© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 07 Issue: 06 | July – September 2016
Paper is available at www.jrps.in | Email : info@jrps.in

Enhancing security of Wireless Network from External Attacks

[1]Monika Rani, Research Scholar, prachi.Rose14@Gmail.Com
[2]DR. VIKRAM SINGH, vikramsinghkuk@yahoo.com

Abstract: A wireless network is any type of computer network that uses wireless data connections for connecting network nodes. Wireless networking is a method by which homes, telecommunications networks & enterprise (business) installations avoid costly process of introducing cables into a building, or as a connection between various equipment locations. Wireless personal area networks (WPANs) interconnect devices within a relatively small area that is generally within a person's reach. For example, both Bluetooth radio & invisible infrared light provides a WPAN for interconnecting a headset to a laptop. Zig Bee also supports WPAN applications. Wi-Fi PANs are becoming commonplace (2010) as equipment designers start to integrate Wi-Fi into a variety of consumer electronic devices. A hacker is somebody who exploits & seeks weaknesses within a computer network or computer system. A hacker can be motivated by a multitude of reasons, such as profit, challenge or protest. Grouping that has evolved everywhere hackers is often referred to as computer underground & these days they are well known community.

Keyword: transmitter, Communications, Framework, Cryptography, Cellular, telecommunications, equipment

[1] INTRODUCTION

A wireless network is any type of computer network that uses wireless data connections for connecting network nodes. Wireless networking is a method by which homes, telecommunications networks & enterprise (business) installations avoid costly process of introducing cables into a building, or as a connection between various equipment locations. Wireless telecommunications networks are generally implemented & administered using radio communication. This implementation takes place at physical level (layer) of OSI model network structure. Examples of wireless networks include cell phone networks, Wi-Fi local networks & terrestrial microwave networks.

Computers are very often connected to networks using wireless links.

[2] LITERATURE REVIEW

Xavier Boyen et al[5] Distributed-password public-key cryptography (DPwPKC) allows members of a group of people, each one holding a small secret password only, to help a leader to perform private operation, associated to a public-key cryptosystem. Abdalla et al. recently defined this tool , with a practical construction. Unfortunately, latter applied to ElGamal decryption only, & relied on DDH assumption, excluding any recent pairing-based cryptosystems. In this paper, we extend their techniques to support, & exploit, pairing-based properties: we take advantage of pairing-friendly groups to obtain efficient (simulation-sound) zero-knowledge proofs, whose security relies on Decisional Linear assumption. As a consequence, we provide efficient protocols, secure within standard model, for ElGamal decryption as within , but also for Linear decryption, as well as extraction of several identity-based cryptosystems . Furthermore, we strengthen their security model by suppressing useless test Pwd queries within functionality.

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 07 Issue: 06 | July – September 2016
Paper is available at www.jrps.in | Email : info@jrps.in

Michel Abdalla et al[6] Modern multi-user communication systems, including popular instant messaging tools, social network platforms, & cooperative-work applications, offer exible forms of communication & exchange of data. At any time point concurrent communication sessions involving different subsets of users could be invoked. The traditional tool for achieving security within a multi-party communication environment are group key exchange (GKE) protocols that provide participants with a secure group key for their subsequent communication. Yet, within communication scenarios where various user sub-sets may be involved within di_erent sessions deployment of classical GKE protocols has clear performance & scalability limitations as each new session should be preceded by a separate execution of protocol. The motivation of this work is to study possibility of designing more exible GKE protocols allowing not only computation of a group key for some initial set of users but also efficient derivation of independent secret keys for all potential subsets

Michel Abdalla et al[7] this paper presents notion of distributed password-based public-key cryptography. The users could jointly perform private-key operations by exchanging messages over an arbitrary channel, based on their respective passwords.

David Pointcheval et al[8] In Asiacrypt 2005, Abdalla *et al.* Propose new method i.e. gateway-based password authenticated key exchange (GPAKE) protocol, within which clients & gateways have to authenticate each other with help of an authentication server to establish a common session key. This paper also provides additional security features such as password protection with respect to malicious gateways & also privacy of key with respect to authentication servers. This paper presents stronger security model for GPAKE schemes, combining all above-mentioned security properties.

