening before lecture:

- Submit your answer for each lecture's paper question via the submission web site in a file named `lec`*`n`*`.txt`, and
- Submit your own question about the paper (e.g., what you find most confusing about the paper or the paper's general context/problem) in a file named `sq`*`n`*`.txt`. You cannot use the question below. To the extent possible, during lecture we will try to answer questions submitted the evening before.

**Lecture 8**

Suppose you are helping the developers of a complex web site at http://bitdiddle.com/ to evaluate their security. This web site uses an HTTP cookie to authenticate users. The site developers are worried an adversary might steal the cookie from one of the visitors to the site, and use that cookie to impersonate the victim visitor.

What should the developers look at in order to determine if a user's cookie can be stolen by an adversary? In other words, what kinds of adversaries might be able to steal the cookie of one of the visitors to http://bitdiddle.com/, what goes "wrong" to allow the adversary to obtain the cookie, and how might the developers prevent it?

Note: an exhaustive answer might be quite long, so you can stop after about 5 substantially different issues that the developers have to consider.

# 6.858 Computer Systems Security

Fall 2014