# CYBER SECURITY THREATS

**DEFINATION:** Cyber security can be defined as the process of defending computers, mobiles devices, network, servers, your information and data from malicious attack. In another word cyber security threats are the attacks that anyone can be victim where attackers are intending to harm their victims. Cyber threats are emerging issue of present world. It has been a big deal as it can even cause electric blackouts, breaches of national security secrets and even a failure of military equipment.

**Cyber security threats** virtually fall into three modes: Financial gain, disruption espionage and state espionage. However there are different common types of cyber threats they are:

1. **Malware:** Malware is a type of cyber threats where attacker unknowingly install software in victim PC or mobile device. The installed software can performs a malicious task on targeted device. The software might corrupt data, destroy storage and may be taking over the system. The hacker using malware is actually looking for money. They spread the malware themselves and even sell it to highest bidder on the dark web. There are different types of malware which is hardly exhaustive:

   **Virus:** It's a type of malware that can spread uncontrollably, damaging any system function by corrupting or deleting files. These viruses usually are executable file (.exe)

   **Trojans:** It is a kind of a delivery system for malware where hacker creates like a legitimate program to trick the victim so that they can install the program in to victim systems. They pose as harmless but they can do a lot of damage.

   **Worms:** It is also one of the types of malware which can self-replicate and can spread through different means such as messages, emails. The main purpose of worms is to steal information. The worms usually search for file sharing system or sort of contact database and transfer it to hacker.

2. **Phishing:** Phishing is also known as email-borne attack that is done tricking the email recipient. In phishing targeted user is mainly contacted by email or even

a telephone and text message. Attacker poses as a legitimate institution to lure individual into providing their confidential data such as personal details, credit card, password, etc. Email is the most common form of phishing attack that comes with mimicking the legitimate identity. This attack has different purpose according to the requirement of hacker. However for an organization as a victim, the purpose of this attack is to exploit employees of the organization to bypass different security layers which makes easier way for hackers to access data.

3. **DDos:** DDos stands for Denial of Service attack or Distributed Denial of service attack. In this attack, an attacker takes over many thousands of devices and they use those devices to invoke the functions of targeted system for an example website where hacker can cause it to crash from an overload of demand. In another word it can be explained as the malicious attempt to interrupt the normal flow of traffic in a server.

   In order to carry out DDos attack the attackers needs to gain control of large online machines. Those machines such as computer and IoT devices are now affected with malware that turns each device into a bot which makes it possible for attackers to have control over on a group of bots. This group of bots is called as a botnet. After establishing the botnet now the attackers send updates instructions to accessed bot to direct the machines. The IP address of the victim is targeted by botnet. And they control each bot to send request to targeted servers that cause the overflow of traffic resulting denial of service attack.
4. **Man in the middle attack:** In this kind of attack, attacker established a position between sender and recipient. This attack generally happens in electronic messages and intercepts them and changing them while transmitting the message. The sender and receiver won't have any knowledge of it. They believe that they are communicating directly with each other.
5. **Ransomware:** This was one of the most popular attacks at one time. And still these attacks are going nowhere. This is the type of attack that involves encrypting data on target system and attackers demand a ransom in exchange to let the user to get access to their old data again. This attack is done by using the tool of fear that can make a user to pay attacker.

6. **SQL injection:** SQL injection is one of the types of attack that uses malicious SQL code for manipulating database so that hacker can access information that is not supposed to be displayed by the developers or owners of any server or application. Attackers mainly focus on sensitive company data, list of user or even a private detail of customer.

   SQL injection is known as SQLI. A successful SQLI attack can result accessing your database, viewing user list, deleting data of the database table or the table itself. In some case attackers might get an access to administrative rights which can be very harmful for a victim. A simple SQLI query can be like "SELECT ITEM FROM ITEM WHERE ID = 999 OR 1 = 1", since 1=1 is always true it can returns all the products or item from the table.

## To combat these attack following measures can be applied

**Malware**

To prevent this attack some of the following measures can be taken:

- Using updated antivirus and anti-malware can protect against most of the malware.
- Firewall can regulate traffics, filter out the packet sent or received on different web application, devices and, server. Using firewall can filter out malicious traffic that is intended to access these devices.
- Email scanning and spam filtering is very important as most of these malware are transfer through emailing. Using a antivirus that can scan attachments can prevent malware transferring through email.

