ISSN : 2350-0743

www.ijramr.com

International Journal of Recent Advances in Multidisciplinary Research

Vol. 02, Issue 12, pp.1071-1074, December, 2015

RESEARCH ARTICLE

ANALYSIS OF BLUETOOTH THREATS AND V4.0 SECURITY FEATURES (LEARNING ASSOCIATION RULE)

***Aditi Vats, Kritika Singh, Dharmveer Singh Rajpoot**

Department of Computer Science Engineering, Jaypee Institute of Information Technology, Noida, India

ARTICLE INFO

Article History:

Received 11th, September 2015
Received in revised form
23rd, October 2015
Accepted 21st, November 2015
Published online 30th, December 2015

Keywords:

Association rule, Feature,
Security, Bluetooth,
Cryptography etc.

ABSTRACT

In today's world the technology which is made wireless communication easier is Bluetooth technology which is used for transferring data in short range. People who are looking to gain information in an unauthorized manner is viewed very closely to any new improvement or invention. Security of data is very important aspect in Bluetooth .Bluetooth security has many other different versions of Bluetooth regarding security and speed of transferring the data which is to be according to the need and demand .Mainly this paper covers man in the middle attack security issues .There will be eavesdropping and MITM attacks when we establish encryption key between two Bluetooth devices. A schema has been designed which is called secure key agreement and is based on elliptic curves cryptography and interlock protocol. It provides an authentication which is bidirectional for two devices and it also provide key integrity verification by exchanging the keys Hash-values which is generated by both the ends. Thus the security is analyzed properly. The results of the method proposed is secure and efficient.

INTRODUCTION

Association rule learning is a very famous and well known technique for inventing interesting relations among variables in large databases. It is mainly used to define basic rules discovered in databases by using different counts of variables. On the basis of this concept of basic rules, Rakesh Aggarwal *et al.* has introduced association rules for inventing similarities among the products in large-scale of data transaction stored by point-of-sale (POS) systems in supermarkets. As an example, the rule \{\mathrm{butter, bread}\} \Right arrow \{\mathrm{milk}\}that has been found in the sales data of a market will indicate that if a customer buys bread and butter together, they will definitely bring milk. For taking decisions about marketing strategies such as, e.g., advertising the pricing or placements of product these type of these information can be used. Based on the given example from market basket analysis, association rules learning are used today in various application areas which includes intrusion detection, Continuous production, and bioinformatics. By Using application of Bluetooth in a vast way, the security problems of bluetooth gather more and more people's mind. The main reason behind its insecurity is that its encryption key agreement process is unsafe. The encryption key is evaluated from numbers which are random and are exchanged between two or more than two Bluetooth devices. As we know the Bluetooth network is open to all, the random numbers generated are very easily eavesdropped and changed. Hence the communication process in Bluetooth in this case will suffer from MITM attack. Thus changing the present encryption key agreement methodology in Bluetooth is a adverse way of modifying the bluetooth security. There are two ways to establish the encryption key between two or more Bluetooth devices. One of the way is D-H key agreement protocol and the other way is with the use of CA. The encryption key agreement protocol in Ad hoc has been amended from the D-H key agreement protocol to key agreement protocol which is based on elliptic curve cryptography (ECC). It is very important to build a type of key agreement protocol in Bluetooth and is against MITM attacks. Thus based on the particular criteria we need a new set of encryption key agreement protocol and data encryption to provide network security in Bluetooth communication.

The encryption key that we need to negotiate in this process is by two communicating devices and with block cryptographic algorithm we implement data encryption. The process of encryption key needs protection against encryption. And the cryptographic algorithm needs to meet with the memory space and computing capability of the Bluetooth devices. The agreement process needs to ignore the participation of user as much as it can. with the help of its short keys,strong security,short parameters and high efficiency ECC can fulfil the demands. And hence it can be used in Bluetooth. The paper presented here designs an encryption key agreement scheme which is secure and in the host Bluetooth devices which is based on interlock protocol and ECC.

Literature survey

Security of Mobile Phones: Prevention Methods for The Spread of Malware: Most of the time malware replicate itself while their is communication take place in between wireless network

****Corresponding author: Aditi Vats,***
Department of Computer Science Engineering, Jaypee Institute of Information Technology, Noida, India.

i.e. bluetooth and it can easily spread itself because authentication check is not as much. Basically in this paper the method which is used is firstly the state of mobile security should be checked and the level of security also , then according to it in academics which is defined is studied and after this go through the solution against the software described in industries regarding bluetooth . Two methods are used one is Word Verification in this method algorithm generates the CAPTCHA.CAPTCHA is the image text to be entered by human being so that software can identify that whether it is written by human being or it can be a machine or robot . There is one more may to identify that is Blue-Watchdog to observe bluetooth by time series analysis .Data collected from the shipments of Desktop PCs and smart phones and tablets. Advantages of this are CAPTCHA have the option of audio CAPTCHAs for the visually impaired people and Spammers are blocked by CAPTCHA. Disadvantage is CAPTCHAs only limit spam and are unable to prevent spam completely. Many software's are available which can easily decode the captcha.

