Computer Networks Project title

**Introduction:**

Internet has become more dependable factor in today’s life where data is transmitted and stored. Every individual and organisations reply on the data which is communicated over internet and any sort of network. The evolution of internet has given users a means to access information in many ways like emails, any chat applications etc. Late on, organisations realised that this could lead them the way to reach their customer for business when enough bandwidth is available. But the big concern here is, to what level the data is secure over the internet. The awareness increased about the data security over various network attacks when data is stored or in transmission. So protecting data from unauthorized access became one of the critical objectives of the information technology. Security concerns kept on rising due to the fast growth of internet, complicated inter-networks, user authentication, violation of the so called security pillars such as authentication, integrity, identification, non-repudiation, availability,, confidentiality, privacy. E-commerce became the major victim for network attacks where the attacker can hijack user credit card information or any sort of banking related processing which in turn affect the firms losing customers along with billions of dollars in revenues. It has been reported that in last few years, many organisations,who stores and maintains user’s confidential and private data has been stolen by breaking the networks(Kapoor *et al.* 2011).

**Cryptography:**

Cryptography deals with making the data discrete for others. It involves a method of secret writing which is known as Cipher, where a plaintext is converted into encrypted text which is referred as cipher-text. The process of data transformation from plaintext to cipher-text is known as Encryption and the reverse of this process in which cipher-text is converted into plaintext is called Decryption. These two processes are controlled by cryptographic algorithms which generates various cryptographic keys(Rob n.d.)(Ganley 2006).

To encounter this reversible process (encryption and decryption), there is a science hidden to break cryptographic security and it is called as Cryptanalysis(Eskicioglu and Litwin 2001).

The fig.5 shows is simple demonstration in cryptographic process in which the eavesdropper have access to the cipher text and still he cannot unwrap the text to see the original content of it. Diagram

Description automatically generated

Figure 5: Block diagram of the Cryptographic system(Eskicioglu and Litwin 2001)

The comprehensive study of a scientific and mathematical method for creating secret codes that meet certain security standards, such as secrecy, authentication, and more, is known as cryptography.

Privacy: This security feature makes sure that only the intended recipient may read the data.

Authentication is the process of establishing the sender's or receiver's identity as part of a security service.

Data Integrity is a security service that informs the recipient of any unauthorized data alteration.

Non-repudiation: A security service that disputes an activity that was already committed. In other words, it is a method for demonstrating that the communication was transmitted.

**Importance of Cryptography:**

There are lot of instances where user data has been stolen by security breach ending up losing the sensitive data. A recent case which got highlighted where RIM(Research in motion) was requested by Government which is used BlackBerry cellular device firm to share the encryption algorithm. But RIM denied the request to share the encryption algorithm. This indicates that the encryption is such a powerful and critical cryptographic technology in today’s means of communication(Schmeh 2006).

Let's use the example below to show why encryption is necessary. Alice and Bob are corresponding with each other over email or chat. Assume that this conversation is being carried out by a phony. The security risks posed by Mallory that may be avoided by utilizing cryptographic encryption are listed below.Diagram

Description automatically generated

Figure 6: Imposter intercepting the data(Schmeh 2006)

Mallory has the ability to influence intercepted data, change sent data covertly, and maintain communication with Alice while posing as Bob.

Alice can accuse Mallory of forging her communication even if she is undetected.

However, Mallory is capable of doing actions that are challenging to stop using cryptographic techniques.

Mallory is able to change messages (But detection cannot be avoided by him)

Data interception is unlikely if it is properly encrypted, but he may use other methods to obstruct communication, including blowing up a data center or shutting off routers (In this case he would be rarely can access the data)

Cryptography is crucial to protect all forms of communication, including emails, web pages, and telnet commands sent over the internet, since if they get into the hands of imposters, security is lost. Mallory must be prevented from listening in on the discussion between Alice and Bob. The following are a few places where cryptography is crucial:

* Industrial, economic, and corporate espionage: Public data networks are crucial for every firm. An attempt to get access to a company's data, including its customers, suppliers, and trade secrets, is known as industrial espionage. Data is jeopardized if an impostor gains access. Therefore, cryptography is crucial for data security.
* Internet commerce has transformed the way people shop nowadays. People now buy items online and conduct numerous large-scale financial transactions there. In this situation, encryption will ensure that all online transactions are secure against fraud and eavesdropping attempts.
* The private sphere: In addition to e-commerce and industrial espionage, there is one more area in which cryptography may make a significant contribution: preventing private conversation. Why we need to encrypt conversation data seems strange. Why do we send written correspondence in an envelope as opposed to a post card is the key to the problem.

