CS808: Computer Security Fundamentals

3.4 Lab: OpenSSL for RSA

Using OpenSSL for RSA Encryption

Those working on Unix based systems are likely to already have OpenSSL pre-installed. You can check by opening a terminal and typing openssl. If you have it installed the terminal will display OpenSSL> before the flashing indicator for command entry to show it is ready to accept openssl commands. For a basic intro to openssl commands in linux see https://www.keycdn.com/blog/openssl-tutorial Part I

For those on Windows, it is advised you use Guacamole. Guacamole provides access to a department Linux machine through a web browser. Using a web browser, access https://guacamole.cis.strath.ac.uk/ and log in using your University DS login. Once logged in click "Linux Labs" where you will be prompted again for your login. From there, on the left hand side, select the top icon "terminal". You will then be able to follow the instructions provided. Remember to log out once you are finished.

Upon loading OpenSSL you can use the following instructions to complete encryption using the RSA algorithm.

1. First generate your RSA key pair:

genrsa –out yourkeys.pem

Recall that .pem is a container file format suitable for OpenSSL's consumption. This should create the file containing the generated keys in /home/abc12345 where abc12345 is replaced with your username

2. Now extract just the public key, where pubout indicates the extraction of the public key:

rsa -in yourkeys.pem -out yourpubkey.pem –pubout

3. Now swap your public key with a friends, we'll call them Bob for simplicity.
4. Encrypt a file with Bob's public key as follows:

rsautl –encrypt –pubin –inkey bobpubkey.pem –in /home/ abc12345/Documents/plain.txt –out cipher.txt

5. Now swap the result, and decrypt as follows

rsautl –decrypt –inkey yourkeys.pem –in cipher.txt –out decrypted.txt

It is worth noting that the rsautl command can be used to sign, verify, encrypt and decrypt data using the RSA algorithm. Recall As that direct use of RSA in its basic form is inadvisable. If making use of OpenSSL or other cryptographic libraries it is important to make sure you are fully aware of the security context to ensure proper use.

◄ 3.3: Video: RSA (10:12)

Jump to...

3.5 Article: Cryptographic randomness and one-time pads ►

CS808