International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 03 | Mar-2018 www.irjet.net p-ISSN: 2395-0072

DEVICE AUTHENTICATION WIRELESS NETEWORK FOR SECURED COMMUNICATION

Chaithra N T[1], Dr. Mahesh K Kaluti[2]

[1]M Tech, CSE, Dept. of Computer Science and Engineering, PESCE, Mandya
[2]Guide, Dept of computer science and engineering, PESCE, Mandya

---

Abstract *- In day-to-day life, providing security for devices is very important as the intruders are finding ways to access the data in networks especially in wireless networks. When the communication takes place between 2 or more devices and if the devices are not authenticated, then it becomes very easy for the intruders to access the data that leads to fatal circumstances. This situation needs to be tackled and a solution is to be provided. So, we propose a simple, efficient authentication mechanism where in the devices authenticated at first and then the user in a particular group will be authenticated to share data or information.*

Keywords- Authentication*, Smart Card, Seed Box, Nonce Process, OTP*

INTRODUCTION

Wireless Internet access technology is being increasingly deployed in both office and public environments, as well as by internet users at home.

*Security in Computer world determines the ability of the system to manage, protect and distribute sensitive information. Security cannot rely on central servers, as there are no guarantees that they will be in radio range all times - devices' availability and motion are quite unpredictable in mobile ad hoc networks.

* Authentication for Devices is a new technique to provide security

for networks. This project proposes and implements a device authentication mechanism in which the devices that need to communicate with each other must belong to the same group and should be authenticated for communication by using Shamir's secret sharing algorithm.

Section 2

LITERATURE SURVEY

2.1 Device Authentication Using Novel Smart Card Software [10]

It is a simple device authentication framework which provides device-oriented authentication and authorization mechanisms for non-PC Internet-ready information appliances. The purpose of the framework is to prevent device spoofing, and to restrict unauthorized access to the device in a future ubiquitous network. Here the smart card will be attached to a device such as an information appliance. *Disadvantage:* If the card gets tampered or damaged then the device authentication will be a problem in this system.

2.2 Gesture based user authentication and face recognition system [11]

Here the user authentication is based on gestures and facial expression captured by a video camera. Unlike pure biometrics, such as fingerprints, iris scans, and faces, gesture-based authentication combines irrevocable biometric information, such as the shapes and relative sizes of body parts, with voluntary movements which can be revoked. *Disadvantage*: Movements and expressions need not always be same. So authentication using this method is not reliable.

Section 3

SYSTEM ARCHITECTURE

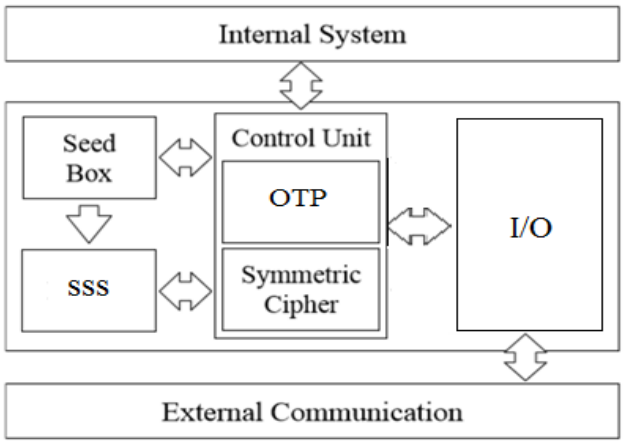

Fig 3a System Architecture

3.1 Device authentication and group authentication

Each device in a group should be registred from the seedbox separately. Once the registration is successful each device will be having preshared key within it. When two devices trying to communicate for any data exchange then we should allow only those devices within the group using nonce process. So that even though devices are "authenticated, it requires to authorise" for data exchange. This is shown in the figure Fig 3a.

- Seedbox performs Group Creation in that process, admin should give Group name & Group key and for each group,'N' number of polynomials will be generated.

- Seedbox is responsible to view requests and take appropriate action.

- Client node send a registration request for a particular group to seedbox/admin by providing its MACID,Owner Name and Group Name.

- Once the node approved for a particular group by the seedbox and get its key-value pairs, a node should be authorized to communicate with another node which is of same group.

3.2 User authentication

- Through login id and password, user authentication is done.

