Abstract: Preventing unauthorized access to corporate information systems is essential for many organizations. Communication security is one of the major area of interest. The data used in communication is very sensitive and needs to be protected and made abstract from intruders of system. The recent branch of network security is Cryptography using Elliptic Curve Architectures which is based on the arithmetic of elliptic curves and discrete logarithmic problems. ECC schemes are public-key based mechanisms that provide encryption, digital signatures and key exchange algorithms. The best known encryption scheme is the Elliptic Curve Integrated Encryption Scheme (ECIES) which is included in IEEE and also in SECG SEC 1 standards.

Keywords - Encryption, Decryption, Authentication, Cryptography

I. INTRODUCTION

Cryptography
Cryptography is a cornerstone of the modern electronic security technologies used today to protect valuable information resources on intranets, extranets, and the Internet. Cryptography is the science of providing security for information.

Objectives of Cryptography
The objective of cryptography-based security is to protect information resources by making unauthorized acquisition of the information or tampering with the information more costly than the potential value that might be gained. Because the value of information usually decreases over time, good cryptography-based security protects information until its value is significantly less than the cost of illicit attempts to obtain or tamper with the information. Good cryptography, when properly implemented and used, makes attempts to violate security cost-prohibitive.

Another objective of all information security systems, including cryptography-based security systems, is to protect information resources at less cost than the value of the information that is being protected. A cryptography-based security system must provide information security at acceptable costs. Determining acceptable costs involves weighing the cost of the security versus the benefits of the security.

Basic Terms Used in Cryptography

Encryption
A process of the original message into an unreadable form is known as Encryption. A process of converting Plain Text into Cipher Text is called as Encryption. Cryptography uses the encryption technique to send the confidential information over an channel. The process of encryption requires two things - an encryption algorithm and a key. An encryption algorithm means the technique that has been used in encryption. Encryption takes place at the sender side. Encryption Algorithm is used to make content unreadable by all but the intended receivers.

\[ \text{Encrypt(plaintext, key)} = \text{ciphertext} \]

\[ \text{Decrypt(ciphertext, key)} = \text{plaintext} \]

Decryption
A reverse process of encryption is called as Decryption. It is a process of converting Cipher Text into Plain Text. Cryptography uses the decryption technique at the receiver side to obtain the original message from non readable message (Cipher Text). The process of decryption requires two things- a Decryption algorithm and a key. A Decryption algorithm means the technique that has been used in Decryption. Generally the encryption and decryption algorithm are same.

- Security Functions of Cryptography
Cryptography is most often associated with the confidentiality of information that it provides. However, cryptography can offer the following four basic functions:

Confidentiality Assurance that only authorized users can read or use confidential information. For example, unauthorized users might be able to intercept information, but the information is transmitted and stored as cipher text and is useless without a decoding key that is known only to authorized users.

Authentication Verification of the identity of the entities that communicate over the network. For example, online entities can choose to trust communications with other online entities based on the other entities ownership of valid digital authentication credentials.
Integrity Verification that the original contents of information have not been altered or corrupted. Without integrity, someone might alter information or information might become corrupted, and the alteration could be undetected. For example, an intruder might covertly alter a file, but change the unique digital thumbprint for the file, causing other users to detect the tampering by comparing the changed digital thumbprint to the digital thumbprint for the original contents.

Nonrepudiation Assurance that a party in a communication cannot falsely deny that a part of the actual communication occurred. Without nonrepudiation, someone can communicate and then later either falsely deny the communications entirely or claim that it occurred at a different time. For example, without nonrepudiation, an originator of information might falsely deny being the originator of that information. Likewise, without nonrepudiation, the recipient of a communication might falsely deny having received the communication.

II. TYPES OF CRYPTOGRAPHIC ALGORITHMS

There are several ways of classifying cryptographic algorithms. In this paper, they will be categorized based on the number of keys that are employed for encryption and decryption. The three types of algorithms are:
1) Secret Key (Symmetric) Cryptography (SKC): Uses a single key for both encryption and decryption.
2) Public Key (Asymmetric) Cryptography (PKC): Uses one key for encryption and another for decryption.
3) Hash Functions: Uses a mathematical transformation to irreversibly "encrypt" information.

