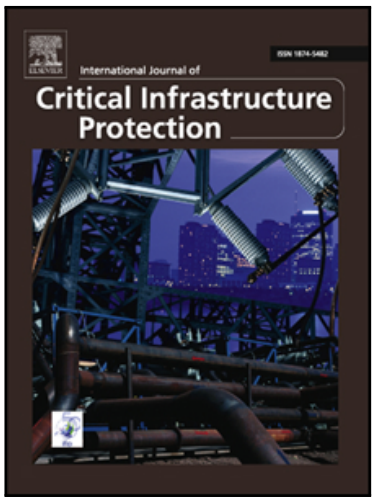

Enabling Bluetooth Low Energy auditing through synchronized tracking of multiple connections

Jose Gutierrez del Arroyo, Jason Bindewald, Scott Graham, Mason Rice

PII: S1874-5482(17)30051-3
DOI: 10.1016/j.ijcip.2017.03.006
Reference: IJCIP 218

To appear in: *International Journal of Critical Infrastructure Protection*

Received date: 9 January 2017
Revised date: 9 March 2017
Accepted date: 12 March 2017

Please cite this article as: Jose Gutierrez del Arroyo, Jason Bindewald, Scott Graham, Mason Rice, Enabling Bluetooth Low Energy auditing through synchronized tracking of multiple connections, *International Journal of Critical Infrastructure Protection* (2017), doi: 10.1016/j.ijcip.2017.03.006

Enabling Bluetooth Low Energy auditing through synchronized tracking of multiple connections

Jose Gutierrez del Arroyo, Jason Bindewald, Scott Graham, Mason Rice[1]

Department of Electrical and Computer Engineering, Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio 45433, USA

Abstract

Bluetooth Low Energy is a wireless communications protocol that is increasingly used in critical infrastructure applications, especially for inter-sensor communications in wireless sensor networks. Recent security research notes a trend in which developers and vendors have opted out of implementing Bluetooth Low Energy link security in many devices, enabling protocol attacks and attack frameworks. To help defend devices with no link security, researchers recommend the use of Bluetooth Low Energy traffic sniffers to generate auditable communications logs. Unfortunately, current sniffers can only follow a single connection at a time, and some are ineffective at capturing long-lived connections due to synchronization problems. These limitations make current sniffers impractical for use in wireless sensor networks.

This paper presents Bluetooth Low Energy Multi (BLE-Multi), a firmware enhancement to the open-source Ubertooth One that enables the sniffing of multiple simultaneous long-lived connections. To increase the capture effectiveness for long-lived connections, a novel synchronization mechanism is proposed that uses transmissions of empty packets to infer information about connection timing. Multi-connection sniffing is achieved by opportunistically switching between connections as they move from the active to inactive state, which is an inherent function in Bluetooth Low Energy to help conserve energy. The experimental evaluations demonstrate that BLE-Multi simultaneously captures multiple active connections while outperforming Ubertooth One when it captures a single connection, paving the way for the development and implementation of automated defensive tools for Bluetooth Low

[1]Corresponding author: Mason Rice (mjrice1761@gmail.com)