ICS 134 – Winter 2015: Homework 3

Name: **Student ID:**

Due date: March 13 @ noon (no extensions and no exceptions)

Submission Guidelines: Upload your homework as a **PDF file** to the class dropbox.

Warning: Homework submissions not following guidelines will not be graded.

PROBLEM 1:

Alice and Bob communicate via signed email. Alice receives three email messages from Bob: one on Tuesday morning, one Wednesday night, and one Thursday evening. Alice waits until Friday morning to read these messages, verifying their signatures in the process. All signatures check out, but Friday at noon Alice receives her weekly CRL, which includes Bob's certificate; Bob noticed that his private key was stolen and reported it on Friday at 6 am. Can Alice trust the signatures on any of Bob's messages? Why or why not?

PROBLEM 2:

An organization expects about 100 Million legitimate users to log into its system daily. What is a better strategy: store passwords using an adaptive hash (bcrypt / scrypt) or an HMAC? Why? If there is no advantage in using one over the other, explain why they are equivalent.

PROBLEM 3:

What are the implications of an organization re-using salts? That is, assume that an organization has one million users, but only generates 500,000 salts, reusing each salt value exactly once. If the reuse of salts becomes known, what does this mean (if anything) for a potential attacker? What if an attacker learns exactly which passwords are stored with the same salt?

PROBLEM 4:

Let's assume that a CA has issued a total of 1,000,000 certificates. Of these, 8192 are currently revoked. The CA uses a Certificate Revocation Tree (CRT) to represent revoked certificates.

a) What is the height of the tree?
b) How long is the "proof" (the answer to a query) that a given certificate is revoked (or not) and how many hashes would one have to perform to verify such a proof?
c) If another certificate gets revoked (or if a revoked certificate is expired), would the root of the tree need to be re-signed by the CA? Why or why not?

PROBLEM 5:

Your company has 30 fax machines and 400 employees. An employee may have one or more of the following permissions for a given fax machine: SEND FAX, STATUS and KILL. SEND FAX allows faxing, STATUS allows querying current fax queue and KILL allows removing jobs from the fax queue. If we want users to experience minimum delay when faxing (or attempting to fax), which method is best: (1) Access Control Matrix, (2) Access Control Lists or (3) Capabilities? Explain your answer.

PROBLEM 6:

Recall the so-called "Zero-Knowledge Cave". Suppose that now there are now **two locked doors** (not just one!) in the middle of the cave. Each door has a lock. Door 1 can be opened with key 1 and Door 2 – with key 2. The prover claims to have both keys. How does the zero knowledge protocol need to change to accommodate this setting? In other words, the verifier must be convinced that the prover has both keys.