Computers & security 4 5 (2 0 1 4) 7 5-8 3

Bluetooth Command and Control channel

Heloise Pieterse [a,*], Martin S. Olivier [b]

[a] Defence, Peace, Safety and Security Unit, Council of Scientific and Industrial Research, PO Box 395, Pretoria 0001, South Africa
[b] Department of Computer Science, University of Pretoria, Private Bag X20, Hatfield 0028, South Africa

Abstract

Bluetooth is popular technology for short-range communications and is incorporated in mobile devices such as smartphones, tablet computers and laptops. Vulnerabilities associated with Bluetooth technology led to improved security measures surrounding Bluetooth connections. Besides the improvement in security features, Bluetooth technology is still plagued by vulnerability exploits. This paper explores the development of a physical Bluetooth C&C channel, moving beyond previous research that mostly relied on simulations. In order to develop a physical channel, certain requirements must be fulfilled and specific aspects regarding Bluetooth technology must be taken into consideration. To measure performance, the newly designed Bluetooth C&C channel is executed in a controlled environment using the Android operating system as a development platform. The results show that a physical Bluetooth C&C channel is indeed possible and the paper concludes by identifying potential strengths and weaknesses of the new channel.