A Review On Methodologies And Performance Analysis Of Device Identity Masking Techniques

D.Prabakaran, H.Sathyapriya

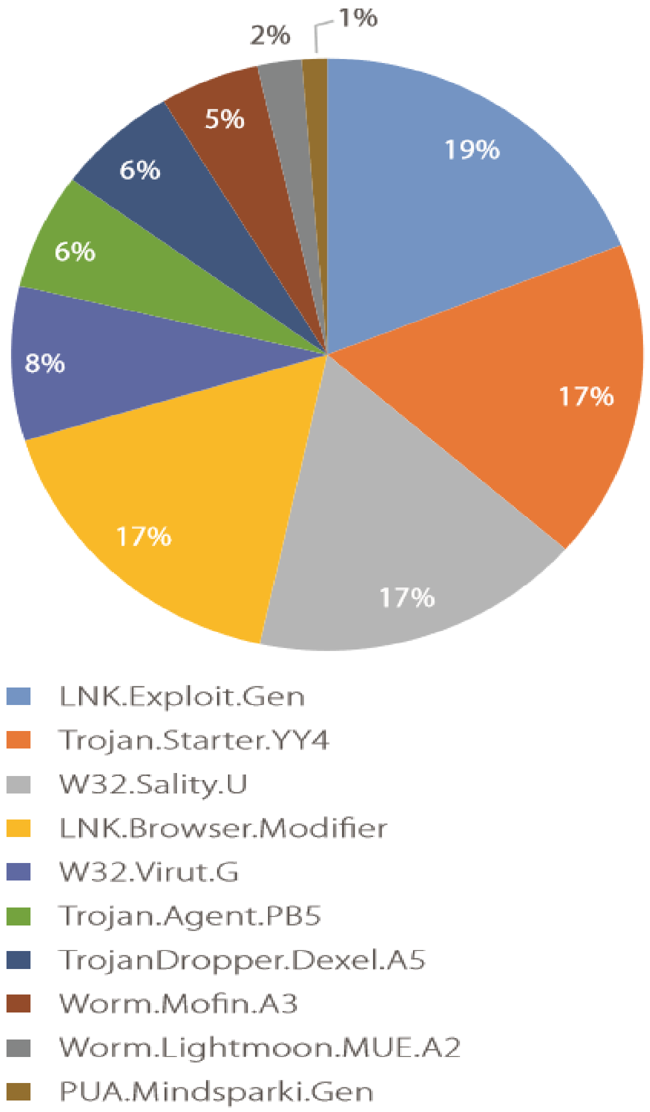
Abstract: The Ransomware is a malicious program,that attacks the compromised nodes of individual system and takes control on the sensitive files to demand revenue (bitcoins) from the administrator.The hacker acquires the information (Device identity)from the insecure proxy server.The device is located based on identity to scan for compromised node or port to perform the attack on system/network.To prevent this,a device identity masking system has been proposed.To avoid the revealing of device identity from hackers.

Keywords: Identitymasking,Cryptography,Administrator,Bitcoins,Private key and Public key.

1.INTRODUCTION

Hacking generally refers to unauthorized intrusion into a computer or a network. The hacker may alter system or security features to accomplish .a goal that differs from the original purpose of the system. Ransomware is a type of malicious software and it was developed in 1980s.It is a software from crypto- virology that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid. It attacks the compromised nodes of individual or organisation system. It takes control on the sensitive files to demand revenue(bitcoins) from the administrator. The hacker acquires the information from the insecure proxy server .The device is located based on the identity to scan for compromised node or port to perform the attack on system or network.To reduce the amount of hacking, Elliptical curve cryptography method is used.It is the method of implementation which uses some basic concepts to secure the device.The major part of the cryptography is encryption and decryption.The data which is encrypted contains all information of original transaction but not in human readable format.It is a public-key encryption technique which uses the same key for generating using elliptic curve equation . It is also a public key cryptographic system where the message is encrypted using private key of sender and decryption is done using sender's public key and the receiver private key. To protect from hackers, device identity is masking using elliptical curve cryptography. The mapping technique convert plain text into hexadecimal and the converted values are encrypted in reverse order to prevent security attacks. It provides better security using small key.The device identity is hidden using elliptical curve cryptography.

