Fall 2010 – CS 686 Security and Privacy
Assignment 2 - due by 11:59pm on Wednesday, Oct 27.

Problem 1: United we defend (30 points) A group of small online game companies decided to sell a group membership, so that any paid member of one online game can enjoy free membership to any other game in the "Federation". Each company now authenticates paid members by checking their usernames and passwords, and then authorizes them according to their expiration dates based on their membership fee. To facilitate these current members, the IT Lord of Federation came up with the following scheme.

All the online game companies in the Federation now share one master secret key MSK. When a paid user logs in to an online game "Alpha-life" with a username and a password, the user is prompted to store a secret file. This file contains the value of $H(MSK|\texttt{username}|\texttt{expiration date})$ and $MSK\langle\texttt{expiration date}\rangle$, where H is a secure hash function and | is a concatenation, and $\langle\rangle$ means a symmetric key encryption.

When a user tries to login another online game "Beta-revolution" by another Federation member, then the user can simply type in the username from "Alpha-life" and upload the secret file from "Alpha-life". The "Beta-revolution" can use its own MSK to decrypt the second field in the file and learn the expiration date. If the decrypted expiration date has not passed, then compute $H(MSK|\texttt{typed-in username}|\texttt{decrypted expiration date})$ and compare to the first field in the secret file. If they match, then the user is authorized to use the "Beta-revolution". Answer the following questions.

Problem 1a (5 points) Alice has a username `wonderland`, and a subscription with "Alpha-life" that expires on April 1, 2011. By coincidence, another user Carol has the same username `wonderland` with "Beta-revolution", with no paid subscription. Can Carol use Alice's secret file to login any online game in the Federation? Explain your answer.

Problem 1b (5 points) When user Alice logs into "Alpha-life", there are two ways of authenticating Alice. One way is to check her username and password stored in "Alpha-life", and the other way is to check her secret file. Modify the secret file so that "Alpha-life" can check the password of any user from "Alpha-life" based on the file alone. Explain how your modified secret file guarantees such password check. (Hint: this modified file would prevent attack described in 1a.)

Problem 1c (10 points) Imagine there is a betrayer in the Federation, "Sith-sense". This betrayer sells subscription at a half-price, so all the users would pay "Sith-sense" and other members had to honor the subscription, without being able to distinguish whether a secret file was created by "Sith-sense" or not. Modify the secret file so that good members can tell which member published each secret file. All good members can communicate with each other (1-to-1 at a time), but this channel utilizes one-time pad so it can be securely used only one time. Explain how your modified secret file facilitates the authentication of the origin of secret file.

Problem 1d (10 points) After such turmoil, "Darth"-vendor offers a free single sign-on service to the Federation. "Darth"-vendor suggests to merge all the username and password database into one location, and all the authentication requests to be served at this central login information database. For their own revenue, "Darth"-vendor will show some advertisements next to the login screen. This does seem to solve many problems that the Federation has had so far. As a member of Federation, could you present to the Council of the Federation what pros and cons there are with this central method vs. your answer 1c?

Problem 2: Online game website with PKI (20 points) When a user sets up an account, ZBoxlive.com provides a unique public and private key pair. When the user comes back to ZBoxlive.com, he sends (username, password encrypted with his private key) to the server. The website pulls the password and the public key for that user from its database and compares the decrypted password with the password stored in the database. If the two passwords match, access is granted.

Problem 2a (5 points) Describe how you can log into another user's account on ZBoxlive.com.

Problem 2b (15 points) Design an authentication scheme in which passwords are encrypted with private keys, but the attack you discovered in Problem 2a is no longer feasible.

Problem 3: Dynamic Packet Filter (20 points) Read the document at
`http://www.cisco.com/univercd/cc/td/doc/product/iaabu/centri4/user/scf4ch3.htm`.

In the summary, they conclude Dynamic Packet Filter is more secure than circuit level but less secure than application layer filter. Explain why this is true with an example attack on a certain application (i.e. web browsing, mail client, FTP client, and so on), where dynamic packet filter will not catch this attack but application layer filter will.