1) Secret Key Cryptography uses the same key for encrypting and decrypting the message.

Plaintext \[\rightarrow\] Ciphertext \[\rightarrow\] Plaintext

2) Public Key Cryptography uses two keys, one for encryption and one for decryption

Plaintext \[\rightarrow\] Ciphertext \[\rightarrow\] Plaintext

3) Hash functions use no key

Plaintext \[\rightarrow\] Ciphertext

III. ELLIPTIC CURVE CRYPTOGRAPHY

Elliptic Curve Cryptography (ECC) is a public key cryptography. In public key cryptography each user or the device taking part in the communication generally have a pair of keys, a public key and a private key, and a set of operations associated with the keys to do the cryptographic operations. Only the particular user knows the private key whereas the public key is distributed to all users taking part in the communication. Some public key algorithm may require a set of predefined constants to be known by all the devices taking part in the communication. 'Domain parameters’ in ECC is an example of such constants. Public key cryptography, unlike private key cryptography, does not require any shared secret between the communicating parties but it is much slower than the private key cryptography.

The mathematical operations of ECC is defined over the elliptic curve \(y^2 = x^3 + ax + b\), where \(4a^3 + 27b^2 \neq 0\). Each value of the ‘a’ and ‘b’ gives a different elliptic curve. All points \((x, y)\) which satisfies the above equation plus a point at infinity lies on the elliptic curve. The public key is a point in the curve and the private key is a random number. The public key is obtained by multiplying the private key with the generator point \(G\) in the curve. The generator point \(G\), the curve parameters ‘a’ and ‘b’, together with few more constants constitutes the domain parameter of ECC. One main advantage of ECC is its small key size. A 160-bit key in ECC is considered to be as secured as 1024-bit key in RSA.

A. ECDSA - Elliptic Curve Digital Signature Algorithm

For authenticating a device or a message sent by the device, Signature algorithm is used. For example consider two devices A and B. To authenticate a message sent by A, the device A signs the message using its private key. The device sends the message and the signature to the device B. This signature can be verified only by using the public key of device A. Since the device B knows A's public key, it can verify whether the message is indeed sent by A or not. ECDSA is a variant of the Digital Signature Algorithm (DSA) that operates on elliptic curve groups. For sending a signed message from A to B, both have to agree on an Elliptic Curve domain parameters. The domain parameters are defined in section Elliptic Curve Domain parameters. Sender A have a key pair consisting of a private key \(d_A\) (a randomly selected integer less than \(n\), where \(n\) is the order of the curve, an elliptic curve domain parameter) and a public key \(Q_A = d_A * G\) (\(G\) is the generator point, an elliptic curve domain parameter). An overview of ECDSA process is defined below.[3]

**Signature Generation**

For signing a message \(m\) by sender A, using A's private key \(d_A\)

1. Calculate \(e = HASH (m)\), where HASH is a cryptographic hash function, such as SHA-1
2. Select a random integer \(k\) from \([1, n - 1]\)
3. Calculate \(r = x_1 (mod\ n)\), where \((x_1, y_1) = k * G\). If \(r = 0\), go to step 2
4. Calculate \(s = k^{-1}(e + d_Ar)(mod\ n)\). If \(s = 0\), go to step 2
5. The signature is the pair \((r, s)\)

**Signature Verification**

For B to authenticate A's signature, B must have A's public key \(Q_A\)
1. Verify that r and s are integers in \([1,n-1]\). If not, the signature is invalid.
2. Calculate \(e = \text{HASH}(m)\), where \(\text{HASH}\) is the same function used in the signature generation.
3. Calculate \(w = s^{-1} \mod n\).
4.Calculate \(u_1 = ew \mod n\) and \(u_2 = rw \mod n\).
5. Calculate \((x_1, y_1) = u_1G + u_2Q_A\).
6. The signature is valid if \(x_1 = r \mod n\), invalid otherwise.