***TOP 10** WINDOWS MALWARE OF 2018*



Quick Heal detected over 181 million windows malware in 2018. They detected 1,325 ransomware per hour and 22 per minute.

It is explained as follows:-

- *Associate Professor, IFET College of Engineering, Villupuram, India-605108,erprabakarand@gmail.com*
- *UG Scholar, IFET College of Engineering, Villupuram, India-605108. hsathyapriya@gmail.com.*

LNK.Exploit.Gen's threatening level is very high.It is under the category of Trojan.The method of propogation is bundled software and freeware.It can be installed automatically through illegal browser extensions on windows systems.It may alter the systems or modify the files without the user knowledge.It also modifies the host files and hijacks the system IP address.After this installation,when the user launches the windows sytem next time the software will run automatically in background and collect all information what is happening further it sends to the hacker. Trojan,Starter.YY4's threatening level is also very high.It is under the category of Trojan.The method of propogation is malicious websites and email attachments.It is a process which able to dropped the file during the execution.It automatically downloads the keyloggers and file infectors.Through this installation,it will leads to crash of the infected sytem by modifying the settings of the computer. W32.Sality.U's threatening level is medium.It is under the category of Polymorphic file infector.The method of propogation is removable or network drives.It injects the code directly into running system process.It steals or hacks the user's confidential information and also deletes the security software. Due to this,the shutting down and process gets delay. LNK.Browser.Modifier' s threatening level is high and it is category of Trojan.The method of propagation is bundle software and freeware.It injects the code into browser to steal the information while browsing the banking credentials.It generates the ads to cause the malfunction.It is a virus which make changes to your browser and settings of the computer. W32.Virut.G's threatening level is medium.It is under the category of file infector and the method of propogation is bundled software and freeware.It is also a backdoor functionality which allow the additional files to be executed on the infected system.It introduce the botnet which is used for data theft and distributed denial of service attacks. Trojan.Agent.PB5 threatening level is medium and the method of propogation is removable disk or network drives.It is a multi-component malware which shortcuts the files functionality and further it spreads through removable drives.Its components are desktop.ini and random extension files.It uses the shortcut functionality and further spread through the removable drives.It display unnecessary advertisement while browsing. TrojanDropper.Dexel.A5 threatening level is high and its under the category of Trojan.The method of propogation is email attachments and malicious websites.It allows other malware into infected system and changes the settings of the computer.It redirects the user to malicious attack on the system.It slows down the system performance due to the trojan virus. Worm.Mofin.A3 threatening level is medium.It is under the category of Worm and the method of propogation is removable or network drives.It contains instructions which launches the malware automatically when the network drives is connected to system.The hackers search for documents such as .doc,.pdf,.xls. Worm.Lightmoon.MUE.A2's threatening level is very low.It is under the category of worm.The method of propogation is spam through email attachments P2P(peer to peer)sharing files.Through the installation,it ables to modify the system settings and registry applications.The information of the user such as folder,file and its names are sent to the unauthorized person.It arrives through the email attachments in spam mails.PUA.Mindsparki.Gen' s threatening level is medium.It is under the category of Potentially Unwanted Applications.The method of propogation is bundle software and freeware.It installs a toolbar powered by ask.com.It asks the user to download the software which is mentioned in the toolbar. It alters the infected system's browser homepage.

