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 16

What are some other situations where an adversary may be able to learn confidential information by timing certain operations? Propose some ideas for how an application developer might mitigate such vulnerabilities.

6.858 Computer Systems Security

Fall 2014