CSC 495/583 Fall 2017 Reading Question 1

Dr. Si Chen

Due on: 10/05/2017

BlueBorne

Last week, a security issue called BlueBorne was disclosed, a vulnerability that could be used to attack sensitive systems via the Bluetooth protocol. Specifically, BlueBorne is a flaw where a remote (but physically quite close) attacker could get root on a server, without an internet connection or authentication, via installed and active Bluetooth hardware.

Security research firm Armis has disclosed eight new Bluetooth vulnerabilities on their technical white paper. **Link:** **http://go.armis.com/blueborne-technical-paper**

Select one of the Bluetooth vulnerabilities that involve Stack Overflow attack. In your own words (don't copy from the paper), in two or three sentences, describe this vulnerability in detail (code-level). You can paste code snippets if needed.

Submission

- Please upload your response **in PDF format** to D2L Assignment before 10/05/2017 23:59:59 EDT. Late submission will not be accepted;
- The assignment should be submitted to D2L directly.