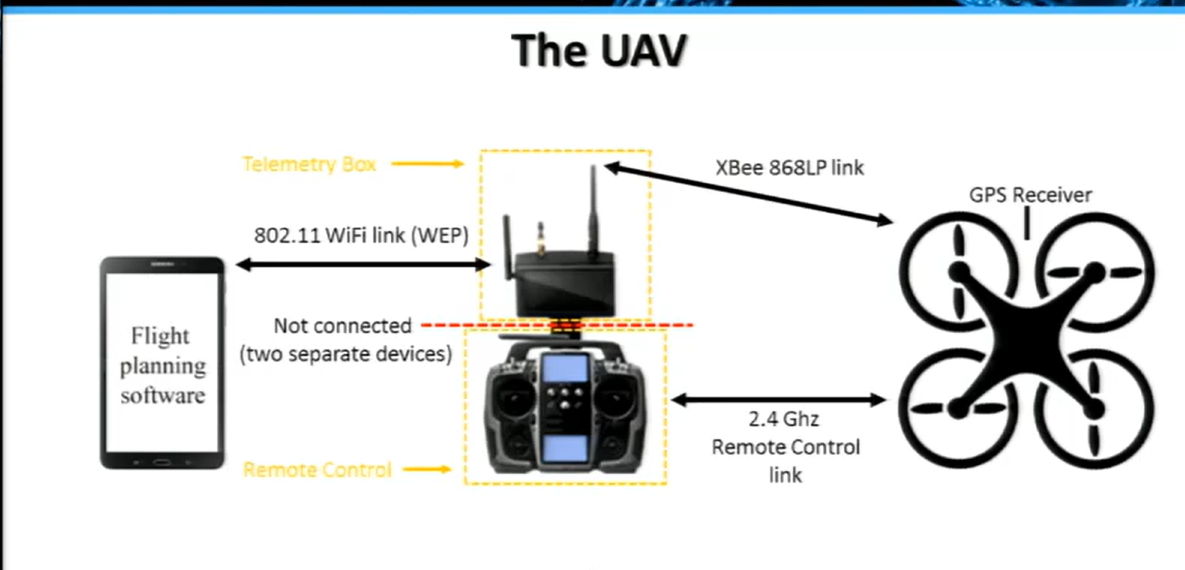
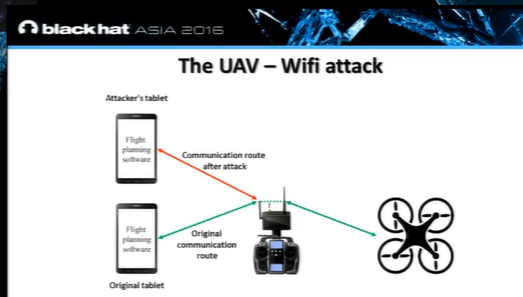
Hacking a professional drone…

This conference is all about security provided in a UAV’s and threats to professional UAVs. There is a difference between a professional UAV and the normal UAVs which are available on the market. They are much more expensive, they can carry up to 3kgs of payload and can be used up to 30 – 45 mins. The UAV system consists of 4 different parts, the UAV, telemetry box, Remote controller, and a device containing Flight planning software. The remote controller is connected with a 2.4Ghz Remote Control link. The telemetry box contains 2 links, one is a wifi link with the device with flight planning software and the other is the XBee link which connects the telemetry box with the UAV



The remote link has a range of 100 meters but the XBee link has a range of up to 2 kilometers. As WEP encryption is somewhat weak, so he attacked the drone by deauth indicating the original user and we can get full control of the drone.



But this attack is limited as the wifi link has a range up to 100 meters so we could exploit the XBee link. The XBee chip on which the telemetry box has some features like API mode, broadcast, remote AT Commands. By using these features one can make an attaker XBee chip (Man-in-the-middle Attack)one can read the traffic(read/send data).In the traffic there are some hex chars are sent. For that we must analyse the android application. By using JD GUI we could visualize what’s going on. Under searching all the files hegot to know a method called send data code command . It’s starts with the static preamble of 5 numbers followed by 3 variables. By transforming it into hexa decimal characters, these numbers are the same ones where we would see in the monitor during the man in the middle attack. Now we can map the commands in the android application.

After this he showed a live demonstration upon the seminar happened