2 DEVICE IDENTITY MASKING METHODOLOGY

The key size and security are the factor to known its strength and limit. To maintain the security of the data transmission and device securable in the communication process, the algorithm which is used is known as cryptograhy. Cryptography consists of encryption and decryption. The device id and password are may be in mixed constants and variables. The plain text are converted into ASCII values. ASCII values are encrypted to image. Decryption is the reverse process of encryption. Cryptography itself consists of several algorithm such as Rivets Shamir Adelman (RSA) elliptic curve cryptography (ECC) and Advanced Encryption Standard (AES) According to the previous analysis, adaptative image steganographic method which obtains high payload with poor image quality using adaptation and radix which is a information hiding scheme. The embedding procedure converts secret message into numeral based on the image pixels variability. In the Reversible data hiding, it uses RDH method to convert embedding secret message into cover image. To improve the enhanced visual stego images. Data hiding scheme is used for converting embedded secret message into cover images using data hiding (DH) technology. Using the Data Hiding technology, the least significant bit (LSB) of cover image produce a stego image. Secured Text encryption is a cryptographic system.It uses mapping technique to encode the message on the elliptic curve based on the affine points. The message or text converts the concepts of public key encryption with equality test (PKEET) and identity-based encryption (IBE) to obtain identity-based encryption with equality test (IBEET). In this Identity -based encryption with equality test (IBEET) technique,it converts into ASCII values further it gets converted into hexadecimal values. The values are encrypted in reverse order for decryption. Phase-Selective Masking is a masking technique which uses radial frequency contours. It is phase dependent masking technique which is used to mask between the magnitude of masking and the adjacent central radial frequency (RF). It does not depend on radial frequency contours. to increase the phase effects. The curvature which is a phase dependent masking decreases the phase with increasing radial frequency. Person Reidentification proposed the Feature Mask Network (FMK) to predict the feature map mask by converting from high level features into low level features. It dynamically extracts the different or various parts for the complementary representation. Multiple -Image Encryption using binary phase, the greyscale image is decomposed into two-pure phase image using two dimensional binary phase mask technique to produce phase encoded image for optical interference. Authenticated key Agreement Protocol is technique based on the elliptical curve cryptography.It is an identity based Multi -Server authentication .It uses two key establish methods such as Key agreement and key transport.Key transport uses only one communicating party whereas key agreement uses two communicating parties. It is used to develop the elliptic curve.It is a public key based scheme such as key exchange,providing security ,encryption.The 32×32 Binary Linear Transformations proposed the transformation from 256-bit input block to 256-output block.In this,Branch number and number of fixed points techniques are used.The Branch number is used to represents the diffusion rate and security measures whereas the number of fixed points represents linear transformations changes from the input block to output block value. In Identity-Based Encryption with Equality test in Cloud computing,it combines the concept of Public Key encryption with Equality Test(PKEET) and Identity-Based Encryption(IBE) .The receiver uses secret value for identity and further sends to cloud server for the equality test.Implementation of Text Encryption using ECC system introduce a new technique known as Classic technique.The mapping of affine points on curve is not used.The values of ASCII are pairing in it.

3.DEVICE IDENTITY MASKING METHODOLOGY- A REVIEW

Hacking refers to the unauthorized intrusion into your system.They can easily modify your system or acquires your information from the insecure proxy server.Recently,Quick Heal Security labs detected 930 million Windows malware.Per day,30,000 Ransoware,2,41,000 Adware and 23,000 Exploits were detected.It is a polymorphic file infector.They also detected 13 Ransomware variants with improved encryption and anti-detection techniques.Several researches has been progress to overcome these Security issues.The Elliptical Curve Cryptography(ECC) uses the several techniques such as PKEET(Public Key Encryption with Equality Text),IBE(Identity-Based Encryption),IBEET (Identity-Based with Equality Test) etc.are the methods suggested to overcome the issues.A Survey has been proposed on the possible solutions for the security threats of Ransomware and it is listed below as follows. Mingwei Tang et al.(2015) proposed an information hiding using adaptation and radix method [1].The author suggested that ,it is used to improve the performance of information hiding scheme.Using the radix channel, the embed information is converted into cover image with high embedding capacity to prevent the information hiding on the curves

Rupali Bhardwaj et al.(2018) presented Dual-Image Reversible Hiding technique [2].It uses RSA algorithm for converting into base-3 numeral framework from secret binary message .This model will enhance or improve the visual stego images which provides the high embedding rate. Chin-NungYang et al.(2016)proposed image interpolation method[3] using Image Interpolation based Data Hiding (IIDH) scheme.The author adopted his method by using addition of secret message of the decimal values into pixels by cover images.It used for generating the cover images and enhancing the better the visual stego images. Keerthi.K et.al(2017) proposed a mapping technique for cryptographic system [4].It uses the mapping technique in which the plain text is converted into ASCII values, further it converts into hexadecimal values.The hexadecimal values are plotted in the x and y co-ordinates based on the inputs.This model is used to provide the security with lesser key size. Michael Slugocki et al. (2018) designed phase selective masking technique [5]which uses the radial frequency contours. The effects of phase depends on radial frequency in between the contours.This model proposed that the effect of phase masking does not changes the radial frequencies shapes between the contours.Finally,It increases the phase effects. Guodong Ding et al.(2019) proposed the Feature Mask Network(FMN) [6].The feature masking is used for high level resnet features.This model suggested that feature masking encodes the person identities accurately by using based network(BN) and Global Representation Network(GRN).It used to improve the image quality. Youhyun Kim et al.(2018) developed a two -dimensional binary phase mask for encryption [7].The original information is decomposed into two-pure phase only images.

