A Survey over the Security Issues of Bluetooth using Elliptic Curve Cryptography

Ahmed Hweishel A. Alfarjat
Applied Science Department,
AlBalqa Applied University,
Jordan,Aqaba.

Hanumanthappa J., PhD
DoS in Computer Science,
University of Mysuru,Manasagangothri
Mysuru-570006.

ABSTRACT

In this research paper,the authors are addressing the problem of algorithms for Wireless LAN for Secured Transmission. This research work also proposes an overview of some of the major attacks that Blue tooth has faced over the years along with some possible solutions. The main aim of this research work is to investigate security features of Bluetooth using Elliptic Curve Cryptography(ECC). The ECC is the latest and fastest encryption method which offers stronger security. As it is known that although a vast majority of devices currently now communicates using Bluetooth methodology, the blue tooth security expert provides automatic updates to its security protocol and user privacy protection techniques. Further protection of the device user's personal information becomes the primary aim. The research work also explores the Bucket Brigade Attack on Bluetooth security using Elliptic Curve Cryptography (ECC). Also it is implied that Bucket Brigade Attack(BBA) is one of the amazing solution to the problem of key agreement or key swapping. Further the beauty of this scheme is when two parties who likes to communicate using symmetric key and an Elliptic Curve Cryptography(ECC) an Intruder(Hacker) enters in between a sender and a receiver. This paper is an attempt to implement the ECC after a survey over the current issues on security.

Keywords

Bluetooth,Cryptography,ECC.

1. INTRODUCTION

Blue tooth is a methodology for short range Wireless data and real time two way voice transfer cooperating data rates up to 3 Mb/s[1][9]. It is also used to connect almost any instrument to any other device. In now a day's Bluetooth enabled equipments such as Mobile phone's,Head sets,PC's,Laptops and printer's,Mice and Keyboards are mainly used all over the world. In the year 2006 one billion Bluetooth equipments are shipped and this number rapidly increases in the near future[1]. The target volume for 2016 is as high as 3 billion Bluetooth devices. Therefore it is highly essential to shown keen interest on Bluetooth security issues. Bluetooth is a technology defined by Bluetooth Special Interest Group(BSIG)[1][9]. Initially Bluetooth was considered as a simple serial cable replacement for electronic devices. Currently as we know that Bluetooth technology supports more advanced functionalities like Ad hoc networking and AP operation for Internet connections. The ongoing developments in Bluetooth technology extends new features such as support for QoS,higher data rates,multicasting and low power consumption. When the application area trying to expand as new products with Bluetooth capability are constantly introduced [9]. With respect to the best our knowledge the Bluetooth technology is made up of different protocol layers ranges from physical radio and baseband to object exchange and service discovery. In addition the BSIG also specifies number of profiles which specify the criteria of messages, procedures and protocols required for supporting a specific service. It is already clear that the Bluetooth instrument is one which supports for either Point-to-Point Communication or Point to Multipoint Communication. Piconet is a network which consists of Bluetooth devices [1][9].

1.1 Bluetooth Security Architecture(BSA)

Security in Bluetooth can be considered as a mechanism of defense against willful acts of smart adversaries' people. The word security either implicitly or explicitly protection to some extent. The word protection is defined as the defense against random events such as accidents and failures. This research work also took an opportunity to swap safety and protection in this thesis work. The security design mainly involves defining a sequence of procedures for the cooperation of algorithms,protocols and their usage. As discussed above one more important aspect of security development specifically in Bluetooth is to design an efficient implementation of opted procedures consisting of their basic elements and interaction. There are so many similarities between WLAN and WPAN therefore they can merge into an individual technology known as WLANs.

