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 3

For a BROP attack to succeed, the server must not rerandomize canaries after crashing. Suppose that, after a server crashes, it creates a new canary by SHA1-hashing the current `gettimeofday()` value. Is this new scheme secure?

6.858 Computer Systems Security

Fall 2014