CIS551 HW3: Drone Research, Engineering And Defense (DREAD)

Part 2

Team members: Archith Shivanagere, Bowen Bao, Siyang Shu.

1. Our Design

   Our mission is to take control of the drone. In order to achieve that, we first research how the Parrot client software controls the drone. We discovered in their SDK document and confirmed by capturing control packets by Wireshark, that the drone is controlled by commands of the structure: AT*{command name}={sequence number}{,command arguments}\r, which is sent through UDP to port 5556 on the drone every 30ms.

   There is a vulnerability in sequence number, as the drone accepts any sequence number larger than that of the last command, and number 1.

   We also discovered that the drone allows to be controlled by only device at a time, and is distinguished by MAC address.

   Having observed this information, we wrote our control console in C++, sending command messages through UDP to port 5556 with sequence number starting from a large number, which is much larger than that of the current command. Also we forged our MAC address to be the same as that of the controlling device.

   By this design, we are able to completely take over the control over the drone, even in the middle of the control of its former owner.

   We closed telnet connection on the drone by

   “iptables -A INPUT -p tcp -m tcp --dport 23 -j DROP”

2. Possible Defenses

   Allow connection to be established through authentications. This will prevent others connecting to the drone’s network, thus preventing the attack.