**Uses of Cryptography:**

Cryptography plays an important role in the internet and below are some of the areas which demonstrates the need of cryptography(Schmeh 2006).

* Email: This is one the traditional way of communication over the internet. So cryptography is used to encode all the mails which flow over the internet and it has also gained importance on intranets also.
* World Wide Web: WWW is a big platform for surfing the data and acts as a database tool search for billions of users on daily basis.
* Client-server connections: Due to the huge growth of computer systems and internet, client server architecture is used in most of the areas where server handles the load and request from clients.
* Virtual private networks: Most of the organisations will have their branches spread across different locations. So it is very important to encode the data which is leaving the company network and decode when it reaches again into the company’s network after moving around over internet. This technique is referred as virtual private network(VPN).
* Payment systems: This is very critical area where money transfer will takes place and payments takes place through credit cards. So it is important to encrypt the card details and net-banking credentials from network attacks.
* Remote access: The services like Telnet and rsh are used to access the remote systems which use the similar functionalities to protect the data being accessed.

Internet banking: This has made the customers to do the bank transactions at home or office provided encryption is involved in the process

**Cryptographic security services (Principles of Information Security):**

Information security is all about protecting data in rest or during transmission. It also protects information and information system from being accessed by unauthorized personal, destruction, disclosure, modification or disruption(Y and Kim 2007). It can also be referred as collaboration of confidentiality, integrity and availability of user or data information. These three principals of information security are known as CIA triad or information security triad. The CIA triad represents a security model that helps users to understand the critical aspects of information security(Perrin 2008).

A picture containing text

Description automatically generated

Figure 7: CIA triad(Y and Kim 2007)

Below are the security services that falls under cryptography to ensure the security of the information and information systems.

**Confidentiality:**

Confidentiality is a concept which refers to protect the data from unauthorised access. This usually protects from passive attackers who tends to analyse the network flow. Information such as user’s sensitive data, bank details, credit card details, government data, and trade secrets has high value and cannot afford to compromise losing these data to third party(Anciaux *et al.* 2006). This is achieved by the means of Encryption. Encryption process will ensure that the data is accessed by the people who are authorised to access that information. Different cryptographic algorithms like AES, DES, RSA can be used to achieve this. Confidentiality doesn’t prevent data tampering where as it will just ensure the unauthorised access to it. Its strength depends on the length of the key in algorithm to encrypt or decrypt. The encryption can be achieved by either symmetric or public key encryption which will be seen in the later section in detail(Bishop 2004).

Diagram

Description automatically generated

Figure 8: Symmetric encryption process(Microsoft 2014a)

Diagram

Description automatically generated

Figure : Encryption that is asymmetric

**Need of Confidentiality:**

Confidentiality is required for various reasons such as:

* If data is disclosed which results in data loss or damage that may contain user data, business secrets, government data etc. So these data should be protected from unauthorised access.
* When data is sent over the insecure network then eavesdropper who constantly listens the network may gain the access. Thus encryption should be used to protect.

**Authentication:**

The Authentication service will provide the assurance that the communication is authenticated from both the entities. In other words it is the assurance that an entity is who he/she claims to be. It will provide assurance the connection is not disturbed by third party who predicts to be the legitimate party to get the unauthorised access to the confidential data. This will stop the masquerade attack(Zhou and Haas 1999)(Diffie and Hellman 1979).

Generally authentication is provided in two ways:

1. **Peer entity authentication:** In peer authentication both the parties involved in the communication are assured of each other’s identity. If the two parties considered themselves as peers then they should implement or follow a protocol which is similar in completely varied environment. For example TCP models in different communication. Peer Entity authentication is given to assure the other party that an entity is authenticated and trustable and not pretending to be a masquerade or trying to gain any unauthorised access.
2. **Data origin authentication:** This gives evidence for the source being received. But it doesn’t provide the protection against any modification or duplication done on the data. Usually this type of authentication supports applications like e-mails in which there is no prior communication has happened between the entities being communicating(Krzyzanowski 2004).

Below are some of the general authentication methods and authentication protocols which are kept in mind while designing any information security system(SANS Institute 2002):

**Authentication methods:**

* Passwords, OTPs, Cryptography with Public Key, and Digital Signatures.