[3] RESEARCH METHOLOGY

The endpoint in an inter process communication is called a socket, or a network socket for disambiguation. Since most communication between computers is based on the Internet Protocol, an almost equivalent term is *Internet socket*. The data transmission between two sockets is organized by communications protocols, usually implemented in the operating system of the participating computers. Application programs write to and read from these sockets. Therefore, network programming is essential for socket programming.

CLIENT SERVER MODEL

It is possible for two network applications to begin simultaneously, but it is impractical to require it. Therefore, it makes sense to design communicating network applications to perform complementary network operations in sequence, rather than simultaneously. The server executes first and waits to receive; the client executes second and sends the first network packet to the server. After initial contact, either the client or the server is capable of sending and receiving data.

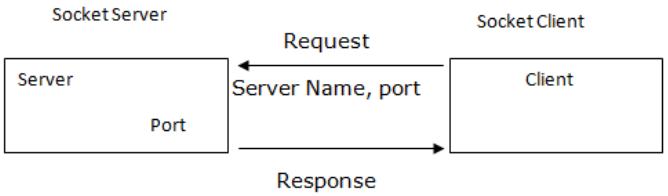


Fig 2 Once the connection is established between Server and Client, they can communicate (read or write) through their own sockets.

Researcher proposes to design & analyze a new server side module & client side module to transfer multimedia contents for wireless Network. Researcher also proposes a novel Key independent & fast & selective video Encryption Technique for Confidentiality of video stream delivered over wireless Network to end user. Deployment & Integration of above two techniques simultaneously for providing Confidentiality & Authentication of Video Delivered or received over self Deployed Wireless Network for Video on Demand Service.

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 07 Issue: 06 | July – September 2016
Paper is available at www.jrps.in | Email : info@jrps.in

To enhance network security of Digital Data by adding New Security Mechanisms. Research proposes to design easy to use graphical user interface for wireless Network.

Work is implemented in one of major used language named C#.NET.

[4] THE PROPOSED PROTOCOL

The data transmission between two sockets is organized by communications protocols, usually implemented in the operating system of the participating computers. Application programs write to and read from these sockets. Therefore, network programming is essential for socket programming. The endpoint in an inter process communication is called a socket, or a network socket for disambiguation. Since most communication between computers is based on the Internet Protocol, an almost equivalent term is *Internet socket*.

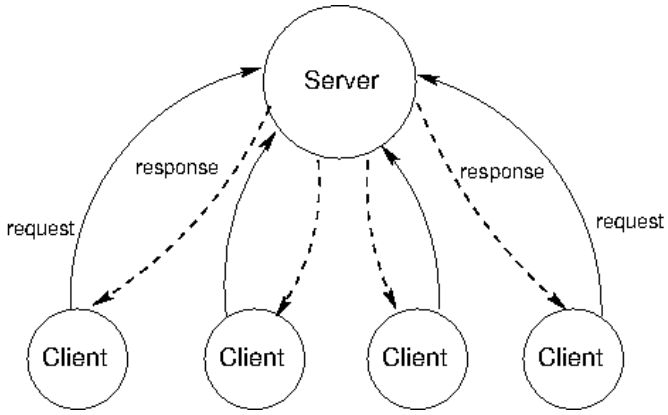


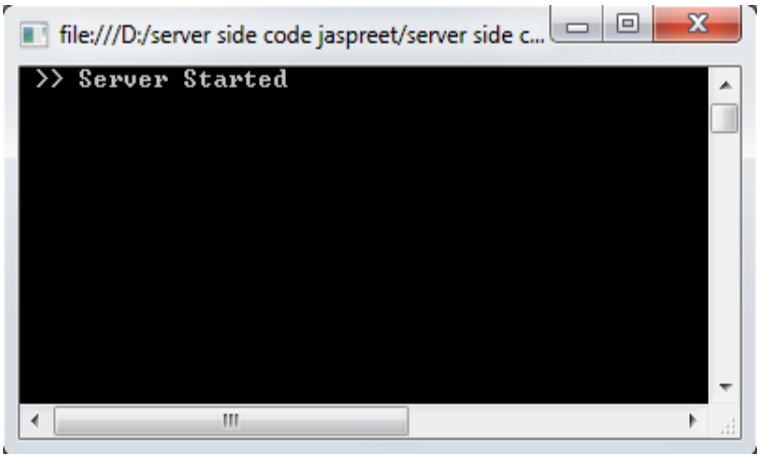
Fig 4 Data Transmission between client and server

