Computer and Information Security

(ECE590-04, Fall 2018, Duke Univ., Prof. Tyler Bletsch)

Pointer to Homework 2

Updated 2018-09-28: Fixed a mistake; change noted with footnote.

Question 0: Accessing the Homework (0 points, but necessary)

Homework 2 is encrypted with two layers of encryption. You'll need to use both your Windows VM and a new VM pre-created for you: Kali Linux.

Accessing your Kali Linux installation

Kali Linux is a Linux distribution focused on providing a wide variety of security tools built-in (both attack and defense). Unlike most Linux distributions, Kali is intended for a single user to run commands which may operate at the kernel level, so the default user for this environment is **root**. This makes Kali powerful but dangerous to use, as the usual user-mode protections are not in place.

Because root is a well known user name, we did not want to set a login password, as these VMs are already the target of brute force login attempts from the Internet. Instead, we have established an asymmetric RSA key pair for SSH access to the root account. You can find the private and public keys created for your *sole individual use* as feedback to a Sakai dummy assignment called "Key distribution".

Use the private key to SSH as user **root** to your VM. The hostname of your VM is given in the comment at the end of your public key.

Outer layer of encryption

For the outer layer of encryption, we will use the OpenSSL cipher suite. This tool is widely available, but you'll be using the one installed on your personal Kali Linux VM. Versions of OpenSSL differ significantly, and a version mismatch can make this step fail, so be sure to use the Kali Linux VM for this part, even if you have another environment with OpenSSL installed.

The SSH keypair provided to you for logging into your Kali VM is based on the RSA algorithm, and can therefore also function as a traditional RSA key pair for asymmetric encryption/decryption in addition to SSH authentication. However, recall that RSA is much slower than symmetric cryptography, so in this step, a manually constructed *digital envelope* is employed using both your RSA keypair and a random secret key.

A 256-bit key was generated randomly for each student and then RSA-encrypted using that student's public key. This encrypted key is available as **`secret-<NETID>.key.enc`**, found in the directory linked from the course site.

Using the **`openssl rsautl`** command, decrypt this using your RSA private[1] key from the Sakai locker.

Now we can decrypt the payload, a 1MB data file available as **`<NETID>.dat`**, found in the directory linked from the course site. Use the **`openssl enc`** command to decrypt this ciphertext. Use the AES algorithm with a 256-bit key. The mode of operation should be the one that chains one block of ciphertext to the next block of plaintext using xor.

To check the result of the decryption process, the SHA1 hash of the output should be:
`6c91c71c722d4d059743d113b0810930a2cd8f4f`

Inner layer of encryption

Once you decrypt the file, copy it your Windows VM. The file is a disk image encrypted with 256-bit AES using VeraCrypt. VeraCrypt is a tool that allows one to store a read/write filesystem inside an encrypted container. Mount the volume and use the secret key to decrypt the volume. The secret key is the MAC address of the kali-vcm-01.vm.duke.edu server (152.3.53.103) written out in the standard representation (hex bytes with colon separators, e.g. "00:11:22:aa:bb:cc", lower case). You do not have access to this server but you can get network information about it using tools learned in Homework 1.

Enclosed in this volume is an HTML file that will link you to the homework.

Do not share the link with others: finding the link is part of the assignment. You may of course discuss how to perform the necessary steps with your colleagues, but please do not post or share information that short-circuits the above procedures (e.g. the inner-level encrypted file).

Be sure to unmount your encrypted volume when you are done.

[1] Updated 2018-09-28. This previously said "public", which was an error.