The phase images will acts as a secret image and private keys .This technique proposed that decryption occurs only if the private key and binary phase masking is correct.It is used to protect our system from brute attacks. Sonali Nimbhorkar et al. (2016) developed a Authenticated Key Agreement protocol [8] using elliptical curve cryptography for cryptographic system.It uses two established methods such as Key agreement and Key transport protocol.The author proposed this model for greater security .And to transfer confidentially than RSA and DSA algorithm. Muharrem et al. (2013) proposed the 32×32Binary linear Transformations method [9].It is an algebraic construction for generating 32×32 matrices.It is used to transform 256-bit input values of the block into 256-bit output values .It is used to prevent attack from truncated differential cryptanalysis and impossible differential cryptanalysis. Sha Ma et al. (2015) presented identity-based encryption with equality test [10] using cryptography technique.It used the concepts of public key encryption and identity-based encryption with equality test.The receiver uses secret value for identity and further sends to cloud server for the equality test.This model proposed that to provide security from Bilinear Diffie Hellman algorithm attack. Reshma K V et al. (2015) developed a Dual-Tree Complex Wavelet Transform (DTCWT)system [11].From this,by

Combining the user identity and new identity it can be used for finger print privacy protection.The author suggested that,it provides high level of security and robustness is achieved. Yong Yu et al.(2016) proposed a Identity-Based Cloud Data Integrity Checking protocol [12].It allows or supports file which is mixed with variables size.The system develops the prototype in protocol.This model proposed that ,it provides the security even under the RSA algorithm .It is also easily implemented in real time systems. Kaitai Liang et al.(2014) designed a Mulit-Hop Identity-Based PRE(MH-IBPRE) [13].It maintains the text size constant and supports the re-encryption to increase the flexibility of information.The receiver can able to access the data by using corresponding private key.This system proposed that,it prevent the data against the selective identity and chosen-cipher text. Vinod Kumar et al.(2018) developed the cloud-assisted TMIS(Telecare Medical Information System) [14]based on the elliptical curve cryptography.It is used to enhance the security.The author suggested that compared to other relating protocols this model provides better security feature and attributes.It provides mananged efficiency and more security. Chuan Qin et al.(2018) proposed the Reversible Data Hiding(RDH) [15].It is based on the embedding mechanism.It describes that the separate capability for encrypted images using the reversible data hiding scheme .This proposed model is used for providing better visual quality and performance.It is used for high embedding rate based on adaptive mechanism.It is will provide better performance for hiding the data Bensenane et al.(2017) developed a 3D masking in a 2D identity recognition system [16].Using this,face recognition ,it will be used to detect the hackers.It uses the Angular Radial Transform (ART) technique whether it is capture image or face image through the extraction.This model proposed that, it will used to reduce the error rate between real face and face mask. Laiphrakpam Dolendro Singh (2015) introduced a new classic technique[17] for cryptographic system.The system removes mapping of characters to affine values on the elliptic curve.The ACII values for the respective plain text are paired up.The author suggested that it will avoid the mapping cost .It needs less power and storage. S.K hafizul Islam et al.(2015) presented the one -way hash function [18]for cryptographic system based on the elliptic curve cryptography.The system improved the third-party authenticated key exchange(3PAKE) without symmetric key.This model is more efficient and low computation cost.It is securable than other protocols. Dimas Natanaela et al.(2018) designed text encryption [19] using elliptic curve cryptography for android chat applications.It secure for messaging application while messaging in smartphone.The author describes that it maintains security during data transmission.It is more accuracy for the received text and needs average time for encryption and decryption. Toughi Shahriyar et al.(2017) proposed an encryption technique [20] based on the advanced encryption system.An image encryption method is implemented by using code computing and elliptic curve cryptography.This model suggested that letters is used for encryption.It is not fully securable. Naglaa F. Saudy at al. (2019)developed a error analysis and detection procedures [21] by using elliptic curve cryptographyIt uses the error detection code for the faulty detection.It will used for error analysis and detection during transmission.It decreases the key size and provides better security.It detects 99./. fault detection during the transmission. Srinivasan Nagaraj et al. (2015) presented a new image encryption technique[22] using matrix operations and elliptical curve cryptography. It can be implemented through DOTNET software .It will transfer data through unsecured channels.The author proposed that it will provides good security . Kirti Dhimani et al. (2017) introduced sharing color images by using two extended visual cryptography methods [23].The construction of original images is done by using first method whereas second is used to recover the original secret image.The author proposed that reduces complexity.It is lossless during the sharing of color images. Sunil Kumar et al. (2018) proposed a new cryptographic model [24].It is based on the intertwining logistic map for securable transmission,It uses 280-bit random key for sorting and diffusion process for generating the text.This model suggested that it provides improved security,sensivity and robustness .It reduces complexity. Manish Kumar et al. (2018) designed a cryptographic model for image encryption [25] .It uses the coupled mapping lattice to secure the images It uses 280-bit randomly for generating the secret keys further it divides into sub keys of each bit. This model proposed that it uses better security and performance.The image encryption is done by using coupled mapped lattice. From the above analysis, it is evident that numerous technologies and frameworks have been proposed to hide the identity of computing device such that to get rid from attacks like Ransomware through the compromised network gateways. The performance of each technology proves to be good in certain aspects and gives its maximum efficiency to oppose the inject of any foreign malicious packets into the device. The miserable point that one has to accept is the hackers has proved to be advanced in technology and the proof is the Ransomware worldwide attack in 2018. Hence we try to propose a new framework before which we tabulate the performance of best technologies framed till now.

