Midterm Examination

CS 239, Spring 2002

Answer all questions. All questions are equally weighted. The test is open book/open notes.

1. Rube Goldberg Key Exchange: Alice and Bob wish to communicate securely. (See attached figure.) They wish to use Diffie-Hellmann key exchange to establish a session key, but want to authenticate the key exchange. Alice has a public/private key pair K_{AE} and K_{AD}, a certificate issued from a particular certification hierarchy proving her identity, and the public key of KS1, the top node in the hierarchy. This certificate was issued by KS4, and, as is customary in certificate hierarchies, is signed by all nodes on the path up the tree. Bob also has a public/private key pair K_{BE} and K_{BD}, but does not yet have a certificate from the certification hierarchy. He does know KS1's public key, and he has access to a local Kerberos system (using secret key K_{BOB}, which is also known to the Kerberos server). One of the servers that works with this installation of Kerberos is KS3. KS3 will issue a certificate in the certification hierarchy to any node that obtains the proper authenticated access to KS3 via Kerberos. Bob has no other evidence sufficiently convincing to get any other node in the certification hierarchy to grant him a certificate.

   Show all messages required to set up the shared session key between Alice and Bob. Include all contents and indicate which messages (if any) are encrypted and which messages (if any) carry cryptographic authentication, showing which information must be encrypted or authenticated.

2. Add node M, Mallory's node, to the diagram used in question 1. How can Mallory cause trouble if he subverts the Kerberos server just before A and B start their Rube Goldberg Key Exchange? What if Mallory subverts KS1, instead? What if Mallory subverts KS5, instead? In each case, describe how Mallory can cause the bad effects.

3. At UCLA we have designed a system called Revere that delivers security-related information from a trusted dissemination center to very large numbers of nodes quickly, reliably, and securely. Assume that Revere could properly deliver updates to the 99.9% of all Internet nodes in a few seconds. Further assume that all Internet users have public/private key pairs, and that occasionally a user's private key is improperly revealed. One way to handle key revocation when it becomes known that a key is compromised would be to use Revere to distribute a revocation message to all nodes in the Internet for each divulged key. Critique this idea, discussing under which circumstances it would be a reasonable scheme and under which circumstances it would be unworkable.