**CMU SE 17-627 Software Security Engineering**

Homework #1

**Nancy Mead Due: Date shown on syllabus**

**READINGS:**

Software Security Engineering book – Chapters 1 & 2, Saltzer & Schroeder paper, HICSS Principles paper, Drone attack articles

**DISCUSSION/EXERCISE:**

Objectives:

* Understand various types of attacks and avoidance techniques
* Learn about historic and modern assurance principles and how they differ

Assignment:

1. Surf the web and find four different actual examples of successful intrusion:
   1. One that resulted from human error (e.g. giving out a password or downloading a virus)
   2. One that resulted from a system configuration error
   3. One that resulted because of a flawed development process
   4. One that resulted from a vulnerability in a COTS project

Describe how each of these attacks could have been avoided. Consider changes in policy, configuration management, software development practice, and COTS acquisition practices.

1. Compare and contrast the HICSS Principles paper with the Saltzer and Schroeder Principles paper.
2. Turn this assignment in on Blackboard BEFORE the next class.