ASSIGNMENT 2
Due: Thursday 3/14 by class time
Preferred hand-in method: email document to {franklin,kkeeton}@cs.berkeley.edu

Write a 3-5 page summary sharing your evaluation, insights and conclusions on the RPC and security papers covered in class. As with the last assignment, we are looking for a combination of original thoughts and synthesis, as well as evidence that you've read the papers. Again, we encourage you to discuss the material and your ideas with your fellow students, but we ask that each of you write and submit your own summary.

The format of this assignment is fairly unrestricted. You should address interesting and relevant issues raised by the papers. Some examples might include (but are not limited to):

- How secure do systems need to be? What's the right combination of techniques to achieve this level of security? What issues remain to be solved?
- How do we know if research in these areas has been successful?
- How should we evaluate these techniques? Are the principles of secure system design used in the Java paper the right factors? What metrics could/should be used for quantitative (or even qualitative) evaluation?
- What's the right tradeoff between security and performance, availability, scalability, etc.?
- What are the right underlying abstractions:
    - for increasing system security?
    - for permitting communication between cooperating parties (e.g., client/server, peer-to-peer)?
- How do security and communication change in the emerging computational models of the Internet?
- How are the systems techniques we discussed used in database systems? (Alternately, how **should** they be used?)