This section clearly explores how security issues have been considered in present public Bluetooth specifications such as blu01,blu03,blu04a,blu07a,1blu99a,blu99b etc.The fundamental Bluetooth specifications are genuinely implemented by the user who resolves how a Bluetooth instrument it's connect ability and discoverability preferences.The various categories of connect ability and discoverability strengths can be chunked into three different parts such as

i. *Silent Preference*:In Silent preference the instrument will never accepts any connections. The Bluetooth simply oversees the traffic.

ii. *Private Preference*:In this phase the instrument cannot determines non-determinable instrument. Connections are only accepted when the Bluetooth Instrument Address (BI_ADDR) of the device is known to the perspective Master. To the best of our knowledge BI_ADDR is a 48 bit address which globally and uniquely specifies a Bluetooth instrument.

iii. *Public Preference*:In a Public preference the instruments can be ascertained and connected to therefore it also called an ascertained apparatus.

The Bluetooth equipment at a time broadly implements the following four different categories of security preferences such as Non-Secure, Service-level enforced security preference,Link level enforced security preference,and service level enforced security preference. We have also taken an opportunity to explore all the four different preferences as follows.

i. *Non-Secure Phase*:As we know in this type of phase Bluetooth does not initiate any security measures.

ii. *Service level enforced security Phase*:In this phase two different instruments can authenticate a non secure ACL(Asynchronous Connection less) link. The various security principles such as Integrity,Non repudiation,Authentication, Authorization,Encryption and Decryption are initiated when an L2CAP CO(Logical Link Control and Adaptation Protocol Connected Oriented) or an L2CAP CL channel request is made.

iii. *Link level enforced security mode*: Security procedures are really initiated when an ACL link was constructed.

Service level enforced security Phase: This phase is exactly similar to Phase-2 except that only Bluetooth devices utilizing SSP can use it. i.e only Bluetooth 2.1+EDR instruments can use this security phase.

2. LITERATURE SURVEY

The review of literature pertaining to the subject is undertaken to understand the better prevailing aspects in the field of Security issues of Bluetooth using Elliptic Curve Cryptography. This effort has been made to search available literature from text books,refereed international journals, reputed international/national conference papers, symposium papers,book chapters,internet data etc relevant to the study. The details of some of the reviews that have been made for the research work are summarized below.

For the last twenty five years,many researcher's,scientists have been actively engaged in proposing and developing a new flexible security issues of Bluetooth using Elliptic Curve Cryptography. It has made a notable contribution to the research group to do further research on the security issues of Bluetooth algorithms using Elliptic Curve Cryptography(ECC).

Rivest R.Shamir.A. and Adleman.L[7]. have discovered the principles of RSA algorithm and also they have developed a method for obtaining Digital Signatures and Public Key Cryptosystems. Already in antiquity encryption was used in warfare and diplomacy. The ancient encryption techniques are insufficient in now a days but some of their ideas are utilized in the new encryption methodology. Public Key encryption techniques use a Public key for encryption and a private key for decryption. Typically Public Key Cryptography is used.

Diffie and Hellman in the year 1976 when introduced the concept of Public Key Cryptography the cryptographic importance of the apparent intractability of the discrete logarithm has been determined[1].

El Gamal first described how this problem may be utilized in Public Key Encryption and digital signature schemes. ELGamal techniques have been refined and incorporated into various protocols to meet a variety of applications and one of its extension create the basis for the U.S government Digital Signature Algorithm(DSA).The Discrete logarithm problem first employed by Diffie Hellman in their Key agreement Protocol was defined explicitly as the problem of finding logarithms with respect to a generator in the multiplicative group of the integers modulo a prime,this technique also can be extended to arbitrary groups[7].

The group of points on an elliptic curve specified over a finite field the jacobian of an elliptic curve defined over a finite field and the class group of an imaginary quadratic number field. Elliptic curves have been extensively studied for over a hundred years and there is a vast literature on the topic.

In the Year 1995 Miller and Koblitz [22][23] separately proposed using the group of points on an elliptic curve defined over a finite field in discrete log cryptosystems. The primary advantage that elliptic curve cryptosystems have over system based on multiplicative group of a finite field is the absence of a sub exponential time logarithm that could determine discrete logs in these groups. While consequently we can use an elliptic curve group which is smaller in size while maintaining same level of security.

