ISSN: 2456-1363
International Journal of Scientific Research & Growth
A Multidisciplinary Peer Reviewed and Refereed International Journal
Volume-3 Issue-1 April- 2018
www.ijsrg.com
editor@ijsrg.com

Case Study Of Cryptographic Techniques In Current Scenarios

[1]Harleen Virdi, [2]Manish Kumar Mukhija
[1]M.Tech Scholar, MITRC, Alwar, Rajasthan, India
[2]Assistant Professor, MITRC, Alwar, Rajasthan, India
Email- harleenvirdi.12@gmail.com, mukhijakumar@gmail.com

Abstract
Data is the most significant entity and basic unit of communication in all form whether it is in electronic form, digital form, verbal form or written form. Due to this, we adopt strict measures to secure the data storage and ensure its valid access at different levels so that its usability and integrity are maintained. Security of any data whether it is in transit or not, deals both with its storage and retrieval.

In today's world of advance communication, everybody prefers to save and retrieve data quickly from any geographic coordinates. To facilitate this, mobile cloud computing and smart phones play a significant role. They supply user to use the techniques for economical storage and retrieval of data using platform, software system and infrastructure being provided by third party.

***Keywords**: - Cryptographic techniques, software system, advance communication.*

1- INTRODUCTION

In cryptography, encryption is the path toward encoding messages or information with the end goal that exclusive approved gatherings can read it. Encryption does not of itself keep away from catch endeavor but instead denies the message substance to the interceptor. In an encryption plot, the proposed correspondence information or message, referred to as plaintext, is encoded using an encryption count, delivering figure message that must be perused if decoded. For particular reasons, an encryption plot, for the most part, uses a pseudo- irregular encryption key made by estimation. It is on an basic level possible to decipher the message without having the key, be that as it may, for an overall plot encryption framework, broad computational resources and capacity are required. An approved recipient can without much of a stretch decode the message with the key gave by the originator to recipients, however not to unapproved.

2- WHY WE NEED ENCRYPTION?

Nowadays we sometimes come across a situation where we need a secure way to transfer images over the network from one point to another, but these images can be attacked over the network. The data transferred can be attacked by direct or indirect human inter action and a very common way in which network security is being compromised is when network resources are accessed by external attackers. Hence, need of data security is not only required on the sender or receiver end but also over the network.

Hence in this work we will be working over three layers data security hence providing shelter to the data by obscuring the main content. This will be done by encrypting the data at sender, receiver and also at the cloud where image will be saved for transferring over the internet in encrypted form , hence providing security at multi layer. Due to flexible, accessible and compared capacity of Cloud computing over traditional online methods of computing and storage, it is becoming main pillar for many technologies.

While transferring the data through internet from one point of contact to another or it is in motion, it is moved from one point to another. Data need to be secured in each manner, whether it is being transferred from one network to another network or from one local device to another one, from one cloud service to another, for all these effectives measures are required to be followed for data protection.

While data is in transit, it has high risk of being exposed and need protection. For this, there are different approaches, like we can either protect data by encrypting it or by encrypting the connections itself which also plays a major role in protecting data and nowadays a popular tool for the same. Along with encryption, there are many other methods through which data can be protected while in transit.

3- TYPES OF ENCRYPTION

In cryptography, encryption is the path toward encoding messages or information with the end goal that exclusive approved gatherings can read it. Encryption does not of itself keep away from catch endeavour but instead denies the message substance to the interceptor. In an encryption plot, the proposed correspondence information or message, referred to as plaintext, is encoded using an encryption count, delivering figure message that must be perused if decoded.

3.1- Symmetric key encryption or Public-key encryption

In symmetric-key schemes, the encryption and decryption keys are the same. Imparting parties must have a similar key before they can accomplish secure communication.

3.2- Asymmetric key encryption

In public-key encryption schemes, the encryption key is published for anyone to use and encrypt messages. the encryption key is distributed for anybody to utilize and scramble messages. Nonetheless, just the accepting party approaches the decoding key that empowers messages to be read.

4- ENCRYPTION ALGORITHMS

Today, strength of encryption is usually measured by key size. No matter how strong the algorithm, the encrypted data can be subject to brute force attacks in which all possible combinations of keys are tried.

4.1- Data Encryption Standard (DES)

DES is the original standard that the U.S. government began promoting for both government and business use. Originally thought to be practically unbreakable in the 1970s, the increase in power and decrease in cost of computing has made its 56-bit key functionally obsolete for highly sensitive information. However, it is still used in many commercial products and is considered acceptable for lower security applications. It also is used in products that have slower processors, such as smart cards and appliance devices that can't process a larger key size.