Contention for Man-In-The-Middle Attacks in Bluetooth Networks: For the short range of transferring the data now a day the technology which is mostly used is bluetooth. For low power consumption bluetooth is suggested basically and the rate of transferring the data within a short range over bluetooth is cheap, fast and at moderate rate. When two or more wireless network are connected with each other adhoc network are formed which is allowed by the bluetooth and this wireless network is known as piconets. The amount of security of bluetooth can be detected by the condition checked it is connected with other devices and also the way it is disable form the devices. In this paper method which is used is SSP using Elliptic Curve Diffie Hellman (ECDH) public key cryptography. To prevent MITM attack a method is proposed which is simple secure pairing which allow two user to connect with each other and a numeric key is generated for comparison. A same physical channel is used within the connected devices so that the communication take place with the same global clock and a hopping sequence is also used for the communication. The main goal of secure simple pairing is to make easy approach for the user to pair with the other device. The other goal of this approach is make efficient and better security in bluetooth device.

SSP is only strongly used for passive eavesdropping and the protection is against this only. MITM attack and passive eavesdropping is not totally restricted or protected by the SSP that use ECHD method. SSP method is less efficient against the attacker to protect the data. So it is very important to find the correct association method to protect the data from MITM attack. Bluetooth Technology: ApXLg level End –to-End Security: The devices that have evolved over a very long period of time with the help of constant and uninviting work or research of the designers, researchers, implementers are the mobile phones, specifically the smart phones that have evolved in the mobile handset industry across the globe. There is a different kind of technology called as Bluetooth that has made the sharing of different types of meaningful information like audio, streaming music, messages and file transfer in a personal area network (PAN) and also has made the communication between users easy. The proposed paper defines an Intrusion prevention system (IPS) and an Intrusion Detection system (IDS)that will be based on different set of rules. In this proposed scheme the reference that we have taken is Android OS and it is needed while using the services of various cryptographic service providers (CSP). Together the IDS and IPS will be creating various possible attacks that has been defined or outlined on the basis of the behavioural pattern of the attacker. Though the proposed approach is very efficient but it is not able to prevent the user from any kind of data leakage which can happen beyond the scope of the set of rules that has already been defined.

Location Privacy Vulnerable from Bluetooth Devices: A new method is proposed to find the location privacy which is secured to transfer the data. The devices which are available their Mac addresses is scanned .As per the scanning of Mac address the risk of location privacy of data is determined and this is compensate with the scanning of bluetooth device . To discover the mac address of bluetooth device hcitool scan is used. The behaviour and the activities of users are recorded and even also the users which are passed from the area which is recorded i.e. how frequently the users come into the range and at what time they leave. Due to the careless configuration of bluetooth the location privacy of it is unprotected. Wireless Security & Privacy: As the technology which is known to as bluetooth is almost aware to everyone and it is used by every single person so its security issues are increasing day by day. While transferring data over the wireless network or while reading, retrieving the information or correcting the data it should be remembered to keep away the intruders and important security measures should be taken.

Option for enabling and disabling the technology is available over the wireless network for the security purpose. Within a secure environment wireless technology allow to communicate and transaction can also take place easily without disabling the facilities which allow us to use the information. Algorithm which is used known as WEP (wired equivalent privacy). This algorithm is depend upon RCY secret key cryptographic algorithm. The main problem which is eavesdropping in wireless network to protect it the algorithm which is used is WEP in this paper. This can also protect the wireless network from unauthorised usage. For this problem integrity check value algorithm is not efficient and data can be replicate easily. There is no authentication or integration protection check between the access point and the end user when the frames transferred over the wireless network.

As there is no authentication message so frames can easily forged in between without any identification or awareness. Transmission of an ECG Data with the Patch-Type an ECG Sensor System using Bluetooth Low Energy: The advancement in the field of wireless network has been widened all over the world as new less power consuming applications in different sectors whether in houses, sensors ,health and fitness center,cars automotive systems ,medical sectors etc. New wireless devices are created which senses the patient's health as a electronic wave connected by wireless network i.e. bluetooth which can be further classified as: Classic Bluetooth and Bluetooth Low Energy (BLE). BLE is a developing technology which consumes less power and efficient for medical purposes and helps to interact with others.BLE technology based devices uses a part of classic bluetooth power that enables the products for better communication. Many Products works on small batteries for almost a year, and that too without changing or charging. BLE is used in different devices such as Smart devices, medical centres and ECG sensors which transmit data into streams avoiding any loss of data with BLE. Packets are transferred by following a set sequence after fixed interval for connecting but it is inefficient in transferring large quantity of data.

