CSE 303: Quiz #2

Due September 18th, 2019 at 1:35 PM

Please use the remainder of this page to provide your answer. To submit your answer, create a pdf whose name is exactly your user Id and the "pdf" extension (e.g., abc123.pdf) and email it to spear@lehigh.edu before the deadline.

Suppose that two parties, Alice and Bob, need to communicate securely, and they often say the same thing to each other. They need to be sure that nobody else can determine the contents of their communication. They also need to be sure that the other party is who she/he claims to be. Devise an encryption/signature/trust strategy for this communication, and describe it in the space provided.

For Alice and Bob to communicate it would be beneficial to make use of keys. Keys are bits of data that can be passed into an encryption function to either encrypt or decrypt a message (thus making it unreadable or readable respectively). A good method for encryption is to use RSA. This makes use of two separate keys for encrypting and decrypting. The benefit of this is that you can keep one public for others and keeps the other a secret making it easier to transfer messages without needing to share a singular key and replace it every time. RSA uses that fact that it is very hard to find two prime factors of some value n to generate keys and is thus very secure. However, since keys don't need to change when each message is sent, if Bob or Alice send the same exact message then it would encrypt to the same value, which could be a potential problem. To deal with this, it is a good idea to add a random amount of padding to each message before encrypting so that every message will at least appear unique when encrypted even if they are not.

Next, to send a message to each other, the sender would encrypt the message with the recipient's public key. This allows the receiver to know that the message was intended for that individual because only his or her private key can then be used to decrypt the message. This verifies the identity of the one receiving the message. To verify the sender is who he or she claims to be, it is best to use a signature. Signatures work by sending a digest (a fixed-size random string of bits) and along with the digest you send an encrypted version of it using your own private key. This works because the receiver can just decrypt the digest using your public key and matching the given base digest to verify that the sender must have access to the correct private key to send a good signature.

Finally, by using all of the methods described above Alice and Bob should have a fairly secure means of communication. The only additional risks that can arise are if you can not reasonably trust that the person in possession of the private keys are who they are meant to be. This can happen if one of the parties share their keys or have them stolen or if the administrator saves an incorrect or outdated public key for the individual. To deal with these problems it is best to have some additional strategies to gain the trust of each other. Examples of these are sharing something that only Bob and Alice would know, something that only Bob or Alice would have such as an ID, a unique gift, or the physical device used to send the message such as laptop or phone, something biological to Bob or Alice such as a fingerprint, or something that can be done to prove the identity such as a proof of work. To have an effective trust strategy it is best to use a combination of the above elements which is called Multi-Factor Authentication. By adding more steps to authentication it makes it much more difficult for any third parties to be falsifying their identity and making it much easier for Bob and Alice to know that it really is the person they are communicating to.