**DDos**

To prevent this attack following measures can be applied:

- Defending at the main perimeter of the network by limiting the rate of router, adding filters, setting lower ICMP, SYN and UDP flood drop thresholds can prevent DDos attack.

- Using high processing power to handle the overflow of the traffic can prevent interruption in the traffic.
- Testing your system against DDOS before deployment of the system and taking strong security measure at the weak point.
- Creating more than two redundancy server can handle interruption of the traffic. If one server is interrupted other server can provide the service.

**SQLI**

To overcome SQLI following measures can be taken:

- Getting rid of text field in the webserver can let not happen SQLI attack. If there is no needs of text field for a system, it's better to get rid of text field in the system.
- Do not construct queries with user input. The input field should be protected with CSRF token for proper validation.
- Do not directly connect your database using an account with admin level-privileges.
- Monitoring SQL statement continuously from database-connected application will help to identify SQL vulnerabilities and rouge SQL statement.

## Cyber security types

1. **Network security:** Network security can be defined as the practice of securing a computer network from unknown access and intruders.
2. **Application Security:** This kind of security focuses on keeping any devices or software free of threats. A successful security should be begins in the designing phases before the device is deployed. Ex. **Antivirus, firewall, and encryption.**
3. **Information security:** This kind of security protects the privacy and integrity of data.
4. **Operational security:** This kind of security includes the decisions and processes for protecting and managing data set.
5. **Data loss prevention:** This kind of security types includes the development policies and processes for managing data and making it sure to make

prevention for loosing data. For applying this security developing recovery policies can be best options which include a setting network policies and permissions.

## Cyber security Measures

1. **Install firewall:** Firewalls are one of the most advantageous and effective goalkeeper between your devices and the internet. Firewall filters incoming and outgoing packets in the internet, so firewall can block unwanted packets entering to your network or device. Once the firewall is installed you have to make sure it is working properly and never turn it off.
2. **Set up Access control list:** Setting up Access control list will allow your organization administrator to control all polices and permission. The admin can control which employee to permit or prohibited for accessing specific system and information of the organization.
3. **Use web filtering system and security program:** Using web filtering system means using firewall for internet. This Internet firewall block harmful sites and the sites which are not appropriate for accessing in the office time. Additionally this firewall helps to block malicious software from attacking your organization computer.
4. **Update system and program regularly:** Hackers are much forwarded now days, it is very necessary to be updated as their might be loop holes for attacker in an old system. Updates contain vital security patches that help to protect our system or information from known bugs and vulnerabilities. We have to make sure that our devices, operating system is up to date.
5. **Use complex Password:**
6. **Awareness in employees**

# Firewall

A firewall can be defined a type of device or cyber security tool that is used for filtering the traffic on any network. Firewall is used to separate network nodes from external traffic sources. It can be used to block specific applications and specific internet traffic sources as well. As we know the main goal of firewall is to block malicious packet request (traffic request) allowing legitimate traffic or packet to the network.

## Step for setting up secure firewall

Firewall is one of the key components for system or a network to provide security. There are some steps to set up the firewall so that the installed firewall is secure.

**Step 1:** The first step to securing your firewall. Firewall can be secured by updating your firewall to the latest firmware, by deleting, disabling default user accounts and changing the entire default password. It is needed to use secure and complex password. Administrative access of any firewall should not be given to untrusted one. Creating access list so that limit the user to make change in the system can reduce the chance of attacking.

**Step 2:** The second steps is to architect firewall zones and IP addresses. The organization has different server such as email, vpn which should be organized into a dedicated zone so that the zone have different limits for inbound and outbound traffic from the internet. The server that cannot access from the internet is required to be placed in internet server for the best filtration. The IP must be used for all networks. NAT (Network address translation) should be configured so that it can allow any internal devices to communicate on the internet.

**Step 3:** Configuring access control list determines which traffic needs permission to flow and which traffic need to be blocked The ACL is set of rule that set policy for inbound and outbound flow of traffic. It is best practice to disable the firewall administration interfaces from public access.

**Step 4:** The next step is to configure other firewall services and logging. It is best practice to configure firewall to report logging and provide enough details to your server. It is necessary if you are using Payment method.

