Part 1: Cryptography and Data Security

Cryptography is the study and practice of techniques of secure communication in the presence of third parties called adversaries. There are two types of cryptography, those are symmetric cryptography and asymmetric cryptography. Cryptography is based on the application of mathematical theory and informatics. Cryptography can be divided into 3 independent dimensions. Also, cryptography can be separated into substitution and transposition. The first one is the type of operations used for transforming plaintext to ciphertext. Substitution is a type of mapping element with plaintext to another element. But in transposition, only elements in the plaintext are rearranged and the only fundamental requirement is that no information be lost.

The second one is the number of the keys used. If both sender and receiver are using the single common key to encrypt and decrypt the message that key is known as symmetric key or symmetric cryptography. The most popular symmetric key system is Data Encryption Standard (DES). If the sender and receiver is using the different key to encrypt and decrypt, that is known as asymmetric cryptography. Asymmetric Encryption uses two distinct related keys. One key known as the public key is used for encryption and the other, the Private key is for decryption. Also, the private key is intended to be private so that the only the authenticated recipient can decrypt the message.

The third dimension is that the way in which the plaintext is processed. In this third dimension, there are two types of cipher is processed. The first one is Block Cipher and the second one is steam cipher. A block cipher forms the input one piece if components at a time, producing an output block for each input block. A steam cipher processes the input elements continually, producing output one element at a time, as it goes along.

Explaining how cryptography can keep the company's data secure

Symmetric cryptography

In symmetric encryption also known as private key encryption, data is encrypted using a single same key that only the sender and the receiver know. Only a single key is used during both the encryption and decryption of the message.

To protect information of the company, symmetric key encryption can be protecting the data and information between the client and the company because only the client and the company knows the private key and only those two can encrypt the message. When the company use their key to encrypt their message and their message is encrypted to scrambled data and no one can read that message except client and the company. If the clients receive the message, they can use the private key to decrypt it and can red as the plaintext. Advantage of using symmetric cryptography is that it is simple encryption method, easy to use, fast and efficient for large amounts of data that will be sending between client companies and main company. Also, symmetric cryptography uses private password authentication to prove the receiver's identity so that hackers won't get the data.

Asymmetric cryptography

Asymmetric cryptography also known as public key cryptography is method of encrypting data intended for only specific recipients. In asymmetric cryptography, both sender and receiver only have their own public and private keys which are long and large random numbers a set of pair together with mathematical algorithms. Public key can be kept secret and private key can be shared with everyone. Asymmetric cryptography also works with digital signatures.

Asymmetric cryptography has two primary use cases. Those are authentication and confidentially. A sender encrypts a message with their own private key and anyone with access to the sender's public key can verify the message. Asymmetric key cryptography keys are thousands of bits long. The longer the key, the less likely is for hackers to crack the paring algorithm and more secure it is. As an example, Josh sent encrypted message to Mark. Both agree to use the public key encryption to encrypt his message. Mark creates a pair of keys: one public key and one private key. Mark keeps the private key and he gives public key to Josh. After, Josh writes his message, he uses the public key to encrypt it. When Mark gets the encrypted document, he uses the private key to decrypt it. By searching on the above example, the message may be signed with a private key, and then every person with the general public key in order to verify that the message changed into created by a person owning the corresponding non-public key. This can be combined with a proof of identity system to know what entity owns that private key, providing authentication. This makes the system extremely secure, because there is essentially an infinite number of prime numbers available, which means the possibilities of keys are near to near to infinite. Asymmetric cryptography is good for the company because the secret key is only known by the sender and the receiver and that will take for a long time for hacker to hack it.

Explaining how symmetric and asymmetric encryption provide message authentication

A message authentication code (MAC) is a procedure that allows communicating parties to verify the received messages are authentic. A MAC required two inputs: a message and a secret key known only to the originator of the message and its intended recipients. This allows the recipients of the message to verify the integrity of the message and authenticate that the message's sender has the shared secret key. Message authentication is a procedure that allows communication parties to verify that received messages are authentic.

By using message encryption, only the sender and receiver share a key so the only the genuine sender would be able to encrypt a message successfully. John is the sender and his parties are receiver. If john sent message to his parties (clients) knows that secret key and matches, it shows that the message is authentic. But there is still problem. If the attacker can capture the file and reorder the block of cypher text, it will decrypt successfully, and the receiver will not know that it has been changed and who change that. To fix this problem, receiver can use the shared secret key to generate code and appends it to the message.

