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

International Journal of Computer Applications
Foundation of Computer Science (FCS), NY, USA

Volume 150
Number 8

Year of Publication: 2016

Authors:
Ahmed Hweishel A. Alfarjat, Hanumanthappa J.

10.5120/ijca2016911591

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.

References

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.
14. W.C. Barker, Recommendation for the triple data encryption algorithm block cipher, National Institute of standards and Technology (NIST), Gaithersburg, MD, USA.
20. Koyama, K., Maurer, U., Okamoto, T., S. Vanstone, New Public Key Scheme based on elliptic curves over the ring \( \mathbb{Z}_n \), Advances in Cryptology-CRYPTO-91, Lecture notes in Computer Science, Springer-Verlag, 576(1993) pp.252-

**Index Terms**

Computer Science Security

**Keywords**

Bluetooth, Cryptography, ECC.