**Step 5:** Finally testing your firewall configuration ensures that is your firewall is secured or not. Testing your firewall to verify the blocking of traffic which is set to be blocked in ACL configurations can ensure you the strength of your firewall policy. The testing should include penetration testing and vulnerability scanning.

**Different type of firewall (firewall architecture):**

- **Packet- filtering firewall:** This is the oldest type of firewall architecture. This kind of architecture of the firewalls basically creates checkpoints at a traffic router and switch. This kind of firewall works performing a single check of any data that is in bounding through the routers which inspect information such as the destination and origination IP address, port number, packet type, etc.
  **Advantage:** This router is not very resource-intensive i.e. this kind of router does not create any huge impact on system performance and they are relatively simple.
- **Circuit-level gateways:** Circuit level gateways firewall are the type of firewall which is meant to quickly and easily approve or deny the traffic packets and the best things is it does not consume significant computing resources.
  **Disadvantage:** while extreme resource-efficient, this kind of router do not check the packet itself. Hence it will be very easy for a packet holding malware but had the right TCP to pass through network. This is why this kind of firewalls is not enough to protect your business by them.
- **Stateful inspection firewalls:** To create a level of protection this kind of firewalls combines both packet inspection technology and TCP handshake verification. However this kind of firewall put more of a strain on computing resources. This leads to slow down the transfer of legitimate packets.
- **Application-level gateways(a.k.a proxy firewall):** Application-level gateways also known as proxy firewall are operated at the application layer which provide security by filtering incoming traffic between your network and the

traffic sources. Proxy firewall also performs deep-layer packets inspections. While performing deep-layer packet inspection it checks actual contents

- **Next gen firewalls:** Next gen firewall architecture includes deep-packet inspection which means this firewall checks the actual contents of the data packet, TCA handshake and also a surface-level packer inspection. This firewall also includes other technologies such as IPSs (Intrusion Prevention System) which is used to work automatically to stop attack against your network.
- **Hardware firewalls:** Hardware firewall is a type of firewall which use physical appliance that can acts in a manner similar to traffic router. These routers intercept data packets and traffic requests before they are connected to any server. This firewall provides security by filtering malicious traffic from outside.
- **Software firewalls:** This kind of firewall can be defined as the firewall which can be installed on any local device. One of the big advantage of this firewall is that it is highly useful for creating defense by isolating own network from other network.
- **Cloud firewalls:** A firewall is called a cloud firewall whenever a cloud solution is used to deliver a firewall. It is also known as FaaS (Firewall-as-a-service). Cloud firewall can be considered synonymous with proxy firewall. One of the advantages of having cloud firewall is that they are very easy to scale with your organization.

## Firewall Architectures for a company

As we know there are different kind of firewall architecture that any company can use to get protected from malicious software or unknown traffic. However different firewall fits to organization according to the level or class of organization. For any organization best firewall architecture should be implemented to add more the security and safe measure to the organization. To have enough protection your company must have multiple layers of firewalls. For example at perimeter you can have cloud or hardware firewall and a software firewall on each side of your network assets. However among different firewall I personally suggest a proxy firewall offers far more robust protection in exchange for additional expenses**. Following are the advantage of proxy firewall:**

- The proxy firewall first establishes a connection to the source of any traffic, after building a connection it inspect the inbounding packet of data rather than letting any packets or data connect directly.
- Proxy firewall looks at both the packet and at the TCP handshake protocol.
- It also checks the actual contents of the information packet and make sure the packet does not have any malicious object.
- Proxy firewall creates extra layer of separation between the client and the devices on network.

# DMZ

**DMZ** stands for demilitarized zone, which is one of most useful tools in firewall engineering today. It is a physical or logical sub network it exposes any company external –facing services to an untrusted network or packet such as internet. The main aim of implementing DMZ is to add an additional security to any company local network. While the DMZ is implemented effectively, it allows the organization extra time for addressing and detecting breaches before they further affect your network.

**Bastion host** can be defined as a kind of computer that is specifically designed and implemented to stand against attack. Bastion host work very effectively hosting a single application like proxy server and removing all the other services so that it can reduce the threat to the computer

It is very crucial to carefully plan and design a DMZ as DMZ is design to segregate network devices, servers, application and system based on risk.

