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

Handout 2
February 9, 2009
Due: February 18, 2009

Problem Set 1

This problem set is due *via email,* to `6857-hw@mit.edu` on *Wednesday, February 18* by the beginning of class.

You are to work on this problem set with your assigned group of three or four people. You should have received an email with your group assignment for this problem set. If not, please email `6.857-tas@mit.edu`. Be sure that all group members can explain the solutions. See Handout 1 (*Course Information*) for our policy on collaboration.

Homework must be submitted electronically! Each problem answer must appear on a separate page. Mark the top of each page with your group member names, the course number (6.857), the problem set number and question, and the date. We have provided templates for LaTeX and Microsoft Word on the course website (see the *Resources* page).

Grading and Late Policy: Each problem is worth 10 points. Late homework will not be accepted without prior approval.

With the authors' permission, we will distribute our favorite solution to each problem as the "official" solution—this is your chance to become famous! If you do not wish for your homework to be used as an official solution, or if you wish that it only be used anonymously, please note this on your homework.

Problem 1-1. Security Policy

In this problem you are to write a security policy for *either* Facebook or Google Latitude. That is, you should answer *either* part (a) or part (b), not both.

For help on writing this policy you can see *Sample Solutions from PS1 2003.* See question 1-4, which asked students to develop a security policy for either the MIT Card or Apple's iPod. Sample solutions for both, as well as a short discussion from the TAs regarding common omissions, are included. These should help guide you in terms of content, format, and length.

(a) Facebook

Facebook is a social networking site (as you probably know). Users of the site have profiles on which they post personal information. This information includes items such as the user's real name, photos, and friends. Certain parts of a user's profile (such as the wall) may be modified by other users. In addition to maintaining profiles, Facebook allows users to designate a set of friends and to send messages to other users. Facebook also uses its members' personal information to target advertisements and may share this information with 3rd parties (such as application developers).

Although the site allows members to communicate in novel ways, the site raises many privacy concerns. Possible issues include:

- What information on a user's profile is sensitive? Who is allowed to view the various types of information?
- How much control does a user have over his or her profile?
- Can users determine who has looked at their profile?
- What kinds of information can Facebook use to target advertisements?
- What information can Facebook share with 3rd parties? This includes both application developers and potential advertisers.
- Can Facebook employees examine the personal information of any user? Keep in mind that some employees may need some or all of this information to perform their jobs.

Your task is to write a short security policy for Facebook that takes into account privacy concerns. Facebook does have security measures in place that address some of these issues. However, these measures are not the only possible security measures, nor are they necessarily the best ones. Be creative.

(b) Google Latitude

Recently Google launched Latitute. This software allows users to share their location and related information with friends. It shows when the location was last updated. Also, when no location has been entered, the location appears as unknown. Users can choose the level of location sharing for each friend individually. Describe a security policy for Latitude, including how many levels of location sharing are desirable, granularity or resolution of the location, and choices for updating information.

Problem 1-2. Many-time Pad

The TAs took 16 sentences $S_1, S_2, ...S_{16}$ from a cryptography paper and encrypted them with a one-time pad to generate 16 ciphertexts $C_1, C_2, ...C_{16}$. Unfortunately the TAs were lazy and used the same one-time pad P to encrypt every sentence (i.e., $C_1 = S_1 \oplus P$, $C_2 = S_2 \oplus P$, etc.). Due to this mistake, you should be able to decrypt the strings and recover the original sentences.

We have provided all 16 ciphertexts in the "enc.tar.gz" file in the Resources section of the course website. This archive contains a file named "`enc<k>.bin`" for each ciphertext C_k. Find S_1 (the decrypted contents of "enc1.bin") and describe the process you used.

HINT: Many of the sentences contain the word "cryptographic."

Problem 1-3. The SHA-3 Competition

In this problem you are going to help Professor Rivest prepare for the Feb 25–28 NIST AHS (Advanced Hash Standard) Conference. There are 42 unbroken submissions in the SHA-3 hash function competition, including the MD6 proposal developed by Professor Rivest, your TA Jayant, and other MD6 team members. (See `http://csrc.nist.gov/groups/ST/hash/sha-3/` for more information about the NIST competition.)

Each team has been assigned several competing proposals to review. You should have received your assigned hash functions in the email with your team assignment. (No team will get MD6, but you are of course free to look at the MD6 submission `http://groups.csail.mit.edu/cis/md6/`.)

Your assignment is to quickly review the assigned submissions, summarize the security properties that have been proven or well-established in the submission (as opposed to hand-waved, hoped-for, or left unmentioned), select one of your assigned submissions as the "best" of your set, and say why you selected it as the best. You don't need to check the correctness of proofs given; your job is more to find out if they are offering any proofs, and if so, of what. It is OK if they establish a property by referencing a suitable proof or related result in the literature.

Only focus on security for this assignment; do not look at speed, simplicity, flexibility, etc.

Here is a (partial) checklist of things you might look for:

- Proofs of mode of operation security – For each of the properties listed below, determine if the submission proves that the mode of operation preserves the property. These proofs should assume the compression function possesses the property and use this assumption to show that the entire construction possesses the same property.
  - Indifferentiability from a random oracle
  - Pseudorandomness
  - Collision resistance
  - Preimage-resistance
- Provable resistance to differential cryptanalysis.
- Provable resistance to linear cryptanalysis.
- Proof that the hash function, when used in a keyed mode for a MAC (message authentication code), is not subject to length-extension attacks.

(If you're interested, you can see the NIST call for submissions for a discussion of what they are looking for `http://csrc.nist.gov/groups/ST/hash/documents/FR_Notice_Nov07.pdf`, and/or look at the MD6 submission for a rather complete treatment `http://groups.csail.mit.edu/cis/md6/`.)

Some submissions prove little or nothing about the security of their method; others may prove quite a bit. Just list the properties that they claim to have established or proven. For each such property, given the page number(s) in the document where they give the proof or evidence for the property.

The documentation for these hash functions is available from the SHA-3 zoo at `http://ehash.iaik.tugraz.at/wiki/The_SHA-3_Zoo`.

Bonus: If your team can cause one of the previously unbroken submissions (including MD6) to be withdrawn from the competition due to a security problem discovered by the team, then all team members get an A for the class with no further work required!