

Lecture 6: Principles of Secure Design

Date: October 9, 2013

Homework Due: Oct. 18 at 5:00pm

1. Why secure design is important
2. Underlying concepts
 - a. Simplicity
 - b. Restrictiveness
3. Principles of secure design
 - a. Principle of least privilege
 - b. Principle of fail-safe defaults
 - c. Principle of economy of mechanism
 - d. Principle of complete mediation
 - e. Principle of open design
 - f. Principle of separation of privilege
 - g. Principle of least common mechanism
 - h. Principle of least astonishment
4. Discussion topic

Discussion Topic

An attacker has changed the home page of the New York Times. The new version indicates disgust with one of the Times' reporters. Throughout this puzzle, assume that no other damage was done.

1. If their intent was to show that the New York Times needed better security on their web page, was this an appropriate technique? Why or why not?
2. The attackers feel that the reporter wronged one of their friends. The Times ignored their letters and protests. So they decided on a more noticeable protest. Was this an appropriate form of protest? Why or why not?