**Authentication protocols:**

* IP Sec, Kerberos, and Secure Shell etc.,

1. **Data Integrity:**

Data Integrity is a security service which ensures that data is not modified or tampered when it is transmitted over the network. It protects the data being deliberately manipulated or damaged by imposters. It is highly essential in electronic business where data flow is huge which includes sensitive and critical data. Especially in banking sector if financial records are modified and if it happens on a hidden part then it leads to a disaster situation. Data integrity is generally achieved by hash algorithms. Hash algorithms will usually generates the fingerprint of the data and if any modification is done in data and results in different fingerprint which ensures that data is tampered(Bishop 2003).

**Hash Codes ensuring the Data Integrity**

A hash value is a fixed length numeric value that identifies the data uniquely. When data is being sent over insecure channel then hash values plays an important role. Once the other party receives the data along with the hash value of it then he/she produces the new hash value out of it and compares the received hash value with the newly produced one. If both are same then it proves that data is not tampered and data integrity is maintained if not then integrity is lost(Microsoft 2014b). A hash function takes a password or key of arbitrary length and generates a fixed length of integer. Cryptography uses the hash functions whose property is so easy that it calculates the hash but it is highly impossible to re-generate the real or original data. Now days SHA-1 and MD5 are commonly used hash algorithms. But as these are considered weak so SHA-256 is being used instead of these algorithms(OWASP 2012). Maintaining the data integrity in cloud has become very crucial. Though there is a lot of security mechanism involved to protect the data but sometimes due to hardware or software faults or might be with the human error which may allow access to unauthorised people who may change the data. To ensure the data integrity on the cloud without taking the data completely from cloud is known as public auditing, which is nothing but verifying the data using public keys based on public key infrastructure and certificates(Wang *et al.* 2013).

**4. Non-repudiation:**

Non repudiation (NR) is the security service that allows two entities to exchange the data in such a way that both the entities cannot deny their contribution/participation in the data exchange.Repudiation is denial of participation by either of the entity in whole part of communication. To encounter this, non-repudiation is introduced to prevent the denial of such claims by any entity. Nonrepudiation protocol follows a mechanism which involves the concepts such ‘proof of origin’ and ‘proof of receipt’ and doesn’t give advantage to either receiver or sender about the message being sent or received. Such NR protocol is known fair NR protocol(Zhou and Gollmann 1996a). Below diagram shows the non- repudiation protocol in which a third party intermediary (TPI) is involved. To ensure the non-repudiation between two entities, TPI will get proof of origin and proof of receipt from originator and recipient then it sends proof of origin to recipient and proof of receipt to originator at the same time

Diagram

Description automatically generated

Figure 10: This service (Coffey and Saidha 1996)

Non-repudiation uses symmetric or asymmetric cryptographic techniques and ensure the below check values(McCullagh and Caelli 2000):

* Approval: It provides the proof of whom approval is required to approve the content of data.
* Sending: It provides proof that who sent the data.
* Origin: This is a combination of sending and approval services.
* Submission: This is a proof that the delivery authority has received the data.
* Transport: It provides the proof to the originator that the word is delivered to the intended recipient.
* Receipt: It provides the validation that the word has been received by the recipient.
* Knowledge: The content of the message which has been received.
* Delivery: It is a combination of knowledge and receipt that provides validation.

Thus non-repudiation is a security service that avoids the below denials to occur from either of the party(Zhou and Gollmann 1996b):

* Authorship denial
* Denial of document sent
* Denial of documents received

Denial of document sent or received at a given time.

Table

Description automatically generated

.

**Cryptographic algorithms:**

1. Symmetric encryption algorithm:  Secret key encryption as two entities share a secret key. This shared key, which both parties must be aware of before communication can begin, is used to both encrypt and decode data. The straightforward approach for symmetric key encryption is shownhere.A picture containing text, clock, screenshot

Description automatically generated

Figure 17: Symmetric Encryption(William and Stallings 2006)

1. Public-key encryption, also known as asymmetric encryption, requires two keys for encryption and decoding. Basically, this method uses the following two keys:• Public Key (Known to All): Confidentiality is provided by the encryption carried out using this key.

• Private Key (Only known to the appropriate entity): Authentication is provided by the encryption performed with this key.

