Abstract

Bluetooth is a technology for connecting devices wirelessly to achieve data transfer at the rate of 720 kbps within a range of 10 to 100 meters. In existing authentication procedure for Bluetooth networks, four levels of key generation viz initialization key, combination key, link key, encryption key were incorporated. Bluetooth devices have limited resources, so we need a small authentication procedure. We proposed a new authentication scheme for Bluetooth networks. We presented enhancement in the authentication procedure of Bluetooth by using Diffie-Hellman Algorithm. This novel authentication procedure acts as the countermeasure against SNARF attack by the introduction of Diffie Hellman algorithm.

References

- KEIJO HAATAJA "Security Threats and Countermeasures in Bluetooth-Enabled Systems" Department of Computer Science University of Kuopio 2009
- Bin Zhen, Jonghun Park and Yongsuk Kim "Scatternet Formation of Bluetooth Ad Hoc Networks" i-Networking Lab, Samsung Advanced Institute of Technology, YongIn city, 440-600, Korea 2003
Enhancing Bluetooth Authentication using Diffie Hellman Algorithm

- John D. Padgette "Bluetooth security in the DOD" Booz Allen Hamilton Herndon, VA, April 19, 2009
- Pushpa R Suri Sona Rani "Symmetric Key Insecurity in Bluetooth Communication" Department of Computer Science and Applications, Kurukshetra University, kurukshetra, Haryana, INDIA.
- Mostafa Akhavan-E-saffar, Vahid Tabataba Vakily "Improvement Bluetooth Authentication and pairing protocol using Encrypted Key Exchange and Station-to-Station MAC Protocols" 2009 international conference on machine learning and computing
- Deepak Jayanna, Gergely V. Záruba "A Dynamic and Distributed Scatternet Formation Protocol for Real-life Bluetooth Scatternets" Department of Computer Science and Engineering, The University of Texas at Arlington 2005
- Karl E Persson and D. Manivannan "Secure Connections in Bluetooth Scatternets" Computer Science Department University of Kentucky Lexington, KY 40506, 2003
- K. E. Persson, D. Manivannan, M. Singhal "Bluetooth scatternets: criteria, models and classification" Laboratory for Advanced Networking, Department of Computer Science, University of Kentucky, Lexington, KY 40506, 2004
- Sanif Sentosa Liong, Payam M. Barnaghi "Bluetooth Network Security: A New Approach to Secure Scatternet Formation" School of Computer Science and Information Technology, the University of Nottingham Malaysia Campus Kuala Lumpur, Malaysia
- Will Garner "Diffie-Hellman Key Exchange"; 2008
- Inigo Puy "Bluetooth" 2008
- James Lewis "Bluetooth Security"; ECE 578 7 March 2005
- Pushpa R Suri Sona Rani "Symmetric Key Insecurity in Bluetooth Communication" Department of Computer Science and Applications, Kurukshetra University, kurukshetra, Haryana, INDIA.

Index Terms

Computer Science

Algorithms

Keywords
| Authentication Algorithm | Diffie-Hellman | SNARF |