**I prefer to design DMZ in internal side due to following reason:**

- **Designing DMZ in the internal side can prevents allowing control over to network and devices.**

## Security threats to any online application

- **Phishing Attack:** It is one of the favorite types of attack of social engineering practitioners. An attacker can set phishing attack to steal user data for example credit card number, personal information and login information. In this kind of attack an attacker posse as a trustworthy entity and fools the victims so that they open an email or the message link send by attackers.
- **Cross-site Scripting (XSS):** Cross-site scripting is one of the common vectors that can insert any malicious code into your website or web application that is found to be vulnerable. It usually targets your website users which can result harming your clients and the reputation of your company.
- **Web scrapping:** some of the attacker might deploy a bots to steal a data from your website. The bot operated by attacker are highly capable of stealing your website content and database information.
- **Backdoor Attack:** It is a form of malware which circumvents login authentication to enter a system. Organization offering employee remote access including file server and databases can be in danger list of this kind of attacks.
- **Cross-site Request Forgery (CSRF):** CSRF also known as XSRF or session riding or sea surf which can deceives the user's browser and logged into your application and they can run unauthorized actions. A CSRF is that dangerous that it can transfer fund in an authorized manner and can even change your passwords. Moreover it can perform a task like stealing session cookies and business data.

# Security measure for web application

- **Ensure sitewide SSL:** Have you ever noticed a lock in a browser address bar that lock means that your site is secure. However SSL should be sitewide and enforced to have a full advantage of SSL and to verify encrypted connections. Every page of your site should be available on SSL. As you may know any information that is transmitted without SSL connection transfer in a form of plain text and can be easily intercepted by hackers. So it is necessary to ensure sitewide SSL in your website.
- **Enable HTTP strict Transport security:** HTTP Strict transport security is a type of security that ensures that your browsers communicate with a website only over SSL. Enabling this security will convert non-SSL request to SSL request automatically.
- **Use SHA256 Encryption:** SHA256 has taken over other security encryption and it has been improving the encryption drastically. You should replace your website encryption with a 2048-bit SHA256 method if it has SHA1 fingerprint. If you own the website you need be updated with encryption method as it will continue to change as ways are found to crack a present encryption method.
- **Use secure cookies:** A secure cookies always transmitted across an SSL which result in preventing cookie with potentially sensitive information to be stolen in a transit. If you are failed to use secure cookies it may allow a third party to intercept a cookie.
- **Protect against SQL injection:** SQL injection is one of the danger attack that any website owner can bear. It is the most important step to protect your website against SQl injection attack. If you restrict your web application to run stored procedures, any attempts to inject SQL on your site forms will fail. It will in let input to pass in a server unless a input meet the certain criteria.

# Encryption Method

# AES

AES stands for Advance Encryption Standard and is one of the encryption algorithms which are trusted as the standard by U.S government. AES algorithm can be defined as a symmetric encryption algorithm that encrypts a fixed block of data at a time. The key with 128-, 192-, or 256-bit long can be used to decipher the text. In AES the 256 bit key encrypts the data in 14 rounds, 192 bit key encrypts the data in 12 rounds and 128 bit key encrypt the data in 10 rounds. The round of AES includes a several steps of substitution, transposition, and more. This encryption is the most used encryption method for today.

Working mechanism of AES:

- **First data is divided into blocks:** Plain text is separated into blocks. The block size of AES is 128 bit. It separate data into 4X4 column
- **Key expansion:** It takes the initial key and uses it to come up with a series of other key for each round of the encryption process
- **Add round key:** The initial key is now added to the block of the
- **Substitute bytes:** In this step, each byte is substituted according to a predetermined table.
- **Shift rows:** The second row is moved one space to the left, the third row is moved two spaces to the left, and the fourth row is moved three spaces to the left
- **Mix column:** each column has a mathematical equation applied to it in order to further diffuse it
- **Add round key again:** Remember those round keys we made at the start, using our initial key and Rijndael's key schedule? Well, this is where we start to use them. We take the result of our mixed columns and add the first round key that we derived:

# RSA

RSA stands for Rivest-Shamir-Adleman derived by three people which name indicates. RSA is an asymmetric encryption algorithm where the process of encrypting data is based on the factorization of the products of two large prime numbers. RSA algorithm is considered as the standard algorithm for encrypting data that is sent over the internet. In RSA user will have pairs of keys, private and public key. A public key is used encrypt our text or message whereas the private key is used to decrypted the encrypted message. RSA is generally used to create secure connections between VPN server and VPN clients. The protocol like TLS handshakes and Open VPN use the RSA algorithm to exchange keys creating a secure channel.

