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 13

What is the worst that could happen if the private key of a user is stolen (i.e., becomes known to an adversary)? Similarly, what is the worst that could happen if the private key of a service is stolen? How should the compromised user or service recover? Think about possible vulnerabilities in the recovery process if the user or service key is known to an adversary.

6.858 Computer Systems Security

Fall 2014