CSC 497/583 Fall 2019 Reading Question 2

Dr. Si Chen

BlueBorne

In 2017, 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 one paragraph, 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 deadline. Late submission will not be accepted;
- The assignment should be submitted to D2L directly.