Proposed Method

This technology discussed will allow the formation of ad-hoc networks that is called piconets and is formed between two or more than two devices that may be wireless. The devices which are connected will share the information with the help of a common clock and hopping sequence and that too on the same physical channel.

The secure key agreement scheme in Bluetooth executes in the following manner. It executes as-

- The two inputs C and D will select the similar elliptic curve parameters that will be generating the similar curve p (EF) .
- D will input a randomly selected number *read* that will be generating a random number *k* in 1, n-1 as a decryption key. And C will perform this similar action as D. Then both will be computing the encryption key Q (dp) respectively.
- C will be generating the part of the encryption key C k and then it will be calculating the hash values C (HK). After that C will encrypt C (HK) and will send the cipher text to D.
- D will decrypt the C (EHK) and then it gets C' (HK).After that D will generate another part of the encryption key DK and it will compute D(HK) .After this it will transmit QD(EHK) to C.
- C will decrypt QD (EHK) to get D'(HK).After this C encrypts CK and then it will send it to D.
- D will be decrypting QCEK and will be obtaining CK'. After this D will compute C'(HK) and then it will verify whether C'(HK) will be equal to C(')HK. If both of them are not equal to one another, D is going to drop the link. And on the other side the communication will carry on. D will encrypt DK and it will send it to C. After that D will compute C'DCD (K)K . Then D will have the final encryption key.
- C will be decrypting QD (EK) and obtaining D'K . Later on D will compute D (')HK and then it will verify that whether D(')HK is equal to '()DHK..And if they are not equal C will drop the present connection. Else C will compute 'CDCDK. Then the final encryption key will be fully established and is successful.

After performing step (5) D is in waiting state. And if D does not receive any message from C after T, then D believes that their connection is suffering from MITM attack and it is going to break the link.

Experimental Results

Description of quality measures

- The response device which is used has very high level of security. Both the devices will get the final encryption key when the communicating devices execute the protocol very honestly and they are identical.
- The parties that are communicating can only get the final encryption key.
- Authentication may happen between two parties.
- In this proposed scheme the final encryption key is independent and Q (Encryption key of ECC) is also independent.
- In this proposed scheme, validation of the integrity of final encryption key may happen.
- In this proposed scheme, it can defend intercepting attack.
- In this proposed scheme, it can defend MITM attacks.
- This scheme has both backward and forward security.

RESULTS

The proposed scheme can provide integrity authentication for the keys. After the authentication process has been performed the key agreement protocol need to be optimized. The protocol that has been optimized not only will guarantee the security but will also reduce the costs of communication and computation and it can be done by means of reducing the times of encryption and decryption operation and the involved information at alternating times.

Conclusion

The paper presented here is designing an encryption key agreement scheme which is based on the interlock protocol and on ECC. The scheme is designed in such a way that it can defend MITM attacks very effectively in the negotiating process of encryption key in Bluetooth. The proposed scheme can also provide integrity authentication for the keys. After that the key agreement protocol is optimized. The optimized protocol can not only guarantee the security but also reduce costs of computation and communication by means of reducing times of encryption and decryption operation and information alternating times. The security of the protocol which has been analysed theoretically will demonstrate that the defined protocol will definitely guarantee the encryption key agreement process security in Bluetooth. The proposed scheme will be compared to the related schemes already present and hence the result shows that the proposed scheme is very efficient.

REFERENCES

Bheemeswara Rao, K. V., Ravi, N., Phani Bhushan, R., Pramod Kumar, K., and Venkataraman, S. (2014, April). Bluetooth technology: ApXLglevel end-to-end security. In *Communications and Signal Processing (ICCSP), 2014 International Conference on* (pp. 340-344). IEEE.

Borsc, M., and Shinde, H. (2005, January). Wireless security & privacy. In*Personal Wireless Communications, 2005. ICPWC 2005. 2005 IEEE International Conference on* (pp. 424-428). IEEE.

Ghallali, M., and Ouahidi, B. E. (2012, March). Security of mobile phones: Prevention methods for the spread of malware. In *Sciences of Electronics, Technologies of Information and Telecommunications (SETIT), 2012 6th International Conference on* (pp. 648-651). IEEE..

Sandhya, S., and Devi, K. S. (2012, November). Contention for Man-in-the-Middle Attacks in Bluetooth Networks. In *Computational Intelligence and Communication*

Networks (CICN), 2012 Fourth International Conference on (pp. 700-703). IEEE..

Kikuchi, H., and Yokomizo, T. (2013, September). Location Privacy Vulnerable from Bluetooth Devices. In *2013 16th International Conference on Network-Based Information Systems* (pp. 534-538). IEEE.

Park, Y. J., and Cho, H. S. (2013, October). Transmission of ECG data with the patch-type ECG sensor system using Bluetooth Low Energy. In *ICT Convergence (ICTC), 2013 International Conference on* (pp. 289-294). IEEE.

****