**Working mechanism of RSA**

1. **Generate the RSA modulus:** The first step is to select of two prime numbers say p and q, and then calculating their products N like: N = p*q, here N will be specified large number
2. **Derived Number (e):** The second step is now; consider a number e as a derived number which should be greater than 1 and less than (p-1) and (q-1).
3. **Public key:** The third step is to generate public key where specified pair of numbers n and e forms the RSA public key.
4. **private key:** After getting public key the private key is generate by calculating p, q, and e. like : ed = 1 mod (p-1) (q-1)
5. **Encrypting formula:** let us consider a plain text message is sent by someone whose public key is (n,e). Now to encrypt the plain text message we can use: C = Pe mod n.
6. **Decrypting formula:** The decryption method directly includes analytics for calculation where we consider receiver C has the private key d, the result modulus will be calculate like:

   **Plaintext = cd mod n**

# Triple DES

Triple DES algorithm was designed for the purpose of replacing the original Data Encryption Standard (DES) algorithm. The DES algorithm is no longer in use as the hackers eventually learned to defeat DES with relative ease. The Triple DES algorithm was mostly used symmetric algorithm in the industry and recommended standard at one time. Triple DES uses encryption method by encrypting blocks of data using a 56 bit key which means Triple DES implements the DES cipher algorithm with three individual keys to each data block. The reality is Triple DES is slightly phasing out however Triple DES is still managing to make a dependable hardware encryption for different industries and financial services.

**Working mechanism of DES algorithm**

The first mechanisms are to generate and distribute a 3TDES key K. The 3TDES key consists of three different key i.e. K1, K2, and K3. The actual length of 3TDES key is 168 bits (3*56). The whole process of encryption is illustrated below:

**Encrypt plaintext:** The first process is to encrypt plaintext block. The process uses the single DES key K1

**Decrypt first process:** The second process is to decrypt the output of the first process. Here the process uses Key 2

**Encrypt second process:** Finally the output of second process is encrypted using DES with key 3

The final output is ciphertext.

The ciphertext can be decrypt by using the reverse process. First cipertext is decrypted using key 3 then again encrypted with key 1 and lastly k1 is again use for decryption and the final output is text.

# DES

DES stands for data encryption algorithm which is a symmetric-key algorithm for encryption of digital data. DES is very unsecure encryption algorithm as it's a short key length of 56-bits which make is unsecure from latest application. Now the DES is an outdated method for encryption of any data. DES once used to provide cryptographic security for the entire government communications.

# Symmetric-key algorithm

Symmetric-key algorithms are the type of algorithm for cryptography that uses only one key i.e. secret key for both encrypting plaintext and decryption. It is required to exchange the key for two entities communicating using symmetric algorithm. Symmetric encryption converts a data into a form that cannot be understood by anyone. It is required to have the secret key for the decryption of the cipher text. The cipher text can only be decrypted by using secret key used while encryption.

Symmetric encryption is old and known for its best technique. Despite of being older it is effective and faster than asymmetric encryption. This encryption is typically used in bulk encryption, database encryption. Some of the platform where symmetric cryptography is used is payment method, hashing or random key generator, etc. **Different kind of symmetric key algorithm is AES, 3DES, RC4, RC5, RC6, IDEA (international data encryption algorithm) and blowfish. Among them RC6 is a stream cipher whereas other are block ciphers.**

# Asymmetric algorithm

Asymmetric algorithm is relatively different than symmetric algorithm where instead of one key secret key is divided into two parts i.e. private key and a public key. The public key can be shared with anyone we can trust or not however the private keys required to be kept in secret. Asymmetric algorithm usually has two use cases: confidentiality and authentication. Message in asymmetric algorithm can be signed by private key. Anyone who accesses the public key is able to verify that the message is created by the one who pose the private key. Anyone with private is only able to decrypt the message

whereas anyone with private key can encrypt the message. Asymmetric encryption is one of the popular and mostly used algorithm in day to day communication exchange channels over the internet. Some of the asymmetric algorithm types are RSA, DSA, Diffie-Hellman key exchange, etc.

