ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

Securing Confident Information by Automatic Self Poisoning

Ganesh Shanbhag[1], Keerthana[1], Mithun[1,] Rohan Salins[2], Melwin D`Souza[3], Pramila Billava[4]

B.E Student, Department of Computer Engineering, MITK, Kundapura, Karnataka, India[1]

Associate Professor, Department of Computer Engineering, SDIT, Mangalore, Karnataka, India[2]

HOD, Department of Computer Engineering, MIT, Kundapur, Karnataka, India[3]

Associate Professor, Department of Computer Engineering, MIT, Kundapura, Karnataka, India[4]

ABSTRACT: The open nature of the wireless medium leaves it vulnerable to intentional interference attacks, typically referred to as Poisson pot. This intentional interference with wireless transmissions can be used as a launch pad for mounting Denial-of-Service attacks on wireless networks. Typically, poison pot has been addressed under an external threat model. However, adversaries with internal knowledge of protocol Specifications and network secrets can launch low-effort attacks that are difficult to detect and counter. In this work, we address the problem of selective Poisson pot attacks in wireless networks. In these attacks, the adversary is active only for a short period of time, selectively targeting messages of high importance. In this project when the hacker tries to attack confidential information of the user, and virus will be automatically downloaded to the hacker's device and all the information regarding the hacker will be automatically sent to the user in no time. This can be an ideal one when your device is hacked or is about to be hacked.

KEYWORDS: Asymmetric, encryption, TPA

I.INTRODUCTION

Wireless networks rely on the uninterrupted availability of the wireless medium to interconnect participating nodes. However, the open nature of this medium leaves it vulnerable to multiple security threats. Anyone with a transceiver can eavesdrop on wireless transmissions, inject spurious messages, or jam legitimate ones. While eavesdropping and message injection can be prevented using cryptographic methods, jamming attacks are much harder to counter. Here we introduce another reliable method which can not only reduce the threat of getting hacked, but also the person who has hacked can be easily identified. Here when a unidentified or unauthorized person tries to read or extract confidential data from your account, an virus will be automatically downloaded in the hackers device resulting which all the information regarding the hacker will be automatically sent to the user using which the user can easily identify the person who is behind his hacking and can also take required measures in order to stop this.
Sometimes it is better to recreate or resend very confidential data or information rather than losing message by hacking it. Hacking of confidential data may lead to very serious problems. Every single person may have many confidential data that has to be reached to the proper person over the internet. But now a days hacking is the greatest problem. So this is our approach to save the very confidential message from hacking and to analyse the details of hacking.

II.RELATED WORK

Many security mechanisms are used to develop this project. They are discussed below.
Cryptography:
Cryptography is the practice and study of techniques for secure communication in the presence of third parties. More generally, cryptography is about constructing and analysing protocols that prevent third parties or the public from

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

reading private messages. various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation are central to modern cryptography.

Cryptography prior to the modern age was effectively synonymous with encryption, the conversion of information from a readable state to apparent nonsense. The originator of an encrypted message shared the decoding technique needed to recover the original information only with intended recipients thereby avoids unwanted persons from doing the same.

Brute Force Attack:

Nothing stops a cryptanalyst from guessing one key, decrypting the cipher text with that key, looking at the output, and if it was not the correct key then moving on to the next key. The technique of trying every possible decryption key is called a brute-force attack.

Brute force attacks work by calculating every possible combination that could make up a password and testing it to see if it is the correct password. As the password's length increases, the amount of time, on average, to find the correct password increases exponentially. This means short passwords can usually be discovered quite quickly, but longer passwords may take decades.

III. EXPERIMENTAL RESULTS

Information about each nodes or devices which are going to participate in the communication is identified using unique IP address. So only the authorized person can participate in the communication to make the system more secure. Below snap shot shows the login form. IP address is used for providing authentication. Fig 1 shows the login process.

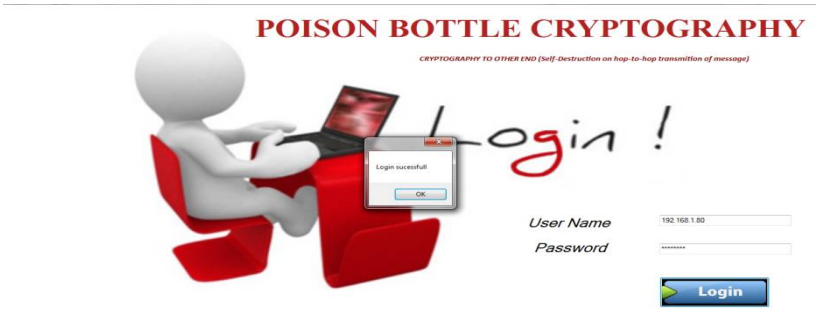

fig: 1

Before sending the confidential data, sender has to encrypt the message. Since this project is based on symmetric key cryptosystem, sender needs a key to encrypt and decrypt the message. So sender requests TPA for the key.