Koyama et all have proposed elliptic curve analogues of the RSA cryptosystem[20]. In these systems works in an elliptic curve defined over the ring Zn where n is a composite integer and the order of the elliptic curve group serves as the trapdoor. The security of these methods is based on the difficulty of factoring n[20].

Kurosawa,Okada et all subsequently showed that these elliptic curve analogues do not have any significant advantages over their RSA counterparts [19]. Charlap and Robbins showed elementary self-contained proofs for some of the basic theory.

Hermelin.M.,Nyberg.K.(1999) theoretically proved that Bluetooth stream cipher with 128 bit key can be wrecked in O(264) steps.

Canniere et al(2001) had proved that E0 stream cipher of Bluetooth has some security imperfections.

Jakobsson.M. and Wetzel.S.(2001)[17] for the first time formulated MITM attack on Bluetooth for version 1.0B. By passive eavesdropping on the initialization Key establishment protocol they also developed a technique to acquire the link key using an off-line PIN crunching attack. They pointed few limitations of version 1.0B like usage of the unit key the short Bluetooth PIN and the confidentiality problem caused by site tracking [17].

3. PROPOSED METHODOLOGY

This research work involves in the Implementation of Bucket Brigade Attack(BBA) using Elliptic Curve Cryptography [17]. The Public Key Cryptography has devised by Diffie and Hellman in the year 1976 and created a great milestone in the history of Public Key Cryptography. RSA was developed by Rivest,Shamir and Adleman in the year 1977 and was published in 1978[17]. The Diffie Hellman Key was based on the use of Discrete logarithm. Elliptic Curve Cryptography (ECC) is based on Mathematical Properties of elliptic curves and it shows to offer equal security to RSA for a much smaller key size. The Bluetooth version 2.1+EDR improves the security of pairing by using Elliptic Curve Diffie Hellman(ECDH) Public Key Cryptography [17]. ECDH is a key agreement protocol for allowing two communicating parties to establish a common secret key over an unsecured path. It becomes a variant of Diffie Hellman Key quid pro quo protocol using ECC [17]. An elliptic curve over real numbers R is a set of points(x,y) which satisfies an equation y2=x3+ax+b in which (x,y,a,b) ε R. The elliptic curve is one which maintains an element O,which is called the point at infinity. The various computations over real number are slow and an inaccurate because due to the presence of round error. Therefore elliptic curves with x,y,a,b ε R are not usable in practical. Instead of elliptic groups modulo p(where p is a prime) are defined in the following way. Two non negative integers a,b<p which satisfies 4a3+27b2 ≠ 0 mod p are chosen [17]. Ep(a,b) specifies the elliptic group modulo p where elements(x,y) are pairs of non negative integers less than p satisfying both y2 ≡x3+ax+b mod p and the point at infinity O[17]. It is worth noting that the number of points on the elliptic curve is not infinite. Even it is not clear how to connect these discrete points on the elliptic curve is not infinite. Moreover it is clear even how to connect these discrete points to make their graph look like a curve. The geometrical definition of operations on these points cannot be used. The algebraic integrity constraints are mainly used to make calculation precisely on elliptic curve groups modulo. The Elliptic Cryptography system can be defined in the following ways. The domain values are as follows:

i. A Prime number p and parameters a and b specifying an elliptic group of points $E_p(a,b)$.

ii. A generator point G on $E_P(a,b)$:One of an important criterion for choosing G is that the smallest value of n(n is said to be the order of point G) for which nG=0 be a large number[17].

