ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

A STUDY ON NETWORK SECURITY TECHNIQUES

Dr.T.Hemalatha*, Dr.G.Rashita Banu,Dr.Murtaza Ali
Assisstant.Professor,Vels University,Chennai.
Assistant Professor,Department of HIT&HIM,Jazan University,Jasan.
HOD, Department of HIT&HIM,Jazan University,Jasan.

ABSTRACT

Internet plays a vital role in our day today life. Data security in web application has become very crucial. The usage of internet becomes more and more in recent years. Through internet the information's can be shared through many social networks like Facebook, twitter, LinkedIn, blogs etc. There is chance of hacking the data while sharing from one to one. To prevent the data being hacked there are so many techniques such as Digital Signature, Cryptography, Digital watermarking, Data Sanitization can be implemented. This paper focus on the various techniques which is used to protect the data.

KEYWORDS: Cryptography, Data Security, Digital Signature, Digital water marking, Data Sanitization.

INTRODUCTION

In recent era, Social networking has become a foremost activity in the Internet today, attracting hundreds of millions of users, spending billions of minutes on such services. Facebook has more than 500 million users and recently surpassed Google in visits . At the same time, LinkedIn hosts profiles for more than 70 million people and 1 million companies .Protecting the data in internet is a critical activity in the world where computing is ubiquitous and information system are interconnected globally. Network security plays an important role in protecting the data from hackers. This paper focuses on various security techniques

NETWORK SECURITY TECHNIQUES

The various security techniques which is used to protect the data from hackers are cryptography, digital water marking, Data sanitization etc.

DIGITAL SIGNATURE

A digital signature algorithm is mathematical scheme which provides authenticity of a digital message and assure the recipient that the message was created by an authorized sender. Digital signatures are often used to implement electronic signatures, a broader term that refers to any electronic data that carries the intent of a signature. Digital signatures employ a type of asymmetric cryptography. For messages sent through a nonsecure channel, a properly implemented digital signature gives the receiver reason to believe the message was sent by the claimed sender. Digital signatures are equivalent to traditional handwritten signatures in many respects, but properly implemented digital signatures are more difficult to forge than the handwritten type. Digital signature schemes, in the sense used here, are cryptographically based, and must be implemented properly to be effective. Digital signature scheme typically consists of three algorithms:

- A key generation algorithm that selects a private key uniformly at random from a set of possible private keys. The algorithm outputs the private key and a corresponding public key.
- A signing algorithm that, given a message and a private key, produces a signature.
- A signature verifying algorithm that, given a message, public key and a signature, either accepts or rejects the message's claim to authenticity

There are many types of digital signatures they are

DIRECT DIGITAL SIGNATURE.

The direct digital signature involves only the communicating parties, sender and receiver. This is the simplest type of digital signature. It is assumed that the recipient knows the public key of the sender. In a simple scheme, a digital signature may be formed by encrypting the entire message or the hash code of the message with the sender's private key. Confidentiality can be provided by further encrypting the entire message plus signature with either the receiver's public key encryption or the shared secret key, which is conventional encryption. A sender may later deny sending a particular message by claiming that the private key was lost or stolen and that someone else forged his signature. One way to overcome this is to include a time stamp with every message and requiring notification of loss of key to the proper authority. In case of dispute, a trusted third party may view the message and its signature to arbitrate the dispute

ARBITRATED DIGITAL SIGNATURE.

In the arbitrated signature scheme, there is a trusted third party called the arbiter. Every signed message from a sender A to a receiver B goes first to an arbiter T, who subjects the message and its signature to a number of tests to check its origin and content. The message is then dated and sent to B with an indication that it has been verified to the satisfaction of the arbiter. The presence of T solves the problem faced by direct signature schemes, namely that A might deny sending a message. The arbiter plays a sensitive and crucial role in this scheme, and all parties must trust that the arbitration mechanism is working properly. There are many variations of arbitrated digital signature schemes. The particular scheme employed depends on the needs of the applications. Generally, an arbitrated digital signature scheme has advantages over a direct digital signature scheme such as the trust in communications between the parties provided by the trusted arbiter and in the arbitration of later disputes, if any.

ADVANTAGES OF DIGITAL SIGNATURES

The following are the main benefits of using digital signatures:

♣Speed: Businesses no longer have to wait for paper documents to be sent by courier. Contracts are easily written, completed, and signed by all concerned parties in a little amount of time no matter how far the parties are geographically.

♣Costs: Using postal or courier services for paper documents is much more expensive compared to using digital signatures on electronic documents.

♣Security: The use of digital signatures and electronic documents reduces risks of documents being intercepted, read, destroyed, or altered while in transit.

♣Authenticity: An electronic document signed with a digital signature can stand up in court just as well as any other signed paper document.

♣Tracking: A digitally signed document can easily be tracked and located in a short amount of time.

♣Non-Repudiation: Signing an electronic document digitally identifies you as the signatory and that cannot be later denied.

♣Imposter prevention: No one else can forge your digital signature or submit an electronic document falsely claiming it was signed by you.