TPA is a private service, which generates and provides key to the destination. While sending the message sender should specify TTL. Time To Live is the time within which the message has to be transmitted. If TTL exceeds the message gets dropped.

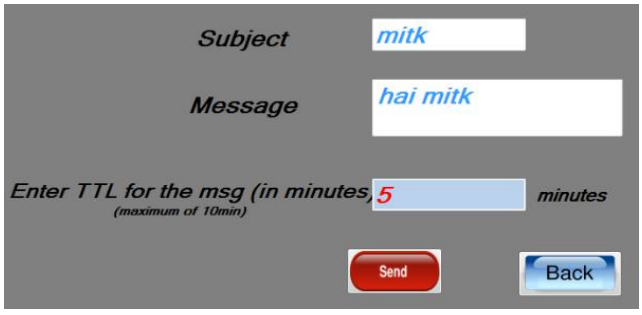

fig: 2

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

Since this project uses the symmetric method of encryption, both sender and receiver should have the same key. If unauthorised person uses hacking techniques like brute force or any other, he should try for all possible combination of keys. If in case the key mismatch found, immediately poison will be released and the very confidential data will be corrupted. The information about the hacker is collected and the acknowledgment about the hacking will be sent to the receiver.

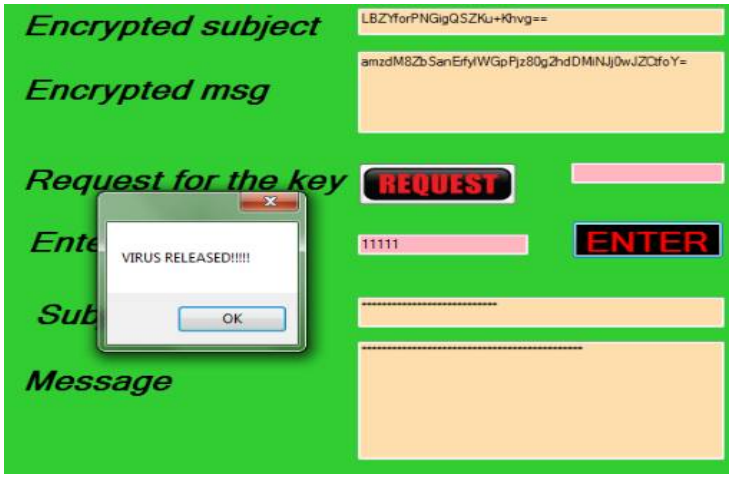

fig: 3

Even if the confidentail data gets hacked before reaching the receiver as shown in fig:3, the data will not be made available to the hacker but still corrupted message is communicated to the receiver. This communication with the corrupted data helps to track the hacker information. The receiver can take legal action.The below snapshot shows the blocking option at receiver side. If any IP adress gets blocked, then that node can't take part in the communication.

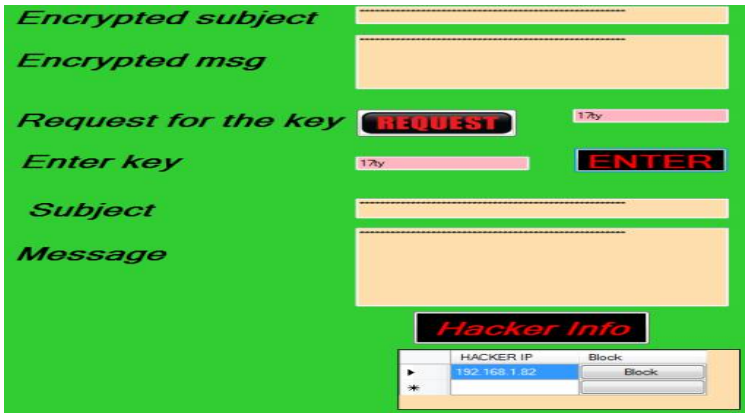

Fig: 4

Above fig: 4 show the information about hacking. Acknowledgment about the communication is sent to the sender. If the message gets hacked, the acknowledgment about hacking is sent to the sender. If TTL exceeds and the message dropped in between the communication, that information is also sent to the sender. So sender can resend the message.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

IV. CONCLUSION

This project mainly concerns about information and network security. We believe that it is better to recreate the data rather than facing the problem by hacking it. So, our concept ensures that the message will be made available only to the intended receiver.

REFERENCES

[1] Data Hiding and Retrieval, A.Nath, S.Das, A.Chakrabarti, Proceedings of IEEE International conference on Computer Intelligence and Computer Network

[2]T Morkel, JHP Eloff " ENCRYPTION TECHNIQUES: A TIMELINE APPROACH" published in Information and Computer Security Architecture (ICSA) Research Group proceeding.

[3] Majdi Al-qdah & Lin Yi Hui "Simple Encryption/Decryption Application" published in International Journal of Computer Science and Security