Massachusetts Institute of Technology
6.857: Network and Computer Security
Professor Ronald L. Rivest

Handout 29
December 9, 1997

Solution to Problem Set 6

Problem 6-1. ZK proof of Satisfying Assignment

This problem is most easily solved by just following the hints given in the set.

The Prover commits, for each wire, a "wire coding type" for that wire. The wire coding type is either AB (that is, 0 is coded as A, and 1 as B) or BA (the reverse). These coding types are chosen independently for each wire. He also commits to a coded value (either A or B) for each wire. Finally, he commits to a coded truth table for each gate, where the rows are coded using A's and B's.

This truth table is permuted on a line by line basis, and committed similarly (so we can reveal only a line of it if we want to).

After performing these commitments, the prover sends the values to the verifier, who flips a challenge coin and sends the result to the prover. Before doing anything else, the prover reveals the coding type AND code of the output wire (i.e. proves the output is a one).

- if the challenge is a zero, just reveal all the tables and the mappings of A's and B's to 1's and 0's. This will not reveal the values on the wire (since we don't know if the wire is an A or a B), but will show that all the tables are correct.
- otherwise, we reveal for all wires if they are A's or B's, AND we reveal ONLY the corresponding line in the table for the inputs and outputs. This establishes a chain that leads up to a 1 output, but doesn't reveal anything about the inputs or the intermediate values. Note it is important we do not reveal the entire table, since some gates could leak information about the mapping of letters to numbers).

We repeat this k times, each time picking new mappings for the wires, and permuting the rows of the tables.

We have a protocol, now we need to show the three parts of zero knowledge proofs hold:

Completenessholds, since any valid prover can do this.

Soundnessholds, since an invalid prover only has a 50% chance per pass of cheating. If he guesses that the call will be a zero, he needs to have well formed tables. But since he doesn't know the solution, if he gets a one instead, he will not have a valid chain that leads to a one output with good tables. If instead he hopes for a one, then he will need to munge the tables in such a way that he gets a chain of entries that lead to a one output. However, since he doesn't know the solution, at least one table has to be invalid, so if the challenge is instead a zero, this will be noticed.

Zero Knowledgeholds since any verifier can easily recreate this conversation by talking to himself. Just guess the challenge, and create valid data for the challenge. If the guess is wrong, rewing the transcript and try again. The guess will be wrong 50% of the time in both cases, so the distribution will remain the same.

Problem 6-2. User identification

This is an opinion essay, so any well written document demonstrating a good understanding of the system and the issues got five points, points were taken off if any obvious points were missing.

- Pros include
  1. no tokens to lose or transfer
  2. no passwords to forget
  3. audit record
  4. humans are probably better than AI's at this when they spend the time to be careful
- Cons
  1. Requires expensive equipment
  2. limits usage to those machines set up as part of the network. no dialup or such.
  3. VERY easy to break into the entire system by corrupting one user: let him be in late at night, when others have gone home. Then, log in to every account that has corrupted user as checker. Then, propagate from that point. Assuming there is a link from every person in the company to every other person (six degrees of separation) then all accounts have been compromised
  4. checkers may get lax if this interrupts work
  5. checkers may be absent due to breaks
  6. if cliques form, then when the clique goes off to a meeting or a social event, when they get back, none of them can log in.
  7. if the power goes out, resuming is slow.
  8. every day, the sysadmin has to be the first person in. No employee can come in late at night to do some work unless the sysadmin is always there.
  9. Mission-Impossible style attacks could still work (video recording, disguises, etc).
  10. Privacy issues.