

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 `lecn.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 `sqn.txt`. You cannot use the question below. To the extent possible, during lecture we will try to answer questions submitted the evening before.

Lecture 7

Suppose an adversary discovers a bug in NaCl where the checker incorrectly determines the length of a particular x86 instruction. How could an adversary exploit this to escape the inner sandbox?

MIT OpenCourseWare
<http://ocw.mit.edu>

6.858 Computer Systems Security
Fall 2014

For information about citing these materials or our Terms of Use, visit: <http://ocw.mit.edu/terms>.