TABLE- I: *COMPARISON OF DEVICE IDENTITY MASKING TECHNIQUES AND PERFORMANCE LEVEL*

Ref	Techniques	Level of Security
[1]	Information hiding using Adaptation and radix technique	High
[2]	Dual-Image Reversible Hiding technique	High
[3]	Image Interpolation method using IIDH scheme	Better
[4]	Mapping technique	High
[5]	Phase Selective Masking technique	Better
[6]	Feature Mask Network	Better
[7]	Two-Dimensional Binary Phase Mask Technique	Low
[8]	Authenticated Key Agreement Protocol	High
[9]	32×32 Binary Linear Transformations method	Better
[10]	Identity Based encryption with equality test	Low
[11]	Dual Tree Complex Wavelet Transform using ECC	High
[12]	Identity Based cloud data integrity protocol	High
[13]	Multi-Hop identity based technique	Medium
[14]	Cloud assisted TMIS	Better
[15]	Reversible Data Hiding	Better
[16]	Angular Radial Transform	Low
[17]	New classic technique	High
[18]	One-way Hash function method	High
[19]	Text encryption based on ECC technique	Medium

[20]	Encryption technique based on advanced encryption	Medium
[21]	Error analysis and detection technique using ECC	Medium
[22]	New image encryption technique based on matrix operations	High
[23]	Two extended visual cryptography method	Low
[24]	New cryptographic model based intertwining logistic mapping	Medium
[25]	Image encryption using cryptographic model	Better

PERFORMANCE COMPARISON- A DISCUSSION

Information hiding using adaptation and radix method and one way hash function technique security level is high but it needs higher memory.Comparing to this, ECC implementation is high effective than RSA. It provides greater security with same key size.It needs lesser memory and low power consumption.

V.CONCLUSION

From the above analysis ,these techniques are securable,reduces complexity.But it cannot be able to send data with higher security and it fails to secure the device.To overcome this,we proposed a model which helps to secure the device and data by using Image and data hiding technique using ECC.

REFERENCES

[1] Mingwei Tang, “An image information hiding using adaptation and radix”, ScienceDirect-Elsevier in Optik 126 (4136-4141),in 2015.

[2] Rupali Bhardwaj, “Hiding clinical information in medical images :An encrypted dual-image reversible data hiding algorithm with base-3 numeral framework”,Optik at August 2018.