For the asymmetric, public and private key pair are different. Most important fact is that the keys must be unpredictable. Then, public key encrypts the data, using algorithms. Finally, with the private key, decrypt the encrypted data and verify that it worked by comparing the result with the original one.

Recommendation for message authentication

For John's company, Secure Hash Algorithm (SHA) and HMAC would be the best option to choose. Secure Hash Algorithm function is based on the hash function MD4 and its design closely models MD4 and produces 160-bit hash values. HMAC has been an increased interest in developing a MAC derived from a cryptographic has code, such as SHA-1. For John's company, SHA 512 would be the best option to choose. Because its message size is less than 2^{128} bits and gives the biggest message digest size (512). Also, it produces 1024 the biggest block size. If John's company is using 64-bit CPU processors, it is good to use SHA 512. But if they use 32-bit CPU processors, company can still use SHA256. SHA256 and SHA 512 will be the best solution for John's company depending of their computer's CPU bit.

Company's Data Security

Advanced Encryption Standard (AES) is the most common and widely symmetric block cipher that is used in the worldwide. This algorithm has an own shape to encrypt and decrypt sensitive data and one of best in the world. It is recommended for John's company because AES is extraordinarily hard for hackers to get the real information when encrypting by AES algorithm. It has 128-bit block size and it support up to three different key sizes such as AES 128, 192 and 256 bits.

Advanced encryption standard (AES), Data Encryption Standard (DES) and Triple DES (3DES) are important ciphers. For John's company, advanced encryption standard (AES) would be the best option for data security. AES is chosen for John's company because AES process is performed in binary and there is a lot more math. AES is a symmetric block cipher and it has a block length of 128 bits and supports for key length of 128-bits, 192-bits or 256-bits. AES 128-bits is the least strong encryption and AES 256-bits is the strongest encryption. Also, AES algorithm is a symmetric block cipher that can encrypt and decrypt data.

AES brings additional security because it uses a key expansion process in which the initial key is used to come up with a series of new keys called round keys. These round keys are generated over multiple rounds of modification, each of which makes it harder to beak the encryption. So that AES would be the best and very helpful for John's company.

Data in Transit

Data transit is the process of sharing and sending data or message through networks or electronic devices. To share data safety, John can send his important company files to his clients by using encryption. John can start with the plaintext message confidential memo to start. This message is not secured so that he would not want to transmit this through an unsecured medium. In order to

protect this data, he would use encryption algorithm which is like a lock and he would have a specific key that was only know to the sender and the receiver. This would convert the data into ciphertext which would not be able to read by anyone who did not have the key. Now, the information has been secured and it is able to be transmitted over the internet or through our network without any concern of individuals capturing the data because it is illegible. One the data gets to his clients; they could use the identical algorithm and the important thing that was shared with them by the way of John to decrypt the records and they will then have the same plaintext exclusive memo layoffs to start. So, this technology helps to ensure that only John and his clients were able to read that sensitive data or messages. While data or messages are transmitting, John can protect data in two ways while it is being transmitted using either link encryption or end to end encryption. So that John can safely share his data with authorized partners.

Data at rest

John can protect data at rest by using encryption. This helps him to ensure the confidentiality of his company's data while it is stored on a device such as thumb drive, a hard drive, a solid-state drive perhaps a CD or DVD. When John upload his data or files to server, those data or files are stored in plaintext. The risk there is that if an attacker somehow gains authorized access to that server, hacker can simply grab those files. John can prevent this by uploading important data on cloud services such as google drive, one drive or iCloud drive …. etc. by using symmetric cryptography algorithm. He should use symmetric cryptography because only both he and his clients will know the secret codes and only they can read the important data and it is also difficult for hacker to decrypt the secret key.

Part 2: Cryptography keys and user authentication

Recommendation: Kerberos 5

Kerberos provides a centralized authentication server whose function is to authenticate users to servers and servers to users. Kerberos relies exclusively on symmetric encryption, making no use of public-key encryption. There are two versions of Kerberos are currently used. They are Kerberos version4 and Kerberos version 5. For john's company, Kerberos version 5 should be used because version 5 is the most updated, widely used method of authentication, more secure, more flexible and more efficient than all previous version of Kerberos.