## Difference between Symmetric and Asymmetric Encryption

- Asymmetric encryption uses two key public key and private key for encrypting and decrypting message whereas symmetric encryption uses a one single key that is requires sharing to the people who can access the message.
- Symmetric encryption is older than asymmetric encryption. Asymmetric encryption is relatively new.
- Symmetric encryption however being older, it is faster than asymmetric encryption.
- Symmetrical encryption model eliminate the need to share the key.
- Symmetric is using easy to understand if you have the key you gain access to the information while asymmetric cryptography exposure to information is limited.
- Symmetric keys are stored in the respective application and if found can be used to forged software licenses while asymmetric does not enable the hacker to forge licenses for other.

# Secure Socket Layer (SSL)/ TLS(Transport layer security)

SSL/TLS stands for secure socket layer/ transport layer security, it is a protocol developed by Netscape. The purpose of its development is to make it possible to transport private documents through internet. SSL is very secure medium for transmitting documents as it uses a cryptographic system. SSL uses asymmetric cryptographic system that has two keys for encryption and decryption. These keys establish a secure encrypted connection in the website.

In another words SSL is a standard security technology that can be uses to establish an encrypted link between the client and the server and a browser or any other server such as mail server.

### Working mechanism of SSL

- Whenever any web browser tries to connect to any website that uses SSL,
- The browser initially request a web server identity which execute the web server to send the browser a certificate copies i.e. SSL certificate (X.509).
- After getting SSL certificate the browser checks whether the certificate is trusted or not.
- The browser sends message to the respective web server if the certificate is trusted.
- Finally the server responds to the browser and start the encrypted session with digitally signed acknowledgment

**HTTPs**

HTTPs is a secure HTTP which is another protocol for transmitting data securely. SSL creates a secure connection where HTTPs is used for transmitting any amount of data over world wide web (WWW). The purpose of designing HTTPs is to make browser, able to transmit data securely between client and server. Both HTTPs and SSL are complementary component for transmitting and creating secure data and connection respectively.

**Explain how a client software, say web browser, firstly establishes that a site certificate is trusted, and secondly how it uses the information contained in the certificate to set up an encrypted communications channel.**

- First your web browser downloads the web server certificate which contains the public key of that server.
- The certificate is signed with the private key of trusted certificate authority.

- Your web browser comes installed with the public keys of all the major certificate authorities which uses a public key to verify that the web server certificate was signed by the trusted certificate authority.
- The domain name and IP address contains by a certificate confirm with the certificate authority that the address listed in the certificate is the one to which it has an open connection.
- Now finally the web browser generates a shared symmetric key which will be used to encrypt the HTTP traffic on this connection. The browser encrypt symmetric key with public key of the server and after encrypting it sends back hence making sure that only the web server can decrypt it as only the webserver will have their private key.

**VPN**

VPN stands for virtual private network; it is a type of programming that is popular for creating a safe and encrypted connection between client and the server. It extends a private network across the public one which helps to enables user to receive and send data through public or shared network like the devices is directly connected to the private network.

When VPN is implemented, the traffic is routed through an encrypted tunnel that is operated by the VPN Company. Using VPN will secure your URL request from ISP. They won't be able to see your traffic. If you are using a site that uses only HTTP then your traffic is no longer secure. Using site that uses HTTPs is secured and encrypted. Using VPN server hides your actual IP address.

**IPS and IDS**

IPS is intrusion prevention system whereas IDS is intrusion detection system. IPS detects the intrusion and takes further action for preventing intrusion whereas

IDS just detect the intrusion. It does not take any action it just leave the rest of the work for administrator.

**Three-way handshake**

A three-way handshake is one of the methods that is used in a TCP/IP network. The purpose of three-way handshake is to create a connection between a client and the host. The reason behind it name three-way handshake is that it is three step method in which the server and client transmit and exchange packets. The three step of three-way handshake is presented below:

1. First the clients check whether a server has open ports or not by sending a Synchronize (SYN) packets to the server.
2. If the ports are open the client receives SYN-ACK packets sent by server.
3. Finally the client acknowledges the packet and sends ACK (Acknowledgement) packet to server.

**Encryption is different from hashing**

Encryption and Hashing both method is used to convert a readable data into a format that is not understandable. Encryption data can be converted back to the original data by the process of decryption but the hashed data is never possible to converted back to the original data.