B. ECDH - Elliptic Curve Diffie Hellman

ECDH is a key agreement protocol that allows two parties to establish a shared secret key that can be used for private key algorithms. Both parties exchange some public information to each other. Using this public data and their own private data these parties calculate the shared secret. Any third party, who doesn't have access to the private details of each device, will not be able to calculate the shared secret from the available public information. An overview of ECDH process is defined below. For enabling a shared secret between A and B using ECDH, both have to agree up on Elliptic Curve domain parameters. The domain parameters are defined in section Elliptic Curve Domain parameters. Both end have a key pair consisting of a private key \(d\) (a randomly selected integer less than \(n\), where \(n\) is the order of the curve, an elliptic curve domain parameter) and a public key \(Q = dG\) (G is the generator point, an elliptic curve domain parameter). Let \((d_A, Q_A)\) be the private key - public key pair of A and \((d_B, Q_B)\) be the private key - public key pair of B.

1. The end A computes \(K = (x_K, y_K) = d_A * Q_B\).
2. The end B computes \(L = (x_L, y_L) = d_B * Q_A\).
3. Since \(d_AQ_B = d_Bd_AG = d_Ad_BG = d_BQ_A\). Therefore \(K = L\) and hence \(x_K = x_L\).
4. Hence the shared secret is \(x_K\).

Since it is practically impossible to find the private key \(dA\) or \(dB\) from the public key \(K\) or \(L\), its not possible to obtain the shared secret for a third party.

C. Elliptic Curve Integrated Encryption System (ECIES)

Integrated Encryption Scheme (IES) is a hybrid encryption scheme which provides semantic security against an adversary who is allowed to use chosen-plaintext and chosen-ciphertext attacks. The security of the scheme is based on the Diffie–Hellman problem. The elliptic curve integrated encryption system (ECIES) is the standard elliptic curve based on encryption algorithm. It is called integrated, since it is a hybrid scheme that uses a public key system to transport a session key for use by a symmetric cipher. ECIES is a public-key encryption algorithm. [11]

To send an encrypted message to Bob using ECIES Alice needs the following information:

- cryptographic suite to be used:
  - KDF
  - MAC
  - symmetric encryption scheme E
- EC domain parameters \((p, a, b, G, n, h)\) for a curve over prime field or \((m, f(x), a, b, G, n, h)\) for a curve over binary field;
- Bob's public key: \(K_B\) (Bob generates it as follows: \(K_B = K_BG\), where \(K_B\) is the private key he chooses at random: \(K_B \in [1, n-1]\).)
- optional shared information: \(S_1\) and \(S_2\).

To encrypt a message \(m\) Alice does the following:

1. generates a random number \(r \in [1,n-1]\) and calculates \(R = rG\).
2. derives a shared secret: \(S = P_r\), where \(P_r = (P_x, P_y) = rK_A\) (and \(P \neq 0\)).
3. uses KDF to derive a symmetric encryption and a MAC keys: \(K_E || K_M = \text{KDF}(S || S_1)\).
4. encrypts the message: \(c = E(K_E; m)\).
5. computes the tag of encrypted message and \(S_2: d = \text{MAC}(K_M; c || S_2)\); outputs \(R || c || d\).

To decrypt the ciphertext \(R || c || d\) Bob does the following:

1. derives the shared secret: \(S = P_r\), where \(P_r = (P_x, P_y) = K_BR\) (it is the same as the one Alice derived because \(P = K_BR = K_BRG = rK_BG = rK_B\), or outputs failed if \(P = 0\).
2. derives the key same way as Alice did: \(K_E || K_M = \text{KDF}(S || S_1)\).
3. uses MAC to check the tag and outputs failed if \(d \neq \text{MAC}(K_M; c || S_2)\).
4. uses symmetric encryption scheme to decrypt the message \(m = E^{-1}(K_E; c)\).

IV. CONCLUSION

Wireless devices are rapidly becoming more dependent on security features such as the ability to do secure email, secure Web browsing, and virtual private networking to corporate networks, and ECC allows more efficient implementation of all of these features. ECC provides greater security and more efficient performance than the first generation public key techniques. Even though ECIES provides some valuable advantages over other cryptosystems as RSA, the number of slightly different versions of ECIES included in the standards may obstruct the adoption of ECIES.

REFERENCES