4.2- Triple DES

Triple DES, or 3DES as it is sometimes written, is the newer, improved version of DES, and its name implies what it does. It runs DES three times on the data in three phases: encrypt, decrypt, and then encrypt again. It actually doesn't give a threefold increase in the strength of the cipher (because the first encryption key is used twice to encrypt the data and then a second key is used to encrypt the results of that process), but it still gives an effective key length of 168 bits, which is plenty strong for almost all uses.

4.3- RC4, RC5, and RC6

This is an encryption algorithm developed by Ronald Rivest, one of the developers of RSA, the first commercial application of public key cryptography. Improvements have been made over time to make it stronger and fix minor issues. The current version, RC6, allows up to a 2,040-bit key size and variable block size up to 128 bits.

4.4- AES

When the U.S. government realized that DES would eventually reach the end of its useful life, it began a search for a replacement. The National Institute of Standards and Technology (NIST), a government standards body, announced an open competition for a new algorithm that would become the new government standard. There were many competitors including RC6, Blowfish by renowned cryptographer Bruce Schneier, and other worthy algorithms. They settled on AES, which is based on an algorithm called Rijndael, designed by two Belgian cryptographers. This is significant because they used an open competition to decide on the standard. Also, selecting an algorithm by two non-American developers with no significant commercial interests helped to legitimize this selection worldwide. AES is rapidly becoming the new standard for encryption. It offers up to a 256-bit cipher key, which is more than enough power for the foreseeable future. Typically, AES is implemented in either 128- or 192-bit mode for performance considerations.

5-ENCRYPTION APPLICATIONS

5.1- Hashes

Hashes are a special use of one-way functions to provide authentication and verification using encryption. A hash function takes a file and puts it through a function so that it produces a much smaller file of a set size. By hashing a file, we produce a unique fingerprint of it. This gives us a way to make sure that the file has not been altered in any way. By hashing a suspect file and comparing the hash to the known good hash, we can tell if any changes have been made. It is unlikely that a file with a different structure would produce an identical hash. Even changing one character changes the hash significantly. The chances of two different files producing the same hash are infinitesimal.

Hashes are often provided on downloaded versions of software to make sure you are getting the real thing. This is important, especially with open source software, where it may have been passed around quite a bit or downloaded from another site. The official Web site will usually post the correct hash of the latest version. If the two don't match, then we know some changes have been made, possibly without the permission or knowledge of the software developers. The most popular hashing algorithm is called MD5.

5.2- Digital Certificates

Digital certificates are the "signature" of the Internet commerce world. These use a combination of encryption types to provide authentication. They prove that who we are connecting to is really who they say they are. Simply put, a certificate is a "certification" of where the information is coming from. A certificate contains the public key of the organization encrypted with either its private key or the private key of a signing authority. Using a signing or certificate authority is considered the more secure method of the two. If we can decrypt the certificate with their public key, then we can reasonably assume the Web site belongs to that organization.

Certificates are usually tied to a particular domain. They can be issued by a central entity, called a Certificate Authority (CA), or created and signed locally as described above. There are several of these organizations, the biggest of which is VeriSign, the company that also runs the domain names system. They have sanctioned many other companies to offer certificates under their authority. Getting a certificate from VeriSign or one of the companies it authorizes is like having someone vouch for us. VPNs also can use certificates for authentication instead of passwords.

6- Encryption Protocols

6.1- IPsec

It's a well-known fact that the IP protocol as designed originally was not very secure. IP version 4 (IPv4), which is what most of the world uses for IP communications, doesn't provide any kind of authentication or confidentiality. Packet payloads are sent in the clear, and packet headers can easily be modified since they are not verified at the destination. Many Internet attacks rely on this basic insecurity in the Internet infrastructure. A new IP standard, called IPv6, was developed to provide authentication and confidentiality via encryption. It also expanded the IP address space by using a 128-bit address rather than the 32-bit currently used and improved on a number of other things as well.

Fully implementing the IPv6 standard would require wide-scale hardware upgrades, so IPv6 deployment has been pretty slow. However, an implementation of security for IP, called IPsec, was developed that wouldn't require major changes in the addressing scheme. Hardware vendors have jumped on this, and IPsec has gradually become a de facto standard for creating Internet VPNs.

IPsec is not a specific encryption algorithm, but rather a framework for encrypting and verifying packets within the IP protocol. IPsec can use different algorithms and can be implemented in whole or just partially. A combination of public key and private key cryptography is used to encrypt the packet contents, and hashes add authentication as well. This function is called Authentication Header (AH). With AH, a hash is made of the IP header and passed along. When the packet arrives at the destination, a new hash is made of each header. If it doesn't compare to the one sent, then you know the header has been altered somehow in transit. This provides a high level of assurance that the packet came from where it says it does. You may choose to do encryption of the packet payload but not do AH, as this can slow down the throughput. AH can also get fouled up in some environments with NAT or firewalls.

