Computer Security Assignment 2

Venkatesh Viswanathan - vviswana - 50290589

21st September 2018

1 Expression for Encryption and Decryption Modes

1.1 Expression for Encryption and Decryption Modes in CFB mode

CFB mode is the Cipher FeedBack mode.

Expression for CFB mode encryption of a stream cipher

$I_i = LSB(IV_{i-1}||C_{i-1})$
$X_i = E(K, I_i)$
$C_i = m_i \oplus S_r(X_i)$
$C_i = m_i \oplus S_r(E(K, I_i))$
$C_i = m_i \oplus S_r(E(K, LSB(IV_{i-1}||C_{i-1})))$

The above are the equations for CFB encryption mode. The following are the definitions for the symbols

LSB - Least Significant Bit
IV - Initialization Vector
C - Cipher Text
m -Message
E(K,I_i) - Initialization Vector is encrypted with Key K.
$S_r(X_i)$ - Most Significant r bits of X_i

Expression for CFB mode decryption of a stream cipher

$I_i = LSB(IV_{i-1}||P_{i-1})$
$X_i = E(K, I_i)$
$P_i = C_i \oplus S_r(X_i)$
$P_i = C_i \oplus S_r(E(K, I_i))$
$P_i = C_i \oplus S_r(E(K, LSB(IV_{i-1}||P_{i-1})))$

The above are the equations for CFB encryption mode. The following are the definitions for the symbols

LSB - Least Significant Bit
IV - Initialization Vector
C - Cipher Text
P_i - Plain Text
E(K,I_i) - Initialization Vector is encrypted with Key K.
$S_r(X_i)$ - Most Significant r bits of X_i

1.2 Expression for Encryption and Decryption Modes in OFB mode

OFB mode is the Output FeedBack mode.

Expression for OFB mode encryption of a stream cipher

$I_i = LSB(IV_{i-1}||S_r(X_{i-1}))$
$X_i = E(K, I_i)$
$C_i = m_i \oplus S_r(X_i)$
$C_i = m_i \oplus S_r(E(K, I_i))$
$C_i = m_i \oplus S_r(E(K, LSB(IV_{i-1}||S_r(X_{i-1}))))$

The above are the equations for OFB encryption mode. The following are the definitions for the symbols

LSB - Least Significant Bit
IV - Initialization Vector
C - Cipher Text
m 0.9cm-Message
E(K,I_i) - Initialization Vector is encrypted with Key K.
$S_r(X_i)$ - Most Significant r bits of X_i

Expression for OFB mode decryption of a stream cipher

$I_i = LSB(IV_{i-1}||S_r(X_{i-1}))$
$X_i = E(K, I_i)$
$P_i = C_i \oplus S_r(X_i)$
$P_i = C_i \oplus S_r(E(K, I_i))$
$P_i = C_i \oplus S_r(E(K, LSB(IV_{i-1}||S_r(X_{i-1}))))$

The above are the equations for CFB encryption mode. The following are the definitions for the symbols

LSB - Least Significant Bit
IV - Initialization Vector
C - Cipher Text
P_i - Plain Text
E(K,I_i) - Initialization Vector is encrypted with Key K.
$S_r(X_i)$ - Most Significant r bits of X_i

2 Cryptographic Hashing And Digital Signatures

2.1 Cryptographic Hashing

Alice finds an algorithm and publishes only the digest of the algorithm in a newspaper, 15 years later when the algorithm is to be discovered again, can she convince the judge that the algorithm was already discovered 15 years ago by her is the question.

No,Alice cannot prove to the judge that she was the one who found it 15 years ago.The explanation goes as such.

A cryptographic hash function is a hash function which takes an input (or 'message') and returns a fixed-size alphanumeric string. The string is called the 'hash value' or the 'message digest'.

The ideal hash function has three main properties:

1)It is extremely easy to calculate a hash for any given data.
2)It is extremely difficult to calculate an alphanumeric text that has a given hash that is Hashing is irreversible.
3)It is extremely unlikely that two slightly different messages will have the same hash that is Hashing is unique enough but not entirely unique.

What Alice cannot prove here is that she is the one has published the hash in the newspaper.A third party member can claim that they were the one who published it having a different input that maps to the same hash value although this is extremely and computationally difficult.