♣Time-Stamp: By time-stamping your digital signatures, you will clearly know when thedocument was signed

DIGITAL WATER MARKING

Digital watermarking is a tool that provides and ensures data security, authentication, and copyright ownership to the digital media. This is a technique used to embed information into a digital data which cannot be easily retrieved by the third party.

CHARECTERISTICS OF DIGITAL WATERMARKING

There are four fundamental factors commonly used to determine the excellence of watermarking scheme. They are robustness, imperceptibility, security and capacity.

Robustness

Watermarked data cannot be detached by any unauthorized users. It should remain secure even after some signal processing such as cropping, transformation, compression, etc.

Imperceptibility
Watermark and the cover image should be perceptually identical that is, the observer cannot see any information embedded in the contents. Once the content is watermarked it should not affect the quality of the cover image. In case of any dispute over the digital media data, embedded watermark can be extracted and it can be used to identify the owner

Security
Watermarked data has been highly secured. Illegal access is denied. No one can detect, retrieve or modify the embedded watermark.

Capacity
Capacity defines the number of bits a watermark encodes within a unit of time or work. This factor describes how much data should be embedded as a watermark to successfully detect during extraction. Watermark should be able to carry huge information to signify the uniqueness of the image or video

DIGITAL WATERMARKING TECHNIQUES

Digital watermarking techniques can be broadly classified into two. They are spatial domain frequency domain watermarking.

SPATIAL DOMAIN WATERMARKING

The term spatial domain defines an aggregate of pixels composing an image. This technique directly modifies the intensity or color values of the selected pixels. This is an earliest and the simplest watermarking technique. Spatial domain method is denoted by the expression,g(X,Y)=T[f(X,Y)].This can be further classified into two namely LSB and SSM

FREQUENCY DOMAIN WATERMARKING

The frequency domain technique first transforms an image into a set of frequency domain coefficients. This frequency technique includes Discrete cosine transformation(DCT), Discrete Fourier transformation(DFT) and Discrete wavelet transformation(DWT)

APPLICATIONS OF WATERMARKING

The main applications of digital watermarking are
COPYRIGHT PROTECTION
Watermarking is used to protect redistribution of copyrighted material through internet. Illegal copying is also prevented through embedding technique.

AUTHENTICATION
Authentication is all about the rights to access. It is the process of confirming an individual identity. Watermarking is also used for identity proof. For example a logo embed onto the paper, ensuresthe authenticity of the document and also the text or an image watermarked on ID-cards,credit cards and ATM cards identifies the appropriate bank and the card holder

SECURITY
Digital data such as text,image, audio and video are highly protected through some special watermarking technique. Watermarked content is not easily tampered by any unauthorized
person. It has been highly secured.

BROADCAST MONITORING
Broadcast Monitoring is a technique of cross-verifying whether the content that was supposed to be broadcasted on TV or Radio has really been broadcasted or not. Watermarking is also a part of broadcast monitoring to ensure whether this particular advertisement or program has been sponsored only by the concern channel in the stipulated time and duration.

TAMPER DETECTION
A fragile watermark technique has been used for tamper detection. If the fragile watermark is damaged or corrupted, it indicates the presence of tampering and hence the digital content is ruined. Tamper detection is very important for some applications that involve highly sensitive data like satellite imagery or medical imagery.

DIGITAL FINGERPRINTING
Digital Fingerprinting is a technique used to identify the possessor of the digital content. A fingerprinting is a technique by which a work can be assigned with a unique identification by storing some digital content in it in the form of watermark. Detecting the watermark from any illegal copy can lead to threat.

DATA SANITIZATION

Data Sanitization is the process of disguise sensitive information and overwriting it with realistic looking but false data of a similar type. Heuristic methods have been proposed to choose the appropriate data for sanitization in order to hide the sensitive information. The following methods are used for Data sanitization they are
Masking Data
Shuffling Record
Substitution Method
Encryption/Decryption

MASKING DATA

Masking data means replacing certain fields with a Mask character(with x) .This effectively disguises the data content while preserving the same formatting on front end screens and reports. The masking characters effectively remove the sensitive information from the record while still preserving the look and feel.

SHUFFLING RECORD

The shuffling method is a very common form of data obfuscation, it is similar to the substitution method but it derives the substitution set from the same column of data. The data is randomly shuffled within the column. The shuffling method is also open be reversed if the shuffling algorithm can be deciphered. Shuffling is a great technique to include in your overall masking approach as it has some real strength. If for instance, to maintain the end of year figures for any financial information in the test database. We can mask the first name of the suppliers and then shuffle the value of their accounts throughout the masked database. If even someone with intimate knowledge of the original database could derive a true data record back to its original values. Shuffling is effective when used on small amounts of record. Shuffle rules are best used on large tables and leave the look and feel of the data intact. They are fast, but great care must be taken to use a sophisticated algorithm to randomize the shuffling of the rows and columns.