[3] Chin-Nung Yang, , “Improving stego Image quality in image interpolation based data hiding”,at ScienceDirect-Computer standards &interfaces,pp.209-215 in October 2016.

[4] Keerthi K, “Elliptic Curve Cryptography for Secured Text Encryption”,International Conference on circuits Power and Computing Technology[ICCPCT],in 2017.

[5] Michael Slugockia, , “Phase -selective masking with radial frequency contours”,Elsevier-vision research 154,pp.1-13 in 2019.

[6] Guodong Ding,,“Feature Mask Network for Person Re-identification”,Elsevier-Pattern Recognition Letters in 2019.

[7] Youhyun Kim, “Interference -based multiple-image encryption using binary phase masks”,Elsevier-Optical and Lsaer in Emgineering 107,pp.281-287 in 2019.

[8] Sonali Nimbhorka, “Comparative Analysis of Authenticated Key Agreement Protocols Based on Elliptic Curve Cryptography”,ScienceDirect-Elsevier in Procedia Computer Science 78,pp.824-230 in 2018.

[9] Muharrem Tolga Sakkali, “On the algebraic construction of cryptographically good 32×32 binary linear transformations”,Journal of Computational and Applied Mathematics 259,pp.485-494 in 2014.

[10] Sha Ma, “Identity-based encryption with outsourced equality test in cloud computing”,Elsevier-Information Science in 2015.

[11] Reshma K V, “ Identity of User Thrashing and Privacy Protection of Fingerprints”,ScienceDirect-Elsevier in Procedia Computer Science 46,pp.652-659 in 2015.

[12] Yong Yu, “Colud Data Integrity Checking with an Identity-based Auditing Mechanism from RSA”,Elsevier-Fututre Genrations Computer Systems in 2016.

[13] Kaitai liang, “Choosen-ciphertext secure multi-hop identity- based conditional proxy re-encryption with constant-size ciphertexts”,Elsevier-Theorietical Computer Science in 2014. .

[14] Vinod Kumar, “ A Secure Elliptic Curve Cryprography Based Mutual AuthenticationProtocol for Cloud-assissted TMIS”,ScienceDirect-Elsevier in Telematics and Informatics 00,pp.1-21 in 2018.

[15] Chuan Qin, “ Reversible Data Hiding in Encrypted Image with Separable Capability and High Embedding Capacity”,ScienceDirect-Elsevier,Information sciences in 2018.

[16] Bensenane Hamdan, “The detection of spoofing by 3D mask in a 2D identity recognition system”,Elsevier in Egyptian Informatics Journal 19,pp.75-82 in 2018.

[17] Laiphrakpam Dolendro Singh, “Implementation of Text Encryption using Elliptic Curve Cryptography”,ScienceDirect-Elsevier in Procedia Computer Science 54,pp.73-82 in 2015.

[18] S.K. hafizul Islam, “An improved three party authenticated key exchange protocol using hash function and elliptic curve cryptography for mobile-commerce enviroments”,Journal of King Saud University -Computer and Information sciences in 2015.

[19] Chaun Qin, “Reversible Data Hiding in Encrypted Image with Separable Capability and High Embedding Capacity”,Information sciences in 2018.

[20] Dimas Natanael, “Text Encryption in Android Chat Applications using Elliptic Curev Cryptography”,ScienceDirect-Elsevier in Procedia Computer Science 135,pp.283-291 in 2018.

[21] Naglaa F.Saudy, “Error analysis and detection procedures for Elliptic curve Cryptography”,Ain Shams Engineering Journal in 2018.

[22] Toughi Shahriyar, “An Image Encryption Based on Elliptic Curve Pseudo Random and Advanced Encryption System,in Signal Proceesing in 2017.

[23] Srinivasan nagaraj, “Image Encryption using Elliptic Curve Cryptography”,ScienceDirect-Elsevier in Procedia Computer Science 48,pp.276-281 in 2015.

[24] Sunil Kumar, “A Secured Cryptographic model using intertwining logistic maps”,ScienceDirect-Elsevier Procedia Computer Science 143,pp.804-811 in 2018.

[25] Kirti Dhiman, “Extended visual cryptography techniques for true color images”,ScienceDirect-Elsevier in Computer and Electrical Engineering,pp.1-12 in 2017.