IST 623 - Intro to Information Security

Homework Lab 2

Ryan Timbrook
NetID: RTIMBROO
Term: Winter, 2020
Date: 2/18/2020
Topic: Using Encryption to Enhance Confidentiality and Integrity

Table of Contents

1 Learning Objective

Learn how cryptography tools can be used to ensure message and file transfer integrity and how encryption can be used to maximize confidentiality. You will use Kleopatra, the certificate management component of GPG4Win, to generate both a public and private key as both a sender and a receiver. You will use the sender's keys to encrypt a file, send it to the receiver, and decrypt it with the receiver's copy of the keys.

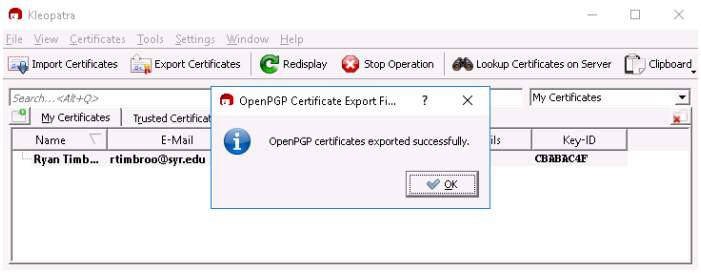
Upon completing this lab, you will be able to:

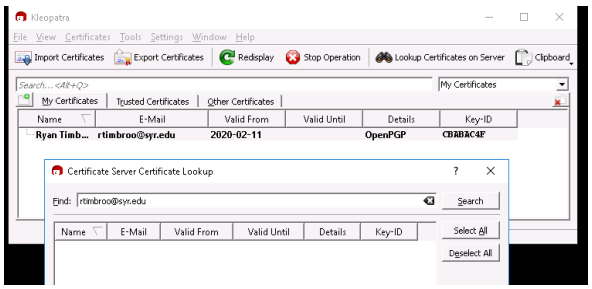
- Apply the concepts of common cryptographic and encryption techniques to ensure confidentiality.
- Understand public and private key pairs and basic asymmetric cryptography.
- Generate a public and private key pair. Upload a certificate to Directory Services server on the Internet.
- Encrypt a data message using a public and private key pair.
- Decrypt a data message using a public and private key pair.

2 Part 1: Screen Prints

2.1 Step #11

2.2 Step #17





3 Part 4: Screen Prints

Encrypt and Decrypt a File from the Sender.

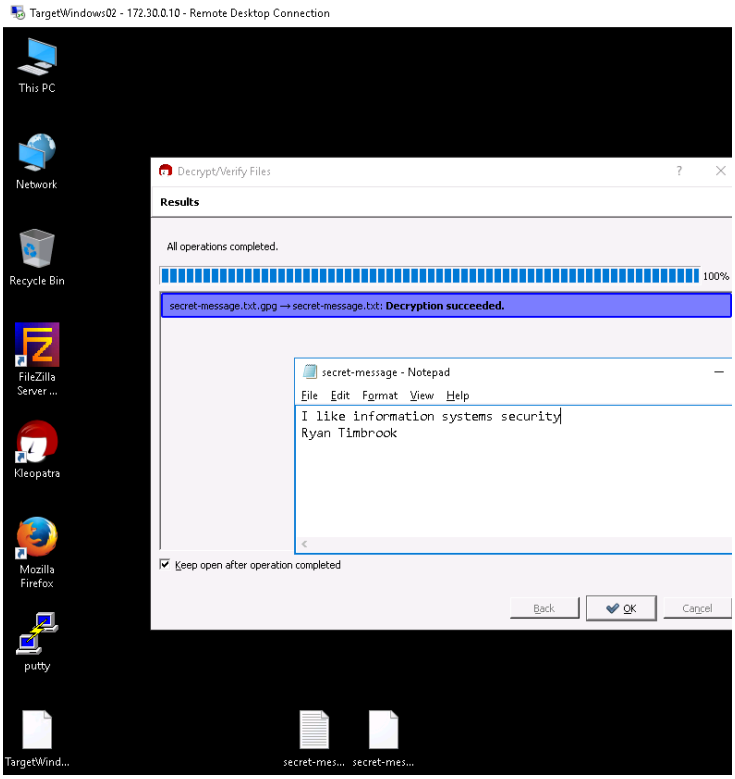
In this section, you will create a file on the vWorkstation and encrypt it using the keys created earlier in the lab. You also will transfer the file to the TargetWindows02 desktop (the receiver) and decrypt it.

3.1 Step #9 - secret-message.txt.gpg file

Submit the secret-message.txt.gpg encrypted file generated in step 9 as a deliverable for this assignment.

3.2 Step #22

Kleopatra decryption results window, the secret-message.txt file in Notepad, and the TargetWindows02 title bar.



4 Part 5: Challenge Question

Question: What is the difference and tradeoffs between X.509 and PGP certificate types?

In terms of key hierarchy, you have to request to a Certification Authority in order for them to issue you an X.509 certificate. On the other hand, you can create your own PGP. Absolute certification methods are an impossibility, because a certificate cannot certify itself. Different methods such as the directory X.509 and referral PGP methods have been proposed to deal with this situation.

Each of these deals with the basic certification question in a different way. However, for two parties in a dialogue, they share a common ground in that they depend on references which are external to the dialogue between the parties. Hence, they are called extrinsic and share common characteristics.

An X.509 certificate is defined as: The public keys of a user, together with some other information, rendered unforgeable by encipherment with the private key of the certification authority which issued it. The naming scheme used in X.509, so that it's associated with a user, the certificate allows an association between a name called "unique distinguished name" for the user and the user's public-key. Authentication relies on each user possessing a unique distinguished name. The main purpose of a CA is to bind a public key to the name contained in the certificate and thus assure third parties that some measure of care was taken to ensure that this binding is valid for both—i.e., name and key.

PGP has two parts: certification and encryption. Comparing PGP with X.509, X.509 is often times spotted as predicating a top-down trust structure that is just dictatorially imposed upon the verifier, while PGP would follow a grass-roots approach—thus more Internet-like. However, both PGP and X.509 define their central role to be played by the verifier regarding certificate acceptance, while certificate metrics is defined in both cases without any influence from the verifier. Further, both are key-transport protocols, and they depend on two types of external references: keys (quantitative) and trust (qualitative). Further still, the web-of-trust in PGP finds its parallel in the X.509 CPS, also when the issuer sets the rules and defines semantic acceptance conditions before certificate signature. The first main difference is possibly syntactic, in the sense that PGP allows certificates to be stacked up so to say as signatures upon signatures, whereas in X.509 the certificates are linked one to another as in an one-way linked-list. A second main difference is semantic, in which PGP allows an association between keys and real-world persons by web-of-trust rules, but not by transitive trust rules, whereas X.509 binds keys to names and accepts transitive trust—even though a proper CPS could also forbid transitive trust in X.509 as a function of the CA’s policies. PGP is based on an “introducer-model” which depends on the integrity of a chain of authenticators, the users themselves. The users and their keys are referred from one user to the other, as in a friendship circle, forming an authentication ring.

Homework Lab 2