University of Colorado at Colorado Springs

Home Work Assignment 2
Due 03-06-01

1. Transfer your FTP server implementation to one of the Linux machines in the cluster assigned to the CS 509 class. Make the FTP server a daemon so that it runs all the time. Also, verify passwords using the /etc/shadow file. Run your daemon as root. You should do this only when you come to demo to me. Request others to login and use your server. You should delete the daemons after demo.

Write a page on how Unix passwords are encrypted and decrypted. Also, describe an approach to make the FTP process secure. You may have to implement this in the future.

2. Team Project: Each one of you, find a friend and form teams of two people. Each team will install a password cracker on one of the Linux machines. Try breaking the passwords in the /etc/shadow file for the Linux server in the cluster of machines assigned to our class. Understand how this password cracker works and write a paragraph or two on it. Discuss its merits and drawbacks.

You will briefly present the cracker to the class. Each group should try to install separate crackers.

3. Perform an implementation of the Vigenère cipher. Implement Kasiski and Friedman tests to break this cipher. Now, try breaking the following two codes. Please, neither accept help from anyone nor help anyone in breaking the code. Grading will be based on what you can do! They are both potentially hard.

   (a) The code given below.

   | K W C S S | G X Y U T | Z B Z W U | D X Y Y J |
   | N P R P W | O P V J J | J X V L L | T B Y U L |
   | V O Z P W | I K Z J Z | Z Z K Y P | O T V N L |
   | Z Z D U Q | M M G L W | N M E N E | J Z V N Z |
   | V V F H W | K T R C F | O M O N D | Z B K Y J |
   | C W N Y N | Z Z N Y E | P A K H G | O N F L Y |
   | Z B K B S | O E V H W | Z L K B W | X Q G B W |
   | M B V R L | O W U Y L | Z Z D C F | Z B Y Y U |
   | G M R L L | Z F K Q F | D Y L Y D | T E V W S |
   | I V F N X | J Z V R S | H X C Y Z | V D V U F |
   | V T X I J | D B Y G A | I E Y C U | C I T C H |
   | C M I N W | S B O L W | K Z V M W | I B J Y A |
   | O P V L H | G I Z H L | Z F K Y G | M A N C L |


(b) During the American Civil War (1860-1865), one of the reasons the Confederates lost is that the Union was able to break a whopping 90% of the South’s messages and report to President Lincoln. The South used the Vigenère cipher with only three possible keywords that varied from message to message. For example, Grant’s troops intercepted a message on eight captured Southern soldiers at Vicksburg trying to slip into Vicksburg with 200,000 percussion caps.

Lieutenant General Pemberton: My XAFV. USLX WAS VVUFLSJP by the BR-CYAJ. 200000 VEGT. SUAJ. NERP. ZIFM. It will be GFOECZOD as they NTYMNX. Bragg MJTPHINZG a QRCMKBSE. When it DDZGJX. I will YOIG. AS. QHY. NITWM do you YTIAM the IIKM. VFVEY. How and where is the JSQMLGUGSFTVE. HBFY is your ROEEL.

J. E. Johnston.

There are no hyphens in the actual text. You will give me the cleartext if you can break the code. Otherwise, let me know in writing how far you were able to go. You will demo what you have been able to do.

4. We will continue with our implementation of the Secure Electronic Transaction (SET) protocol. As you know, it is very complicated and hence, we will take things slow and move along making sustained progress along the way.

We will now deal with the manner in which interaction between any two parties proceeds in SET. Let the two parties be called Alice and Bob. Alice initiates the communication, and Bob receives it. In other words, Alice encrypts her message, and Bob decrypts the message he receives from Alice.

There are several keys involved: one symmetric key for encrypting the actual data, also called property description; two pairs of public-private keys, one pair for signature (called public-private signature keys), and another pair for exchanging public keys (called public key-exchange key). There are also a couple of certificates involved: one for Alice and another for Bob. We will deal with certificate issuance later.

For the time being, we will assume that all encryption is symmetric or private key based. The symmetric encryption algorithm of choice, at the current time, is the Vigenère cipher.

The Encryption Process: The encryption process at Alice’s end is shown below.
E₁: Alice runs her data or property description through an 1-way algorithm, a hash, to produce a unique value known as the message digest. This is a kind of digital fingerprint of the data and will be used to test the integrity of the message.  

At this time, since we do not know how a hash is implemented, compute the message digest to be simply a parity bit. I have requested Dave Lohmann, our esteemed systems administrator, to install several message digest modules in Perl on the cs and other machines. The digest modules are Digest::MD2, Digest::MD4, Digest::MD5, Digest::SHA1. I will let you know if he is able to install them in the next few days. I will request you to give a choice of these algorithms if they are installed soon.

E₂: Alice then encrypts the message digest with her private signature key to produce the digital signature.  

For the time being, let this encryption be done using a Vigenère cipher. The key used is a private key although it is a symmetric key and is not an asymmetric key, as it should be according to the SET standards.

E₃: Next, Alice generates a random symmetric key and uses it to encrypt the property description, her signature and a copy of her certificate. The certificate contains her public signature key. In order to decrypt the property description, Bob will require a secure copy of the random symmetric key.  

For the time being, let the random symmetric key to be a Vigenère key. Let the certificate contain another Vigenère key for the time being. The certificate also contains a participant’s name; and, two dates: beginning date and expiration date in YYYYMMDD format.

E₄: Bob’s certificate, which Alice must have obtained prior to initiating secure communication with him, contains a copy of his public key-exchange key. To ensure secure transmission of the symmetric key, Alice encrypts it using Bob’s public key-exchange key. The encrypted key, referred to as the digital envelope, is sent to Bob along with th encrypted message itself. Assume that the certificates are exchanged securely, say, by hand or by certified surface mail.

E₅: Finally, Alice sends a message to Bob consisting of the following: the symmetrically encoded data or property, signature and certificate, as well as the asymmetrically encrypted symmetric key.

The Decryption Process: The decryption process at Bob consists of the following steps.

D₁: Bob receives the message from Alice and decrypts the digital envelope with his private key-exchange key to retrieve the symmetric key.

D₂: Bob uses the symmetric key to decrypt the property description, Alice’s signature and her certificate.

D₃: He decrypts Alice’s signature with her public signature key, which he acquires from her certificate. This recovers the original message digest of the property description.

D₄: He runs the property description through the same one-way algorithm used by Alice and produces a new message digest of the decrypted property description.

D₅: Finally, he compares his message digest to the one obtained from Alice’s digital signature. If they are exactly the same, he confirms that the message content has not been altered during transmission and that it was signed using Alice’s private signature key.
If they are not the same, then the message either originated somewhere else or was altered after it was signed. In that case, Bob takes some appropriate message such as notifying Alice of discarding the message.

Implement the encryption and decryption processes as two modules or packages. Instantiate them for each of the participants in SET. Store all code and data for each of the participants in a separate directory.

Describe salient details of your implementation in a write-up between one and two pages long. You will have to demo the code to me.