SUBSTITUTION TECHNIQUES

Substitution is one of the most effective methods of applying data masking and being able to preserve the authentic look and feel of the data records .Different types of substitution cipher. The cipher operates on single letters simple substitution cipher. The cipher that operates on larger groups of letters is poly graphic cipher. A mono alphabetic cipher uses fixed substitution over the entire message, polyalphabetic cipher uses a number of substitutions at different positions in the message, unit from the plaintext is mapped to the possibilities in the cipher text and vice versa

ENCRYPTION/DECRYPTION

Encryption is the process of encoding messages or information in such a way that only authorized parties can read it. Encryption does not itself prevent interception, but it denies the message content to the interceptor

CONCLUSION

In this paper the various techniques of network security are discussed and by using this technique will protect the data from the hackers. The researches can do research on any one of the technique and come out with a proposed new network security technique which will be more useful for the individuals as well as for organization which are using confidential data and also for databases.

REFERENCES

[1] Academia.edu.http://www.academia.edu/. Online; accessed 09 January 2014].
[2] A. Acquisti and R. Gross. Imagined communities: Awareness, informationsharing, and privacy on the facebook. In Privacy enhancing technologies, pages 36 –58. Springer, 2006.
[3] A. Acquisti, R. Gross, and F. Stutzman. Faces of facebook: Privacy in the age of augmented reality. BlackHat USA, 2011.
[4] Harshita Dudhe, Ankit Jain, "A Novel Hybrid Digital Watermarking using DWT, DCT and SVD", in IJDACR,Volume 2, Issue 10, May 2014
[5] Baisa L. Gunjal, R.R. Manthalkar," AN An Overview of Transform domain robust Digital Image Watermarking Algorithms",in Journal of Emerging Trends in Computing and Information Sciences,Volume 2 No. 1
[6] Mrs. Rashmi Soni1, Prof. M.K.Gupta2, "DigitalWatermarking of Wavelet Transforms Based on Coding and Decoding Techniques",in IJCSMC, Vol. 3, Issue. 3, March 2014, pg.1045 –1051.
[7] M.D Imaduddin and Ganji Pullarao,"Real Time Simulation Based on Image Protection Using Digital Watermarking Techniques",in International Journal of New Trends in Electronics and Communication (IJNTEC-ISSN: 2347 -7334) Vol. 2, Issue. 2, Mar. 2014.
[8] Dharm Singh, Naveen Choudhary, Madhuri Agrawal,"Spatial and Frequency Domain for Grey level Digital Images",in Special Issue of International Journal of Computer Applications (0975 –8887) on Communication Security, No.4. Mar.2012.
[9] Sonika Yadav1, Rahul Gupta," Sonika Yadav1, Rahul Gupta," DIGITAL WATERMARKING FOR COLOR IMAGES USING WAVELET TRANSFORM",Progress In Science and Engineering Research Journal ISSN 2347-6680 (E), PISER 13, Vol.02, Issue: 03/06 May-June, Page(s) 137-143.
[10] Lalit Kumar Saini1, Vishal Shrivastava2,"A Survey of Digital Watermarking Techniques and its Applications", International Journal of Computer Science Trends and Technology (IJCST) –Volume 2 Issue 3, May-Jun 2014
[11] Reshma Vartak1, Smita Deshmukh2," Survey of Digital Image Authentication Techniques",in International Journal of Research in Advent Technology, Vol.2, No.7, July 2014 E-ISSN: 2321-9637.
[12] Paramjit Kaur1 ,Dr. Vijay Laxmi2 ," Review on Different Video Watermarking Techniques",in International Journal of Computer Science and Mobile Computing, Vol.3 Issue.9, September-2014, pg. 190-195.
[13] Radhika v. Totla, K.S.Bapat,"Comparative Analysis of Watermarking in Digital Images Using DCT & DWT",in International Journal of Scientific and Research Publications, Volume 3, Issue 2, February 2013.
[14] Zhiwei Li, Warren He, Devdatta Akhawe, and Dawn Song, "The Emperor's New Password Manager: Security Analysis of Web-based Password Managers"pp.465-479 [5].
[15] Kolanoori Pravallika, B.Srinivas Reddy, "XSS Worm Propagation and Detection in Online Social Network" International Journal of Science and Research Impact Factor (2012) pp.458-460
[16] AsifMuhamma, NitinTripathi, "Evaluation of OpenID Based Double-Factor Authentication for Preventing Session Hijacking in Web Applications" Journal of Computer (2012) pp.623 -628
[17] Divya, Mahesh, R.Ushasree, "Data Implication Attacks on Social Networks with Data Sanitization" International Journal of Current Engineering and Technology (2014) pp.417- 422
[18] Ben Stock, Martin Johns, "Protecting Users Against XSS - based Password Manager Abuse" Journal of ACM (2014).
[19] Ben Stock, Sebastian Lekies, Tobias Mueller " Precise client-side protection against DOM -based Cross-Site Scripting" pp.478 – 486
[20] Abdul RazzaqZahid Anwar, H. Farooq Ahmad, Khalid Latif FaisalMunir, "Ontology For Attack Detection: An Intelligent Approach To Web Application Security" Journal of Elsevier (2014) pp.124 -146.