Notes for October 5, 2000

1. Greetings and Felicitations!
   a. Homework #1 due on Thursday, October 12; date on tentative syllabus was changed. In general, go with the date on the assignment.
2. Puzzle of the day
3. Robust Programming
   a. Go through handout, emphasizing principles
   b. Information hiding and abstraction
   c. Error handling
4. Common Implementation Vulnerabilities
   a. Unknown interaction with other system components (DNS entry with bad names, assuming finger port is finger and not chargen)
   b. Overflow (year 2000, *lpr* overwriting flaw, *sendmail* large integer flaw, *su* buffer overflow)
   c. Race conditions (*xterm* flaw, *ps* flaw)
   d. Environment variables (*vi* one-upsmanship, *loadmodule*)
   e. Not resetting privileges (Purdue Games incident)

Puzzle of the Day

Saul Alinsky illustrated one of his rules of tactics for an organizer with the following example:

> The third rule is; *Whenever possible go outside of the experience of the enemy.* Here you want to cause confusion, fear, and retreat.
>
> General William T. Sherman, whose name still causes a frenzied reaction throughout the South, provided a classic example of going outside the enemy's experience. Until Sherman, military tactics and strategies were based on standard patterns. All armies had fronts, rears, flanks, lines of communication, and lines of supply. Military campaigns were aimed at such standard objectives as rolling up the flanks of the enemy army or cutting the lines of supply or lines of communication, or moving around to attack from the rear. When Sherman cut loose on his famous March to the Sea, he had no front or rear lines of supplies or any other lines. He was on the loose and living on the land. The South, confronted with this new form of military invasion, reacted with confusion, panic, terror, and collapse. Sherman swept on to inevitable victory. It was the same tactic that, years later in the early days of World War II, the Nazi Panzer tank divisions emulated in their far-flung sweeps into enemy territory, as did our own General Patton with the American Third Armored Division.[1]

1. What lessons does this passage teach attackers?
2. What lessons should computer security administrators draw from this passage?

[1] Saul Alinsky, *Rules for Radicals*, Random House, Inc., New York, NY (1972) pp. 127–128.