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

Handout 28
November 9, 1999

Problem Set 7

This problem set is due on *Thursday, November 18, 1999* at the end of class. Late homeworks will *not* be accepted. You are to work on this problem set in groups of three to four people. (Be sure that you all understand the solutions turned in to each problem.)

Mark the top of each sheet with your names, 6.857, the problem set number and question, and the date. **Type up your solutions**[1], and be clear. Points may be deducted if your TA has problems understanding your solution.

Problem 7-1. Phone Monopoly

Alice, Bob, and $n-2$ of their favorite friends are playing a game of Monopoly over the phone. They need to roll the dice (two six-sided dice), but they don't trust each other to report the roll of each die accurately. Design a protocol whereby the n of them can fairly generate the random numbers they need, without trusting anybody else. Make sure your protocol is resistant to $n-1$ of the players colluding against the n^{th}.

You may, if you wish, answer this question assuming that there exists a sufficiently secure commitment protocol (a la problem set 5) that does not require a trusted third party. Describe the possible attacks you want to be secure against, and argue that your solution protects against each of these attacks.

Bonus: can you solve this problem without relying on a secure commitment scheme?

Problem 7-2. Protocol Design

Design and analyze a protocol for the following situation.

Alice is an employee of ABC Corp. She has a public RSA key P_A and a secret RSA key S_A. ABC has many PC's, any one of which Alice may wish to sit down at and log in to. All the PC's run the same software, and all are connected to a central ABC server via a network. The server is capable of storing user files remotely and securely, and capable of performing secure cryptographic operations securely. Assume that the PC and server software is secure, but that the network connection is not secure.

Alice wishes to use her secret key S_A to sign documents, etc. However, she does not have a smart card or any secure way of carrying her secret key with her from PC to PC. Alice is, however, capable of remembering a password.

Your answer should show:

- How the server can store an encrypted form of Alice's secret key.
- How Alice can securely download the secret key from the server.
- How well your protocol protects Alice's secret key from various attacks, including at least:

[1] If you latex your solutions, include a URL or AFS path where I can find the latex file(s); I will distribute my favorite solution for each problem to the class as the 'official' solution – this is your chance to become famous! Note that if I choose your solution, then you get an extra point on that problem.

–An off-line dictionary search for Alice's password by a passive eavesdropper who overhears Alice download her secret key (your solution should definitely protect Alice against this threat).

–An attack on Alice's secret key by a corrupted server.

–An on-line attack by someone attempting to impersonate Alice to the server.

–An on-line attack by someone attempting to impersonate the server to Alice.

You should also try to be efficient, and minimize the number of messages required by the protocol.

Problem 7-3. More Dining Cryptographers

Professor Rivest is having dinner with his friends. When they finish their dinner and begin preparing to pay, the waiter informs them that their meal has already been paid for. Clearly one of them has paid for the meal, but being polite, they don't want to force the one who was generous to admit it. On the other hand, they want to make sure that the restaurant isn't cheating them (eg, if more than one of them paid), and they also want to make sure that the NSA isn't picking up the tab for use as blackmail later (ie, none of them paid).

One of the cryptographers (from a different school) proposes the following protocol: each of them picks a random number from Z_n (for some sufficiently large n, at least a few hundred), and passes that number to his left. When he receives each number, he increments it by 1 if he paid for the meal, else he leaves it alone. Then he passes it to his left. When each number has gone all the way around the table, each person reveals the number of people he believes have claimed that they paid for the meal. If each of them reveals 'one', then they're done.

Analyze the security and correctness of this protocol.

Problem 7-4. Payment Schemes

Argue as clearly as you can that a "token-based" payment scheme is impossible if all parties have unlimited computational power.