Diagram

Description automatically generated

Figure 18: Asymmetric Encryption-Public key encryption(William and Stallings 2006)

Diagram, schematic

Description automatically generated

Figure 19: Asymmetric Encryption-Private key encryption(William and Stallings 2006)

1. Data Integrity Algorithm: In this algorithm, a hash function H takes an input of a message of data M and outputs a hash value of h=H. (M). This procedure prevents any unauthorized change of messages and is known as a "One Way Hash Function" since it is irreversible (William and Stallings 2006).

2. Public-key encryption is another name for the asymmetric encryption technique, which requires two keys for both encryption and decryption. The following two keys are the main inputs for this algorithm:

• Public Key (Known to All): Confidentiality is provided while using this key for encryption.

• Private Key: This key is used for authentication during encryption and is only known by the relevant entity (William and Stallings 2006).Diagram

Description automatically generated

Figure 18: Asymmetric Encryption-Public key encryption(William and Stallings 2006)

Diagram, schematic

Description automatically generated

Figure 19: Asymmetric Encryption-Private key encryption(William and Stallings 2006)

1. Data Integrity Algorithm: This algorithm uses a hash function H that takes a message from data M as input and outputs the hash value h=H. (M). This procedure prevents any unauthorized change of communications because it is irreversible, earning it the name "One Way Hash Function" (William and Stallings 2006).Diagram

Description automatically generated

Figure 20: Block of hash function h = H(M)

**Application Design and Architecture:**

The proposed chat application design contains two entities and a trusted third party server. Below figure shows the simple architecture of the chat application being developed with Java.

Diagram

Description automatically generated

**Implementation:**

## Security protocol for key exchange

Diagram

Description automatically generated

Figure 36: Graphical representation of security protocol

Notes: Actual chatting starts in step 8 using AES key which is generated at both the nodes using the above protocol.

**Step 1:**

Node A generates a pair of RSA key (private along with public key) and sends the public key to a TTP server

Node B generates a pair of RSA key (private along with public key) and sends the public key to a TTP server

**Step2:**

Node A requests and receives the node B public key from TTP server.

Node B requests and receives the node B public key from TTP server.

**Step3:**

Node A sends the below data to Node B

Node A generates a random number, Na

It is a challenge from Node A to Node B

A’s ID, {Na}Kb, {{H(Na)}Ka-1}Kb

Where,

Ka-1 is A Private Key.

Kb is B Public Key.

Na is Random number generated by A

H (Na) is Hash of Na

[H((Na))] Ka-1 means H [Na] is encrypted using A Private key.

{[H(Na)] Ka-1 }Kb means [H(Na)] Ka-1 encryption done using B public key.

{Na}Kb means Na encryption done using B public key.

Data sent:

A’s ID

{{H(Na)}Ka-1 }Kb

{Na}Kb

**Step4:**

Node B decrypts the received data from A and obtains the secret component that is Na. Now B has its generated random number that is Nband Na which is obtained from Node A.

So Node B calculates the Shared secret key (AES key) that is Kab = Hash(Na+Nb)

**Step5a:**

Node B sends the below data to Node A

Node B has already generated a random number, Nb

This is response from Node B to the challenge given by Node A

B’s ID, {Nb}Ka , {{H(Nb)}Kb-1}Ka, {Na}Kab

Where,

Kb-1 is Private Key

Ka is Public Key

Nb is Random number generated by B

H(Nb) is Hash of Nb

H(Nb)}Kb-1 means H(Nb) is encrypted with Private key of B

{Na}Kab means Na is encrypted with Shared secret key Kab

Data sent is :

B’s ID

{{H(Nb)}Kb-1 }Ka

{Nb}Ka

**Step5b:**

Node B sends the below data and this is a challenge to the Node A from Node B

{Na}Kab

Where Na is the random number of A,

Kab is the shared secret key.

**Step6:**

Node A decrypts the received data from B and obtains the secret component that is Nb. Now A has its generated random number that is Naand Nb which is obtained from Node B.

So Node A calculates the Shared secret key (AES key) that is Kab = Hash(Na+Nb)

By using this key Kab, Node A will decrypt the step-5b data sent by Node B that is {Na}Kab.

Note: Now both the nodes have the same shared secret key Kab (AES key).

**Step7:**

Node A sends the below data and this is a response to the Node B from Node A for its challenge

{Nb}Kab

Where Nb is the random number of B,

Kab is the shared secret key.

**Step8:**

Finally both the nodes have shared secret key that is Kab and now the actual chatting will start.

This protocol follows the “Key Agreement” process which is a type of key management protocol in which both the entities generate the shared session/secret key based on some secret between them.