

Background:

Whittaker's book, *How to Break Software*, provides an excellent list of stereotyped tests (which he calls *attacks*). The idea behind an attack is that you come up with a theory of error, then My experience with students dealing with this material is that they get very confused about the differences among whittaker's attacks. So:

Activity:

- Divide the class into 4 (or preferably 5) groups
- Each group starts with a different class of attack, where the classes are output, data, computation, media, and file. I explicitly tell students NOT to work on input attacks, because they already understand most of these.
- I assign the starting attack category to each group. They then create 3 attacks of that kind. After that, they rotate to another attack category.
- At 6 pm, students present exemplars of the attack categories.

Here's what happened

- To motivate the work, I gave students a multiple-choice quiz with several tests, and for each test, I asked whether this was an example of a file attack, media attack, etc. The students got predictably confused, and were thus ready for a statement that they would never learn how to tell these apart until they worked with the ideas. (Up to here, everything worked as expected)
- In the groups, it became clear that many students had not yet read the book. Therefore, much class time was taken skimming Whittaker's book, and then fishing for ideas at the just-been-exposed level of work.

Here's what we'll do:

- Give students this exercise (create 3 tests per category) as an assignment, have them turn it in.
- For the lab, I'll grade the best two examples and not worry about grades for the rest.