The private key is an integer k,where 2<=k<=n-2. The public key is the point Q=Kg. A key swapping between obama and hanums can be performed easily with ECC as an analogue to the Diffie Hellman Key swapping. The Diffie Hellman works similar to the following way as follows[17].

i. Obama keys are (K_A,Q_A) and hanums Key are (K_B,Q_B). Obama computes the secret key $K=K_AQ_A$ and hanums computes the secret key $K=K_BQ_{A.}$ Both computations to create the same result because $K=K_AQ_B =K_Ax(K_BG)=K_BXK_AG=K_BQ_A=K$. Therefore Obama and hanums can use the symmetric key encryption of messages with 3DES, Blowfish or AES[17].

ii. The encryption and Decryption procedure are as follows. The Plain text message m is specified as a point P_m on $E_P(a,b)$.The various straight forward methods of transforming the message m into coordinates on the elliptic curves exist. When Obama likes to encrypt and send P_m to hanums he picks a positive an integer k and creates the cipher text $C_m=\{kG,P_m+kK_B\}$. Hanums can try to calculate and decrypt the cipher text by computing P_m+kQ_B $-k_BX(kG)=p_m+kx(k_BG)-k_G=P_{m.}$ Finally the hanums decodes the plain text message m from the point P_m[17].

4. MEASURING PERFORMANCE OF ALGORITHMS

There are two aspects of algorithmic performance namely time complexity and code complexity. Time complexity deals with time taken by instructions. How fast does the algorithm perform and What affects its runtime? Algorithms can not be compared by running them on computers. Run time is system dependent. Even on same computer would depend on language,Real time units like microseconds not to be used. Generally concerned with how the amount of work varies with the data. To measure time complexity it is normally performed on Counting number of operations involved in the algorithms to handle n items. Meaningful comparison is done by running algorithms for very large values of n. There are several other terms used in estimating the complexity.

They are as follows:

Worst Case complexity:The worst case guarantees that the performance of the algorithm will be at least as good as the analysis indicates.

Average Case Complexity:It is the best statistical estimate of actual performance,and tells us how well an algorithm performs if you average the behavior over all possible sets of input data.However,it requires considerable mathematical sophistication to do the average case analysis.

ROC(Receiver operating characteristics),

TPR:True positive rate

TNR:True negative rate and also sensitivity, selectivity etc...

Area under the ROC graph would give the performance analysis of any system or the algorithms practically.

Here the authors have discussed in nutshell the various aspects of development of algorithms related to ECC and are planning to estimate the performance analysis of ECC in particular in their future work. This paper is a bird's eye view about the activities involved in development of any algorithms and is a guideline for a beginner in the research field about algorithm development[20].

5. CONCLUSIONS

In this research paper the authors have proposed a survey based security issues of Bluetooth using Elliptic Curve Cryptography. As it is known that security issues of Blue tooth is a highly good and an innovative topic to further enhance a quality research,the authors are planning to practically implement this work either by using the network simulators such as NS2 or NS3 in our next research paper.

Bluetooth security issues are investigated and the feasibility of some of them is like to demonstrate in our network research laboratory. Overall security in Bluetooth network is based on security of the Bluetooth medium, the various security issues of Bluetooth protocols and Bluetooth security parameters used in Bluetooth communication.

There are several weaknesses in the Bluetooth medium, Bluetooth protocols and Bluetooth security parameters which tries to weak the performance of a Bluetooth network. Even then an attempt is being made to overcome the security problems both theoretically and therapeutically. As this is a stepping in paper about the concept, the authors acknowledge the support rendered by their friends and colleagues to take-up further work under ECC.

6. REFERENCES

[1] W.Diffie and M.Hellman,New directions in Cryptography,IEEE Transactions on information Theory,Vol.22(1976),pp.644-654.

[2] Bluetooth SIG:Bluetooth Wireless Technology Surpasses One billion devices.

[3] Tan A:Bluetooth gets high speed boost.CNET Networks,ZDNet Asia,newscopy march 9,2006.

[4] Suomalainen.J.,Valkonen.J.et all:Security Associations in Personal Networks–A Comparative Analysis .Proceedings of the fourth European workshop on Security and Privacy in Ad-hoc and Sensor Networks(ESAS-2007),LNCS,Vol.4572,springer-verlog,pp.43-57.