Cryptography is the process of converting plaintext (ordinary text, just as message) using process encryption into cipher text using process decryption. Encryption is a method of transforming original data, called plaintext or clear text, into a form that appears to be random and unreadable, which is called cipher text. That text can be understood by a person by a computer. (Executable code) is called Plain text or clear text. After transformation into cipher text, then it is impossible to process this text by human as well as machine until it is decrypted.

In this research our aim is to enhance the security. For this purpose we develop server side and client side module, after that enabling transmission among client and server. To enhancement the security in wireless network by improving encryption and decryption algorithms. Within this research we would provide triple layer security first from username/password, second from one time password, third one with use of enhanced encryption & decryption techniques.

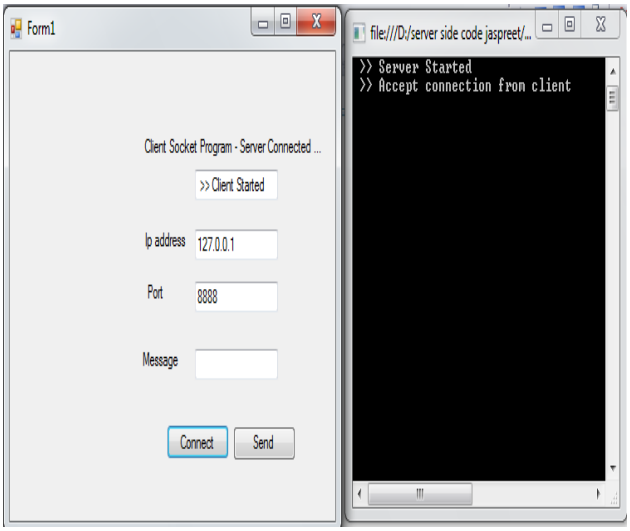
[5] RESULT AND ANALYSIS

We have to show the implementation on the server and client side and how to server and client communicated and transmissions of secure data.

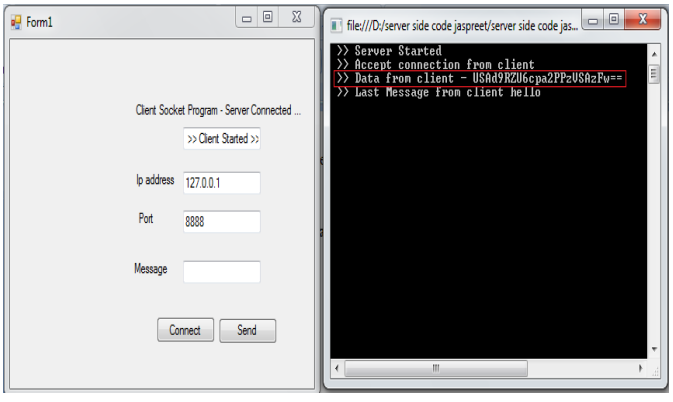


© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 07 Issue: 06 | July – September 2016
Paper is available at www.jrps.in | Email : info@jrps.in

The following figure shows the start of server side socket through .net framework. The Server Socket Program here is a C# Console based Application. This program act as a Server and listening to client's request. when the server starts, screen display a message such as 'server started'.



In this figure show that communication between server and client. The C# Client Socket Program is a windows based application. When the C# Client program execute , it will establish a connection to the C# Server program and send request to the Server , at the same time it also receive the response from C# Server .



In this figure Sending encrypted data to server from client and decryption of encrypted data on server side. When the C# Client program starts, it will connect to the C# Server Socket Program and start to reads data from NetworkStream, and also write to the NetworkStream. When you start the client program you will get a message from Server "client started". When press the button at the bottom of Client window, it will send a message to the Server and also receive response from the Server.

[6] CONCLUSION

Issue of ADHOC Network security is the demand of day. The proposed implementation has enhanced the security of ADHOC Network. Data transmission could be made more secure from hacker to by encrypting data on sender side and decrypt it on client side. To perform this we need to merge two technologies.

