Ben Walker
10-18-18
CSC 495: Blueborne

The l2cap vulnerability works by being able to form a packet with a custom payload (in l2cap_recv_frame), this payload then can be used to overflow the calling function (l2cap_recv_acldata) return address. Since the Bluetooth functions operate at a privileged level, the overflow accesses the return address of a privileged function allowing for privileged access to the host OS. Due to the lack of checking for how large the payload is, allows for this overflow.