This kind of a attack on Hashing is called as the **Collision Resistance Attack.**A good hashing algorithm should be hard to find two different inputs that output to the same hash value that is, two inputs a and b such that
H(a) = H(b) but a not equal to b.

Finding such an input pair that maps to the same hash value is extremely difficult.Every hash function with more inputs than outputs will necessarily have collisions.Consider SHA-256 that produces 256 bits of output from a large input. Since it must generate one of 2^{256} outputs for each member it is clear that some inputs will hash to the same output. **Collision resistance does not mean that no collisions exist but they are hard to find.There have been incidents where hashing Algorithm MD5 has been broken.A 2013 attack by Xie Tao, Fanbao Liu, and Dengguo Feng breaks MD5 collision resistance in 2^{18} time. This attack runs in less than a second on a regular computer.**

The birthday paradox also supports this that if a hash function produces N bits of output the attacker need to compute only $2^{N/2}$ hash operations for random input and he is supposed to find a matching input. Hence to conclude this problem, Alice **cannot justify** that she was the one who published the digest in the newspaper as a third party member might claim it with a different input although it takes 2^{128}(in case if the hashing algorithm is SHA-256) computations to find a input that outputs to the same hash value.

2.2 Digital Signatures

Can Alice prove if a Digital Signature was released instead of a Hash?

Yes, Alice can prove if a Digital Signature was released instead of a Hash. A digital signature is a mathematical technique used to validate the authenticity and integrity of a message.Digital Signatures are based on public-key cryptography such as RSA where we generate a public and a private key.The general working of a digital signature is that when a signer electronically signs a document, the signature is created using the signer's private key, which is always securely kept by the signer.Then a hash is created by the signing algorithm and encrypting that hash. The resulting encrypted hash is the digital signature. The signature is also marked with the time that the document was signed. If the document changes after signing, the digital signature is invalidated.

Consider Alice has released a digital signature(encrypted hash in a journal) that was encrypted with her private key. After 15 years, alice can prove that she was the one who found it because only she can decrypt it using her public key. No other third party can decrypt because their public key cannot decrypt the hash and hence Alice **can justify** to the judge that she was the one who found it 15 years ago. The reason for encrypting the hash instead of the entire message or document is that a hash function can convert an arbitrary input into a fixed length value, which is usually much shorter. This saves computaional time.

3 Attack On Public-Key Cryptography

3.1 Information that can be obtained by Eve

Considering RSA, I will generalise it to a public-key cryptography.The general idea of a public-key cryptography is that a message encrypted with the public key P can only be decrypted with the private key K.

In RSA, the public keys are n and e. If eve changes these 2 keys, she can decrypt all the messages sent between Alice and Bob.Here n is $p*q$ where p and q are two prime numbers and e is a coprime number to totient(n). totient(n) = (p-1)(q-1).

Consider Alice and Bob have their own seperate private keys and their own public keys. Their public keys are placed on a file in a server for which Eve has an access to that file. So potentially Eve has Alice and Bob's public keys.

The normal flow will be that if Alice has to send a message to Bob, Alice will encrypt the plain text using her public key and send it to Bob which Bob will decrypt it using his private key. Now Consider Eve is in the middle of this and has access to both their public keys.

1) Eve replaces Alice and Bob's public keys with two other public keys. So now she has altered the file to have her own public keys.

2) Alice now wants to send a message to Bob and she encrypts the plain text with the public key present in the file.(She thinks that this is the public key of Bob, but indeed it is the public key of Eve.)

3) Now Eve can decrypt the message using her private key and hence she can have access to the messages that are sent between Alice and Bob. This kind of a attack is called as the Man in the Middle Attack.

4)Furthermore, Eve can send forged/fake messages to Bob as Eve has Bob's public key as well.

3.2 Detecting Eve's subversion of the keys

The question here is can Alice and Bob find that Eve has changed their public keys. Alice sends a message using Eve's public key unknowingly as stated earlier. Eve can decrypt the message and she can send her own message to Bob with Bob's public key. In this case, Bob will not get a garbage value while decrypting the message and hence Alice and Bob cannot find that Eve is doing a Man in the Middle attack.

Also there is also another important factor called as the **Public Key Certificate.**A public key certificate is a digitally signed document that serves to validate the sender's authorization and name. The document consists of a specially formatted block of data that contains the name of the certificate holder (which may be either a user or a system name) and the holder's public key, as well as the digital signature of a certification authority for authentication. Using this factor, both Alice and Bob can find if Eve is in the middle.

