

Version of April 24, 2002 (another change today, correction of the first sentence).

COP 6855

Spring 2002

Take-home exam

Due Monday, April 29 at midnight. For everybody, including remote FEEDS. No extensions or makeups.

We are building a voting system to be used for federal, state, and county elections.

Voters register in advance at a voting precinct (based on where they live). Voting precincts keep lists of all the voters registered at their locations.

When there is an election registered voters can vote in two ways:

- Going to the voting precinct and using a local terminal there.
- Through the Internet using a remote browser.

In order to vote, a user must be authenticated and the system checks that she has not already voted.

Each precinct keeps its own database of the received votes and tallies the results after the end of the voting period.

A central elections authority receives local precinct results and adds them together to determine the result of the election. This authority also keeps a list of all voters to avoid double registrations.

If the election is contested, the votes at each precinct must be checked and recounted by officers from the central authority.

- a) Select a set of general security policies for this system.
- b) Enumerate possible attacks to this system. Consider each architectural unit and each architectural level.
- c) Choose a security model and use it to refine the policies you selected in a).
- d) Define the security requirements for the components of this system (OS, hardware, DBMS, communications,...) based on your previous choices. Try to select specific systems, e.g., Intel Pentium, Windows XP, J2EE, etc., that you'd recommend in order to fulfill your requirements.

Make any necessary assumptions for unspecified aspects and describe them explicitly. Avoid unnecessary descriptions or irrelevant aspects.

Grading is based on proper selection, precision, reasonable completeness, and appropriate use of class concepts.

Bonus: try to find new patterns (describe the idea, if possible using UML).

Note the version date at the top of this page, I may make corrections along the week. Clarifying questions can be sent to: ed@cse.fau.edu during regular hours, or to edbfen@yahoo.com after hours and on the weekend of April 27-28. Please no phone calls or visits. Look at my SD 2001 talk on Internet security for the answers to last year's exam (page 45) and use it as a guideline. I discussed part of that exam in class also.

I prefer hard copies for the exam answers but if it is difficult for you to bring the papers to my office you can send an e-version.