And on the part of .net play its best role to develop GUI interface to make system easy to operate by user

I. Socket Programming

II. Data Encryption.

[7] FUTURE SCOPE

A *socket* is one of the most fundamental technologies of computer networking. Sockets allow applications to communicate using standard mechanisms built into network hardware and operating systems. Although network software may seem to be a relatively new "Web" phenomenon, socket technology actually has been employed for roughly two decades.

Software applications that rely on the Internet and other computer networks continue to grow in popularity. Many of today's most popular software packages -- including Web browsers, instant messaging applications and peer to peer file sharing systems -- rely on sockets.

REFERENCES

[1] David Pointcheval, Olivier Blazy, *New Smooth Projective Hash Functions and One-Round Authenticated Key*

Exchange(18_22 august 2013, Santa Barbara, California, USA), Springer-Verlag, LNCS 8042, pages 449_475.

[2] David Pointcheval, Olivier Blazy, *Efficient UC-Secure Authenticated Key-Exchange for Algebraic Languages*(26 February - 1 March 2013, Nara, Japan)), 16th International Conference on Practice and Theory in Public-Key Cryptography (PKC '13)Springer-Verlag, Kaoru Kurosawa Ed., Springer-Verlag, 2013.

[3] David Pointcheval, *Password-based Authenticated Key Exchange.* (21-23 may 2012, Darmstadt, Germany)Springer-Verlag, LNCS 7293, pages 390-397.

[4] David Pointcheval, Michel Abdalla, *Contributory Password-Authenticated Group Key Exchange with Join Capability*, (February 14-18, 2011, San Francisco, CA, USA), A. Kiayias Ed. Springer-Verlag, LNCS 6558, pages 142-160.

[5] David Pointcheval, Xavier Boyen, *Strong Cryptography from Weak Secrets*, (3 – 6 may 2010, Stellenbosch, South Africa), D. Bernstein and T. Lange Eds., Springer-Verlag, LNCS 6055, pages 297–315.

[6] David Pointcheval, Michel Abdalla, *Flexible Group Key Exchange with On-Demand Computation of Subgroup Keys*, (3-6 May 2010, Stellenbosch, South Africa)), D. Bernstein and T. Lange Eds., Springer-Verlag, LNCS 6055, pages 351-368.

[7] David Pointcheval, Michel Abdalla, *Distributed Public-Key Cryptography from Weak Secrets*, (18_20 march 2009, Irvine, CA, USA), S. Jarecki and G. Tsudik Eds. Springer-Verlag, LNCS 5443, pages 139_159.

[8] David Pointcheval, Michel Abdalla, *Password-Authenticated Group Key Agreement with Adaptive Security and Contributiveness*, (21 – 25 June 2009, Gammarth, Tunisia) B. Preneel Ed., Springer-Verlag, LNCS 5580, pages 254–271.

[9] Rafael Álvarez, Leandro Tortosa, *Analysis and design of a secure key exchange scheme*, Information Sciences 179 (2009) , Elsevier

[10] David Pointcheval, Michel Abdalla, *Anonymous and Transparent Gateway-based Password-Authenticated Key Exchange*, December 2–4, 2008, Hong-Kong, China – M. Franklin, L. Hui and D. Wong Eds. Springer-Verlag, LNCS 5339, pages 133–148.

[11] Emmanuel Bresson, Olivier Chevassut, and David Pointcheval, *Provably-Secure Authenticated Group Diffie-Hellman Key Exchange*, ACM Transactions on Information and System Security, Vol. 10, No. 3. August 2007.

[12] Kumar Mangipudi, Rajendra Katti, *A Secure Identification and Key agreement protocol with user Anonymity (SIKA)*, journal homepage: www.elsevier.com/locate/cose, Computers & security 25(2006) 420 – 425.

[13] Chin-Chen Chang, Jung-San Lee, An anonymous voting mechanism based on the key exchange protocol, journal homepage: www.elsevier.com/locate/cose, Computers & security 25(2006) 307– 314.

[14] Tseng, Y.M., 2005, Weakness in simple authenticated key agreement scheme, *Electronics. Letters* 36 (1) pp. 48–49.