[5] William Stallings:Cryptography and Network Security Principles and Practice.3rd Edition,Upper saddle river, New jersey,PH,2003.

[6] Spill .D. and Bittau.A.:Bluetooth–Eve meets Alice and Bluetooth,Proceedings of the first Usenix workshop on offensive technologies(WOOT-2007),Boston,MA,2007.

[7] Rivest .R.,Shamir.A. and Adleman.L.:A Method for obtaining Digital Signatures and Public Key Cryprosystems,Communications of the ACM,Vol.21,No.2,Feb,1978,pp-120-126.

[8] Borisov.N.,Goldberg.I.,and Wagner.D.,Intercepting mobile communications the insecurity on 802.11 Proceedings of the 7th Annual International Conference on mobile computing and Networking,ACM Press,2001.

[9] Bluetooth SIG:Bluetooth Wireless Technology Surpasses one Billion Devices,Bluetooth SIG,press release,Nov.13,2006.

[10] D.Kugler,Man in the Middle attacks on Bluetooth,in Proc 7th International Conference Financial Cryptography(FC'03),Gosier,Goudeloupe,French West Indies,Jan.27-30,2003,pp.149-161.

[11] M.S.Hwang,C.C.Lee,J.Z.Lee et al,A Secure Protocol for Bluetooth piconet's using Elliptic Curve Cryptography,Telecommunication systems,vol.29,no.3,pp-165-180,2005.

[12] C.T.Hager and S.F.Midkiff,An Analysis of Bluetooth Security vulnerabilities in Proc Wireless IEEE Communication and Networking Conference(WCNC-2003),New Orleans,LA,USA,Mar-16-20,pp-1825-1831.

[13] D.Bae,J.Kim,S.Park and O.Song,Design and Implementation of IEEE 802.11i architecture for next generation WLAN in Proc 1st SKLOIS Conf Information Security and Cryptology(CISC-2005),Beijing China,Dec 15-17,Springer verlog,pp.346-357.

[14] W.C.Barker,Recommendation for the triple data encryption algorithm block cipher,National Institute of standards and Technology(NIST),Gaithersburg,MD,USA.

[15] S.Das,F.Anjum,Y.ohba et al,Security issues in Wireless IP networks in Mobile internet:Enabling Technologies and Services.

[16] E.B.Fernandez,S.Rajput,M.Vanhilst,Some Security issues of Wireless systems,Jan 24-28,2005.

[17] M.Jakobsson,S.Wetzel,Security weaknesses in Bluetooth.LNCS,Vol.2020,pp.16-191,springer-verlag,2001.

[18] Hypponen.K.,Haataja.K.,"Nino" Man in the Middle Attack on Bluetooth Secure Simple pairing,proceedings of the IEEE Third International Conference in Central Asia on Internet,The next Generation of Mobile,Wireless networks and Optical communications Networks(ICI-2007),Tashkent,Uzbekistan,Sept 26-28,2007.

[19] K.Kurosawa,K.Okada and S.Tsujii,"Low exponent attack against elliptic curve RSA,Advances in Cryptology"-ASIACRYPT-94,Lecture notes in Computer Science,Springer-Verlag,917(1995),pp.376-383.

[20] Koyama.K.,Maurer.U.,Okam oto.T.,S.Vanstone,New Public Key Scheme based on elliptic curves over the ring Zn,Advances in Cryptology-CRYPTO-91,Lecture notes in Computer Science,Springer-Verlag,576(1993)pp.252-

[21] Ahmed Hweishel A.Alfarjat,Hanumanthappa.J.,"A Survey over the Security issues of Bluetooth using Elliptic Curve Cryptography",International Journal of Computer Applications.

[22] V.Miller,"Uses of Elliptic Curves in Cryptography,Advances in Cryptology-CRYPTO-85,Lecture notes in Computer Science,Springer-Verlag,218(1986),pp.417-426.

[23] Koblitz.N.,Elliptic Curve Cryptosystems,Mathematics of Computation,48(177):203-209,1987.