As in above paragraph, Kerberos relies exclusively on symmetric encryption. Kerberos servers perform both authentication and key distribution. For human user, the master key is derived from his or her password. For network device the key is configured in. All the keys are stored securely at the KDC. Suppose a client wants to access a file server but with Kerberos, the client must be verified through a trusted third party. This third party is called Key Distribution Center (KDC). KDC includes two servers; Authentication Server (AS) or a Ticker Granting Server (TGS). Here how Kerberos work with an example. When user USER login his workstation contacts the KDC with an authentication service

request message. The KDC generates a per day session key, SB. The KDC generates a per day session key, SB. And the so-called ticket-granting ticket that contains SB and the ID of USER and the ticket is encrypted using the KDC's own key. The KDC then sends back a message to USER's workstation, and this message is the authentication service response. The message contains the per day session key and the ticket-granting ticket (TGT) and the message is encrypted using the shared master key between USER and key distribution center (KDC). And because KB is the master key shared between USER and KDC. Only USER's local workstation can decrypt this message. Ans then it can store the private key and the ticket granting ticket. USER's local workstation will then use SB for subsequent messages with the KDC and it would include the TGT to remind and convince the KDC to use SB. That is, any new request to the KDC will include the TGT in the request message and the new ticket from the KDC will be encrypted using SB.

All communications between the different parties involved a secret key. Also, to make Kerberos work, all servers and parties must be registered with Kerberos by using their user ID and password so that Kerberos will works. By using Kerberos, there are some benefits that is localhost does not need to store passwords. Above paragraph shows how Kerberos and key distribution woks. That will solve John's worrying about fake user log in.

R**ecommended Software: Key Management Service (KMS)**

KMS makes it easy for John to create and manage cryptographic keys and it is a secure and resilient service that uses hardware security modules that have been validated under FIPS 120-2. AWS KMS is recommended for Joh's company because it protects the master keys that protect company's data and they never leave AWS KMS unencrypted.

Part3: Cloud Computing

Cloud computing is a paradigm shift that provides computing over the internet. Cloud computing service consists of highly optimized virtual data centers that provide various software hardware and information resources for use when needed. There are basically three layers of cloud computing. Those three layers perform like a pyramid. The bottom layer is the Infrastructure as a Service (IaaS) which is known as the foundation step. In this step is good for companies that need to scale up or down quickly, or that experience sudden changes in capacity. Also, in this step, company can start doing cloud hosting by buying or renting thousands of servers. The second step is Platform as a Service (PaaS). This step means that this is the place where software is developed. Company can run, test and launch application on this step. The top step is known as Software as a Service (SaaS). This layer is the top of the pyramid and most familiar to people. In cloud, users can upload their files and data with private or public. Also, uploaded data and files are already backup to prevent hardware failure. Some clouds are paid. Some are free. Hence, it is recommended for the John's company and it is fast, save time and money.

To make data file secure on cloud, John should use cloud services that encrypt data and he should backup data locally. Also, he must avoid storing sensitive data and information on cloud. Even

he stores sensitive data on cloud, he should use symmetric encryption and share with his clients. So that only he and his client can only view those sensitive data with private key and so that hackers cannot take those data and information. Making password is also important because if the password is short and simple, attackers can guess it and they can easily adjust it. Key aspect of long password is length (longer is better), mix of capital and small letters, numbers and symbols.

Security risks and countermeasures

Data Control: In cloud computing, data in the cloud can potentially be accessed by anyone. As an example, John share important data with his clients via cloud and another third parties can also access to that data. Countermeasures this problem by limiting the access of the data or he can encrypt it when he put it in the cloud.

Malicious Insiders: If we are using the cloud computing, we have to trust to employees and cloud provider with extraordinary level. Because of this occur malicious insiders that can harms to the customers. Countermeasures: Always encrypt the data, install antivirus software, make partner with a security vendor that offers managed network services and use the advanced software such as Splunk or Exabeam to do advance analytics to be more protective the data.

Data loss: Losing data is a major disaster for the company and that is sensitive. There are some ways to prevent this data loss problem such as always record the backup with external hard disk or uploading to another cloud service and always apple the strong API access control.

Account or Service Hijacking: Account or service hijacking is a kind of identity theft and has evolved to be one of the most rapidly increasing types of cyber-attack. It is happening in cloud computing by sharing the account credentials between users and services and forgot to active the 2FA (two factor authentication) in their respective accounts. Countermeasure: Stop sharing the accounts credentials between users and services, secure access- apply a boot and braces approach, encryption and build a layered defense.

For John's company, using cloud computing is recommended because using cloud computing can reduce the company's business costs, free up company's IT resources and provides scalability to grow with his business.