But if Eve unknowingly sent the same message that was sent by Alice, to Bob, then while decrypting Bob will get a garbage value because the message sent by Alice was encrypted with Eve's public key and not Bob's.

For a clearer version, I would like to give an example.
Consider X and Y are the public keys of Alice and Bob respectively.
Eve replaces U and V instead of X and Y in the file.
Alice sends a message M using the public key of Bob(which is corrupted now, it should have been Y but it is corrupted as V).
Eve can easily decrypt the message M using her private key and can send a forged message F to Bob with Bob's public key Y.In this case,both Alice and Bob cannot find that Eve has changed their public Keys.
Instead of sending the forged message F, if Eve sends the message M that was encrypted with the public Key V, then Bob cannot decrypt with his private key or he will get some garbage value because of a different public-private key pair.In such a case, Bob and Alice can find that their public keys were altered by someone.

Example

- Alice Public Key = X and Bob Public Key = Y
- Eve replaces x by u and y by v
- Alice's Corrupted Public key = U and Bob's Corrupted Public key = V
- Alice encrypts a message M = "My Account Number 12345" using V to output ciphertext C.
- C is received by Eve and not Bob because M was encrypted with V and not with Y.

- Eve can decrypt ciphertext C by using her private key.
- Eve now alters the message M into F as F = "My Account Number 98765" and sends F to Bob. She had encrypted F with Y, Bob'public key.
- Bob can decrypt it using his private key and can retrieve F . Now Bob can find that Eve has altered the message using a public-key certificate, Both Alice and Bob can find if Eve is in the middle.

Using a public-key certificate, Both Alice and Bob can find if Eve is in the middle.

4 Why Cryptosystems Fail

4.1 Security of computer systems and it's Evolution

Security had major evolution after world war 2. Before World war 2, security(cryptography) was handled by the government bureaucrats. They were reluctant to accept their failures and hence incidents such as the British Navy codes were cracked by the German. So after the 2nd world war, cryptography was taken over by cryptosystem engineers.

4.2 Building and Operating Secure Systems

The paper clearly states that Implementing secure computer systems using the available encryption products is beyond most organization's' capabilities currently.The flaw in building a secure system happens in many places such as it might the vendor's mistake or the equipment designers mistake or even at the application level.It also suggests 2 methods to tackle such problems, one is to have a certification for the human work involved and the other is a system level approach to designing and evaluating security.The paper also states that the vendor's to train the people who work at the application level to manage the system. It also doesnt want security products to be certified under ITSEC unless the manufacturer can show that both the system factors and the human factors have been properly considered.

4.3 Main proposal of the paper

The main proposal of the paper is to site the various failure models of banking systems.It turns out that the threat model commonly used by cryptosystem designers was wrong: most frauds were not caused by cryptanalysis or other technical attacks, but by implementation errors and management failures. The paper also suggests a new paradigm shifts in cryptography.

4.4 Security in Banking-then and now

There has been a huge amount of change in terms of security in banking sectors then and now. The ATM frauds that were given as examples are reduced to a minimum now as the general public are aware about the Skimmer machines and fraudulent keypads. Moreover all transactions are immediately notified to us by either our email or through our SMS. Regarding the other protection mechanisms, even when we transfer money online we are sent a one time message to our registered account to check as an additional security. Such has been the importance given to security in banking sector now a days.

4.5 Security in other industries to Banking sectors

Security in banking sectors is much more important compared to other industries. Incidents of a single man who looted almost a million dollars from a bank in USA from a home system has been reported.The consequences are much more when a security failure happens in a banking sector and it affects many lives wheras when a security failure happens in a social media only a few persons are affected. Considering this, Security is important in all industries but it is more important when banks are involved.

5 References

https://searchsecurity.techtarget.com/definition/digital-signature
https://en.wikipedia.org/wiki/Collision_resistance
https://simple.wikipedia.org/wiki/Cryptographic_hash_function
https://security.stackexchange.com/questions/12066/can-i-detect-a-mitm-attack—
https://www.protectimus.com/blog/mitm-prevention-and-detection
https://searchsecurity.techtarget.com/definition/public-key-certificate