3.3 Modules used

The proposed mechanism should be placed between the internal system (e.g. software application) and the external communication (e.g. wireless interfaces), as a security middleware. The figure 3a shows the architecture of the proposed mechanism and its internal building blocks.

- The Seed Box is a storage unit responsible to hold all known pre-shared keys kn, where each kn corresponds to one different secure cluster. Each kn receives a mnemonic name, assigned by the device's owner, to be easily associated to a secure cluster.

- The I/O is the building block responsible for the communication of the mechanism with the network communication interfaces (the layer just below the mechanism).

- The Control Unit involves the functions, wherein a device enrolls itself for authentication (which involves nonce process which means generation of an arbitrary number called cipher text) for the purpose of communication.

- Shamir's Secret Sharing (SSS) implementation for secure key, authentication and Validation process.

- One Time password (OTP) is used to generate a challenge message.

- For encryption and decryption we use Symmetric Ciphering.

Section 4

HARDWARE AND SOFTWARE REQUIREMENTS

4.1 Hardware requirements

- 2GB RAM
- 80GB Hard disk
- ..Pentium IV and above processor
- At least 4 machines , 1 for administrator, 2 from one group cluster and another from different group cluster

4.2 Software requirements

- Operating System: Windows Version
- Software: Visual Studio 2010
- Language: C#
- Application: Windows Forms

Section 5

SYSTEM DESIGN

System design is the process of defining the architecture, components, modules, interfaces, and data for a system satisfy specified requirements. It implies a systematic and rigorous approach to design.

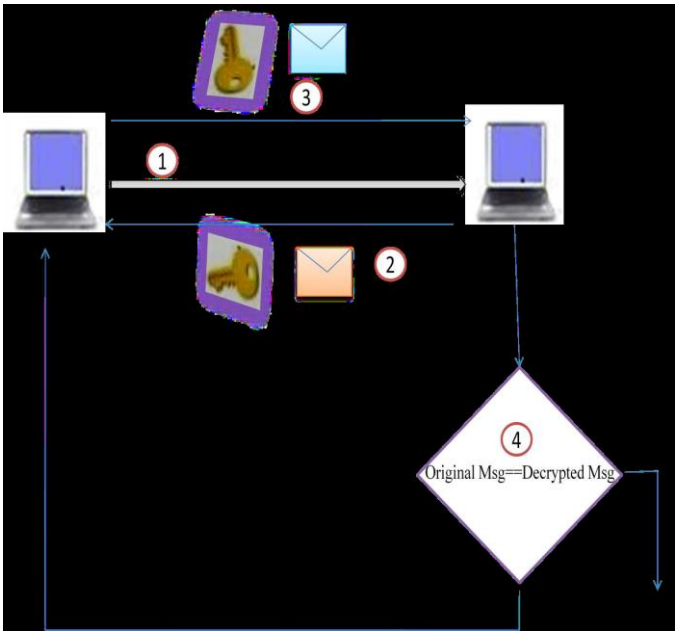

Fig.5a System design

In the beginning the device requests for the registration as shown in the figure Fig 4.1 by sending its MAC id, group name to which it wants to join.

- Resource manager manually checks for presence of the device
- If device is present then he sends he is approval to the device indicating that it is registered. Seed box contains the pre shared sets along with the unique pre shared key for a particular group.
- Once the device is registered for a particular group, seed box gives the pre shared set using which pre shared key has to be generated.
- Another device say D2 which is also registered sends the request for communication, with this device say D1 as shown in the figure Fig 4.1.
- D1 generates the one time password(OTP)
- This OTP generated is encrypted using the pre shared key to form cipher text.
- D1 sends the Cipher text to D2 ,D2 using its own pre shared sets generates pre shared key.
- Then using the preshared key cipher text is decrypted and it is sent back to D1.
- D1 checks if received message is equal to its own message. If same, two devices are allowed to communicate further.

Section 6

IMPLEMENTATION

System implementation is that stage of development life cycle, when the theoretically designed system is turned in actual working system. This phase is very critical so it must be carefully planned and controlled. Otherwise it can cause chaos. All possible constraints must be taken into consideration before implementing the system because the new system must assure the users about its effective working.

6.1. Modules Implementation

Our project is divided into two main sub parts or divisions- Node, Seed box.

6.1.1 Group Creation

At the server side the admin can create the different groups along with its secret key.

