GNU Privacy Guard

Sumayyah Alahmadi sfa8135@rit.edu

CSEC.744.01

Professor Jonathan Weissman

1- how does the e-mail look in the Web browser compared to how it looks in Thunderbird? Why is this the case?

The email in Web browser was string of random alphabet (encrypted form) while in the Thunderbrid was in regular readable form. This is because the email was encrypted in both cases but web browser doesn't have the facility to decrypt the message which is why we see the email in encrypted form in the web browser. However, Thunderbrid have the mechanism to decrypt the message so that is why we were able to see the normal message because it was already decrypted in Thunderbrid.

2- When encrypting the e-mail to your partner, which key did you use?

The partner public key. Public key is available to anyone and anyone can encrypt the message but only the receiver can decrypt the message.

3- When your partner decrypted the e-mail, which key did he/she use?

His/her own private key which is known only to that partner, so no one can decrypt and see the message but him/her.

4- When signing your e-mail to your partner, which key did you use?

My Private key, the purpose of digital signature is equivalent to handwritten signature which is to authenticate the sender. Digital signature is a proof that the message was created and sent by the claimed party. Sign the message with my private key which is not available to anyone but me so that no one can sign it but me. This will assure the receiver that this message is coming from me and not someone else.

5- When your partner verified your signature, which key did he/she use?

My public key. Since my public key is available to everyone. Anyone can verify the signature and proof it is has been created and sent by me. If the receiver couldn't decrypt the message then it is a proof that this message doesn't come from claimed sender because only sender public key is a tool to verify the signature

6- How was confidentiality accomplished?

Encryption process assure confidentiality. When receiver use his/her private key to decrypt the message and read it. It is a proof that no one can read the message but the intended receiver.

7- How was integrity accomplished?

By digital signature the receiver will make sure that the mrssage has not changed during the transition. Receiver use the same hash algorithm and compare the generated hash with the received hash from the sender . if the two hashes are equal then it is proof that the message has not changed.

8- How was nonrepudiation accomplished?

Using digital signature help with non-repuiation which assuring the sender won’t deny the fact that he\she have sent the message.