Outline for the Day

Reading: handout

1. Greetings and felicitations!
   a. Puzzle of the day
2. Robust library
   a. Tokens and their generation and analysis
   b. Functions
3. 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)