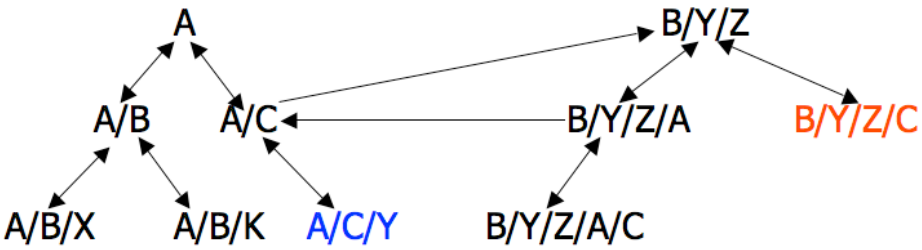
CSC 474 – Network Security

In-class exercise

Student Name:_____ Score:_____

(1) (2 points) Consider the following organization of CAs. Each node represents a CA, and a directed edge from one node to another represents that the former CA issues a certificate to the latter one. For example, the edge from A to A/C represents A has issued a certificate to A/C. Some edges are bi-directional, which represent that both CAs issue certificates to each other.



Explain how A/C/Y can verify the certificate of B/Y/Z/C? How can B/Y/Z/C verify the certificate of A/C/Y?

For A/C/Y to verify the certificate of B/Y/Z/C, it locates the chain of certificates following A/C/Y → A/C → B/Y/Z → B/Y/Z/C, and verifies the certificates following this order using public keys already verified (known or in a verified certificate).

The same process applies following the chain B/Y/Z/C → B/Y/Z → B/Y/Z/A → A/C → A/C/Y.

(2) (2 points) Explain how Kerberos deals with replay attacks?

Kerberos uses timestamps in authenticated messages to deal with replay attacks. Note that timestamps only are not sufficient.

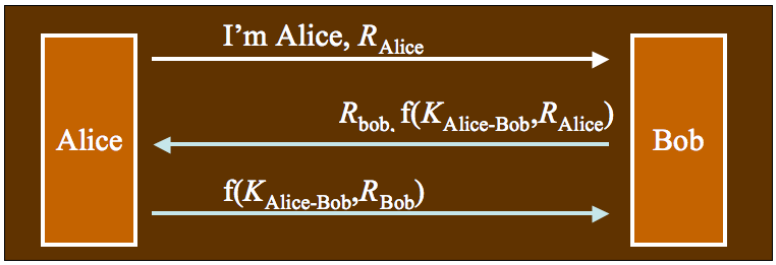
(3) (3 points) What is dictionary attack? Describe a mechanism used to mitigate dictionary attack? How and why is this mechanism effective?

Dictionary attack is an attack in which the attacker compiles words and strings commonly used as parts of a password into a dictionary and tries combinations and simple transformations of them to guess user's passwords. There are online and offline dictionary attacks. In general, offline dictionary attacks are more of a threat.

Slowing down responses to incorrect passwords can mitigate online dictionary attacks. It works because it reduces the number of passwords an attacker can try.

Password salts can be used to mitigate offline dictionary attacks. Password salts work because they increase the number of hash operations or the size of the dictionary that an attacker has to perform or store for offline dictionary attacks.

(4) (3 points) Consider the following authentication protocol. It's vulnerable to attacks.



(a) (1 point) What attack is this protocol vulnerable to?

Reflection attacks.

(b) (2 points) Explain how this attack happens.

See handouts on authentication for details. Basically, an attacker Trudy can start two parallel sessions to Bob, and use the response from Bob in the second session as her (forged) response in the first session.