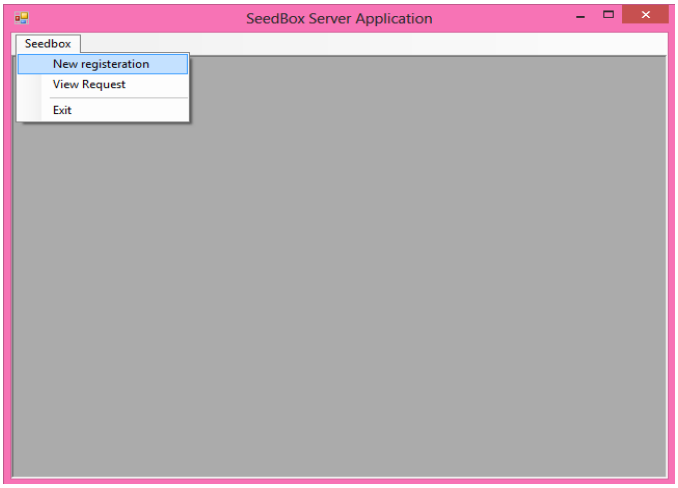

Fig 6.1.1a Seed box Operations Snapshot

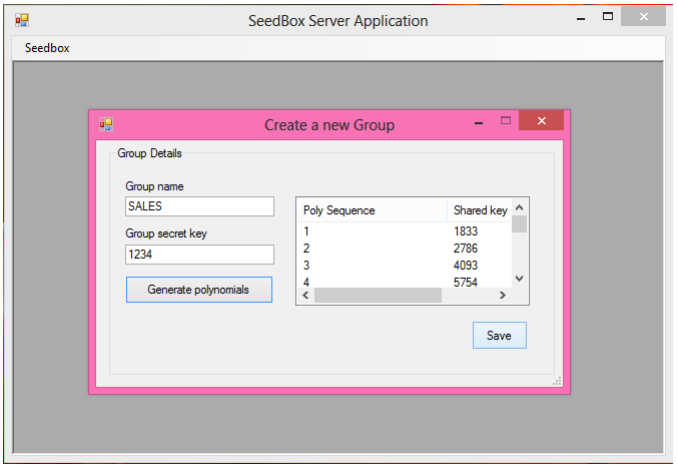

Fig 6.1.1b Group Creation Snapshot

6.1.2 Remote Registration

In the beginning the device requests for the registration by sending its MAC id, group name to which it wants to join. This information is sent to seed box or admin for the approval.

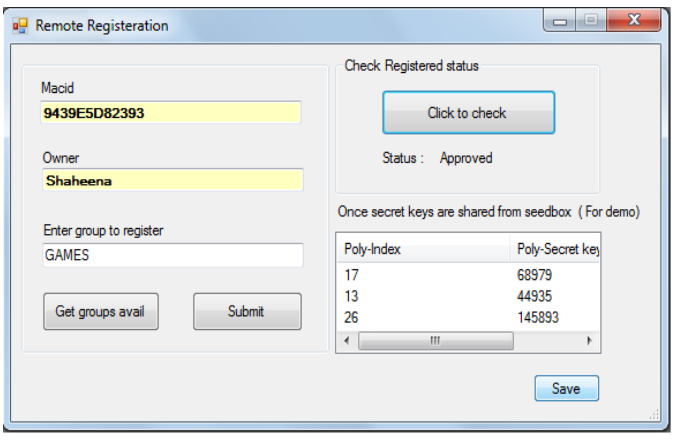

Fig 6.1.2a Node Remote Registration Snapshot

6.1.3 View Request

The admin can view the pending request and can either approve, reject, delete the request.

