Information Security Risks Posed by the Bluetooth Security Weaknesses to the Bluetooth-Enabled Phones

1 Chrispus Kimingichi Wanjala, 2 Samuel Mungai Mbugua, 3 Juma Kilwake 1,2,3
Kibabii University, Chwele - Kimilili - Kamukuywa Rd, Kenya
1 cwanjala@kibabiiuniversity.ac.ke, 2 smbugua@kibabiiuniversity.ac.ke,
3.jkilwake@kibabiiuniversity.ac.ke

ABSTRACT

As the widespread use and acceptance of Bluetooth technology increases, concerns are being raised related to security vulnerabilities of this technology. Inadequate device resources and lack of user awareness has compounded this issue where the emphasis on design constraints, functionality and ease of use sometimes outweigh security concerns. The research determines vulnerability of Bluetooth security and the security risks these vulnerabilities poses to the users' information stored in Bluetooth-enabled phones. The research design was based on multi-case study where two cases were selected. Questionnaires and interview were used in data collection. Both qualitative and quantitative approaches were used in data analysis. Descriptive statistical method was used for data analysis. The key findings from the study were that to improve security of information stored in Bluetooth-enabled phones, application layer security should be employed to provide additional security measures not provided in the current authentication and authorization process. Secondly the E0 encryption algorithm currently used for encryption is too weak and therefore the DES and AES algorithm should be used due to their efficiency and reliability. Lastly it was found out that most users have no knowledge on how to configure these devices thus manufactures of these devices should provide users with user documentation that explains the use and device configurations.