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

Handout 27
October 31, 2002

Problem Set 5

This problem set is due on *Thursday, November 7, 2002* at the beginning of class. Late homeworks will *not* be accepted.

At the end of each problem, tell us how each person contributed (writing, designing, coding, proof reading, moral support, etc).

Problem 5-1. SPKI/SDSI

In SPKI/SDSI certificates are "cumulative": no certificate invalidates any other certificate. In this way, certificates can be used in a natural way to form *groups*. For example, the certificates:

$$\begin{aligned} K\text{ta} &\longrightarrow K\text{mit kevin\_fu} \\ K\text{ta} &\longrightarrow K\text{mit thien\_loc\_nguyen} \end{aligned}$$

defines the group "ta" for the key K (which might be the 6.857_2002 key, say). Each certificate adds a new possible meaning (or member) to the name (i.e. group) K ta.

Please consider the following modification to SPKI/SDSI, and present your evaluation of it in terms of utility, security, ease-of-use, workability, applicability for the web-access application described in class, and/or other criteria you feel relevant. Limit your discussion to one page.

In this proposed modification, everything works as usual, except for reducing name certs. These are certs of the form:

$$KA \longrightarrow K'$$

By definition, these are certs with only a key on the right-hand side.

The modification is that a new reducing name cert with the same left-hand side as a previous cert is intended to *replace* the previous cert. (Assume that each cert contains its date of issue, so that priority can be determined.) Thus, at most one reducing name cert should be valid for a given key/identifier pair at a given time. The goal is primarily to allow for smooth key rollover, so that a party can replace his old public key with his new one when it seems desirable to do so.

Problem 5-2. Term projects

In 1 or 2 pages, give us a status report on your term project. Provide responses to comments written on your proposal. Here are optional suggestions for your status report. Give updates on any decisions you may have changed. If you are implementing something, let us know how far along you are. If you needed to obtain permission from others (e.g., the MIT committee on testing of human subjects), let us know how things are progressing. List any requests for help or special equipment.

Problem 5-3. Zero knowledge

This problem investigates a way to show in zero-knowledge that a ciphertext $c = g^m r^N \bmod N^2$ is the Paillier encryption of either $m = 0$ or $m = 1$.

The proof consists of a sequence of t rounds.

Each round has three messages.

First message (Prover $\longrightarrow$ Verifier):

> The Prover picks a random bit $m' \in \{0, 1\}$, and sends the ciphertexts $c' = g^{m'} r'^N \bmod N^2$ and $c'' = g^{1-m'} r''^N \bmod N^2$ to the Verifier: c' and c'' are Paillier encryptions of 0 and 1 in a random order.

Second message (Verifier $\longrightarrow$ Prover):

> The Verifier sends a random bit $b \in \{0, 1\}$ to the Prover.

Third message (Prover $\longrightarrow$ Verifier):

- If $b = 0$: The Prover shows that c' and c'' encrypt 0 and 1 in some order, by revealing the randomization parameters r', r'' used in their encryption.
- If $b = 1$:
  - If $m = m'$, then the Prover shows that c and c' encrypt the same message by revealing the N^{th} root of c/c'.
  - Else $m = 1 - m'$, then the Prover shows that c and c'' encrypt the same message by revealing the N^{th} root of c/c''.

(a) Completeness

Show that if c encodes $m = 0$ or $m = 1$, then the Prover always succeeds (i.e., the Verifier never fails in its check of the third message).

(b) Soundness

Show that if c does not encode $m = 0$ or $m = 1$, then the Prover will be caught with some significant probability.

(c) Zero-knowledge

Show that this protocol is ZK, by showing how the Verifier can generate transcripts on its own that have exactly the same distribution as the transcripts generated by interacting with the Prover according to the protocol above.

In all the questions, you can make any reasonable assumptions you can justify.