6.2- Point-to-Point Tunnelling Protocol (PPTP)

PPTP is a standard that was developed by Microsoft, 3Com, and other large companies to provide encryption. Microsoft has added it to Windows 98 and later releases. This made it seem a likely candidate to be the major standard for widespread encryption technology. However, some major flaws were discovered in PPTP, which limited its acceptance. When Microsoft bundled IPsec with Windows 2000, it seemed a tacit admission that IPsec had won as the new encryption standard. However, PPTP is still a useful and inexpensive protocol for setting up VPNs between older Windows PCs.

6.3- Layer Two Tunnelling Protocol (L2TP)

This is another industry-developed protocol, and is endorsed by Microsoft and Cisco. Although used frequently in hardware-based encryption devices, its use in software is relatively limited.

6.4- Secure Socket Layer (SSL)

This protocol was designed specifically for use on the Web, although it can be used for almost any type of TCP communications. Netscape originally developed it for their browser to help stimulate e-commerce. SSL provides data encryption, authentication on both ends, and message integrity using certificates. Most of the time, SSL is used when connecting to a Web server so that we know the information we send it is being protected along the way. Most people don't even realize that SSL is running in the background. Usually it only authenticates one end, the server side, since most end users don't have certificates.

7- ENCRYPTION APPLICATIONS

Phil Zimmerman is a programmer who was heavily involved with human rights. He was concerned that the growing use of computers and communication networks would make it easier for the state security agencies of repressive regimes to intercept and gather information on dissidents. Phil wanted to write some software that would help these people keep their information private and safe from the eyes of the brutal regimes that ruled them. This software could quite literally save people's lives. He also didn't entirely trust his own government not to observe his personal data as it travelled across interconnected networks. He knew how easy it would be for the government to build systems to search every line of every e-mail for certain key words. He wanted to provide people with a way to protect and guarantee their constitutional right to privacy.[3]

8- SECURITY IN MOBILE DEVICES

Mobile data security is defined as an effort to secure data on mobile devices such as tablets and smart phones. Generally, mobile security is something which enterprises work on to safeguard sensitive information whose security can be compromised because of its use on several mobile devices. Mobile data security becomes more and more important each day as mobile devices have gone from communication tools to cameras for still and video photography and mini computers for emailing, searching, maps etc.

Mobile Data Security becomes more and more important each day as mobile devices have gone from communication tools to cameras for still and video photography and mini computers for emailing, searching, maps etc.

Mobile devices which transmit enterprise data & access corporate networks pose a risk in terms of keeping sensitive information secure. It is necessary to prevent corporate data from getting exposed through users' devices. There are several tools available including encryption, remote wipe, (MDM) mobile device management applications and more.

9- CHALLENGES IN MOBILE SECURITY

Mobile devices which transmit enterprise data & access corporate networks pose a risk in terms of keeping sensitive information secure. It is necessary to prevent corporate data from getting exposed through users' devices. There are several tools available including encryption, remote wipe, (mdm) mobile device management applications and more.

10- CONCLUSION

We could see that we have to face a lot of challenges while dealing with images on insecure mobile devices. To handle that, we have a few mechanisms. But still, due to increasing volume of data used and transferred, we need combinations of these techniques.

11- ACKNOWLEDGMENTS

Our thanks to the experts who have contributed towards development of the template.

12- REFERENCES

[1] Abhishek Vichare, Tania Jose, Jagruti Tiwari, "Data security using authenticated encryption and decryption algorithm for Android phones", Computing, Communication and Automation (ICCCA) International Conference, 2017, Electronic ISBN: 978-1-5090-6471-7, Print on Demand(PoD) ISBN: 978-1-5090-6472-4, pp 789 - 794, May 2017 13

[2] Sourabh Chandra, Smita Paira, Sk Safikul Alam , "A comparative survey of Symmetric and Asymmetric Key Cryptography", IJCSE, Electronic ISBN: 978-1-4799-5748-4 DVD ISBN: 978-1-4799-5747-7 INSPEC Accession Number: 15059055 DOI: 10.1109/ICECCE.2014.7086640 , pp 83 – 93 Nov. 2014

[3] Agrawal Monika, Mishra Pradeep, "A Comparative Survey on Symmetric Key Encryption Techniques", International Journal on Computer Science and Engineering (IJCSE), Vol. 4, pp. 877-882, May 2012

[4] Seth ShashiMehrotra, Mishra Rajan, "Comparative analysis of Encryption algorithm for data communication", International Journal of Computer Science and Technology, vol. 2, Issue 2, pp. 292-294. June 2011

[5]https://en.wikipedia.org/wiki/encryption

[6] https://ico.org.uk/media/for-rganisations/guide-to-data-protection/encryption-1-1.pdf

[7] http://books.gigatux.nl/mirror/securitytools/ddu/ch09lev1sec1.html