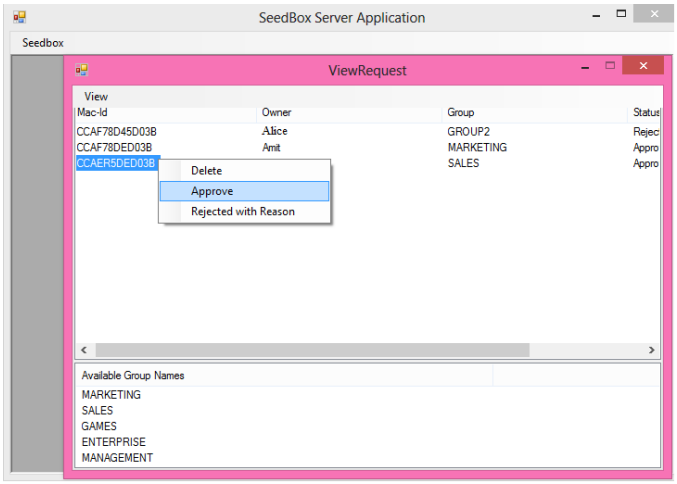

Fig 6.1.3a View Request Snapshot

6.1.4 Join Group

Join Group screen displays list of IP address and corresponding group name. The Group Joining process is done between the two nodes which are in same group and without the interaction of SEEDBOX or ADMIN. Clicking on the IP address of the device allows the further communication with it.

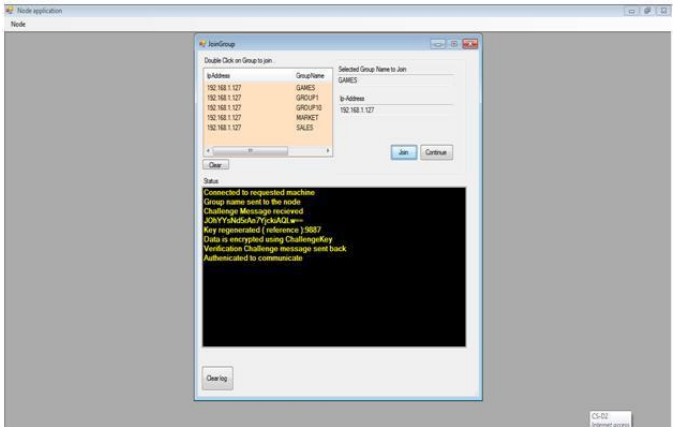

Fig 6.1.4a Join Group Snapshot

Section 7

CONCLUSION

The authentication mechanism provided eases out the work of the people who spend a lot of time in monitoring their devices. The proposed mechanism thwarts security attacks, such as Man in the Middle (MitM) and replay attacks. The proposed mechanism is not only an ad hoc networks secure solution, and can be set on any kind of computer networks, offering a light and distributed security solution

BIBLIOGRAPHY

1.Borisov, N. Goldberg, I. and Wagner, D. (2001), Intercepting Mobile Communications: the insecurity of 802.11. In: International Conference on Mobile Computing and Networking - MobiCom'01. Proceedings. Roma, Italia.

2. Bosselaers, A., Govaerts, R. and Vandewalle, J. (1996), Fast Hash on the Pentium. In: Advances in Cryptology - CRYPTO'96, Lecture Notes inComputer Science, Springer-Verlag, and Proceedings. Santa Barbara, CA, USA.

3. Capkun, S., Hubaux, J.P. and Buttyan, L. (2003), Mobility Helps Security in Ad Hoc Networks - MOBIHOC'03,4. Proceedings. Annapolis, MD, USA.

4. Feeney, L. and Nilsson, M. (2001), Investigating the Energy Consumption of a Wireless Network Interface in an Ad Hoc Networking Environment. In: IEEE Infocom'01, 20. Proceedings. Anchorage, AL, USA.

5. Harkins, D. and Carrel, D. (1998), RFC 2409. The Internet Key Exchange (IKE). IETF Network Working Group Request for Comments.

6. Krawczyk, H., Bellare, M. and Canetti, R. (1997), RFC 2104. HMAC: Keyed-Hashing for Message Authentication. IETF Network Working Group Request for Comments.

7. RSA Security Inc. (2001), RSA SecurID Authentication: a better value for a better ROI. RSA Whitepaper. Available at: <http://www.rsasecurity. com/ products/securid/>.

8. Schmidt, B. Schimmler, M. and Adi, W. (2002), Area Efficient Modular Arithmetic for Mobile Security. In: International Conference on Wireless Networks - ICWN'02. Las Vegas: CSREA Press. Proceedings. Las Vegas,NV, USA. p.208-214.

9. Stajano, F. and Anderson, R. (1999), The resurrecting duckling: security issues for ad hoc wireless networks. In:AT&T Software Symposium, 3., Middletown. Proceedings. NJ, USA.

10. Applications and the Internet Workshops, 2007. SAINT Workshops 2007. International Symposium [15-19 Jan. 2007]

11. Advanced Video and Signal-Based Surveillance (AVSS), 2012 IEEE Ninth International Conference.