Security Protocols

CIS-3240 Homework #5

Peter Chapin, Vermont State University

This homework covers security protocols.

1. Suppose Alice and Bob, who have never met each other, wish to share a symmetric session key securely but are not able to use any public key cryptography. Various protocols for solving this problem have been discussed in the security literature. Described below is a simple protocol that uses a trusted intermediary named Trent. In what follows the notation K_{xy} stands for a symmetric key shared by users x and y. The notation $\{M\}_{Kxy}$ stands for a message M encrypted with key K_{xy}.

   a. Alice sends a message to Trent saying *Alice, Bob* indicating that she wishes to get a session key for communication between herself and Bob.

   b. Trent generates a session key K at random and sends to Alice $\{K\}_{Kat}$, $\{K\}_{Kbt}$. Here K_{at} is a symmetric key that Alice shares with Trent (and similarly for K_{bt}). Trent has a library of these keys that has been previously set up securely.

   c. Alice decrypts $\{K\}_{Kat}$ (she now knows K) and sends a message to Bob saying *Trent, Alice,* $\{K\}_{Kbt}$. This tells Bob that Alice whishes to communicate with him and the session key has been encrypted with a key Bob shares with Trent.

   d. Bob decrypts $\{K\}_{Kbt}$ and then uses K to encrypt a message to Alice. Alice and Bob continue their communication securely using K.

   This simple protocol is quite weak. Explain how Mallory, a Dolev-Yao attacker, can trick Alice into thinking she is Bob.

2. Should trust be transitive? That is: if A trusts B and B trusts C, should A trust C? Consider the following situation among users of GPG: Alice trusts Bob to sign keys correctly and she indicates this to her GPG. Thus she will accept as valid any keys she receives that Bob has signed. Furthermore Bob trusts Carol to sign keys correctly in the same sense. Suppose Bob receives a key that Carol has signed. Since he trusts Carol he believes the key is valid and he goes ahead and signs the key himself. As a result, Alice's GPG will now accept that key as valid. Is Alice happy about this?

3. Consider the following situation: Suppose VTSU/Williston had a certificate authority (CA) that signs public keys for the VTSU/Williston community. Suppose the other campuses had similar CAs. At the state college system (VSC) level suppose that there was a certificate authority that signed the keys of the various VTSU campus CAs.

   Now suppose that Alice, a VTSU/Williston student, wishes to obtain the public key of Bob, a VTSU/Castleton student. Alice downloads Bob's key from a public key server and finds it signed by the VTSU/Castleton CA. She finds the VTSU/Castleton CA's key on the same key server and finds it signed by the VSC's CA. Furthermore the VSC CA has signed the VTSU/Willison CA's key as well. Alice has a copy of the VTSU/Williston CA's public key that she knows is correct. Should Alice trust the copy of Bob's public key? Draw a diagram representing these certificates. Is there a certificate chain from Alice's "trust root" to Bob's key? Compare this situation with that described in the previous question.

4. One method of doing "secret splitting" is to XOR a random string into the message and then give one party the random string and the other party the result of the XOR operation. Neither party knows the

secret by themselves but if they get together they can recover the secret. How might you split a secret three ways? Can you generalize your method to split a secret N ways?