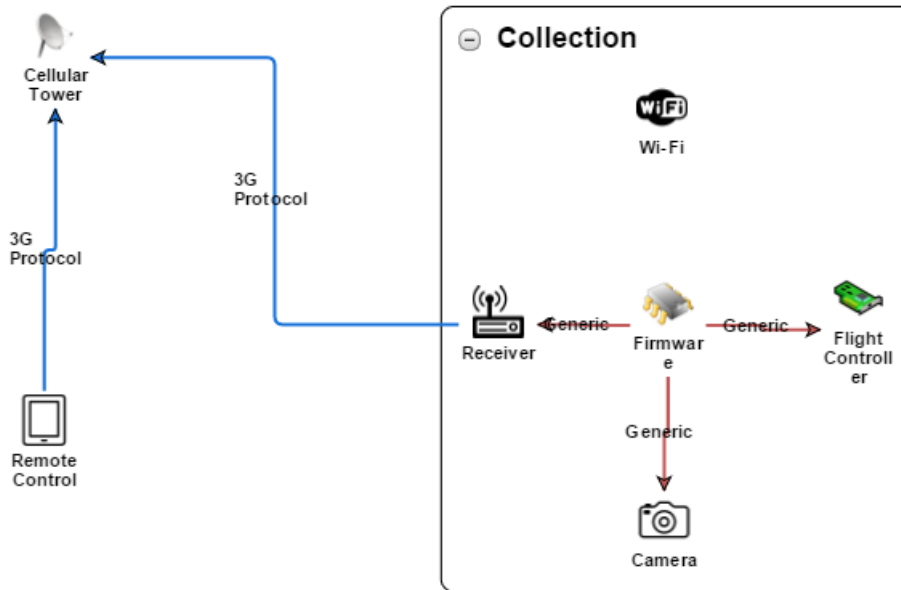


Drone Threat Model - 1

01/17/2017

Threat Model



Threats

Threat	Source	Risk	Status	Date Created
Malware Infection into Product Software	Camera	Critical	Open	01/17/2017
Man in the Middle Attack	Camera	Critical	Open	01/17/2017
Unsolicited Data Collection and Sharing	Camera	Critical	Open	01/17/2017
OS Command Injection	Firmware	High	Mitigated	01/17/2017
Overflow Buffer	Firmware	High	Mitigated	01/17/2017
Insecure Firmware - OWASP	Firmware	Critical	Mitigated	01/17/2017
Denial of Service through Resource Depletion	3G Protocol	Medium	Open	01/17/2017
Cross Site Request Forgery aka Session Riding	3G Protocol	Critical	Open	01/17/2017
Unauthorized Access for Remote Service	3G Protocol	Critical	Open	01/17/2017

Denial Of Service (v3)	3G Protocol	Low	Open	01/17/2017
Cross Site Scripting	3G Protocol	Medium	Open	01/17/2017
May be Subject to Elevation of Privilege Using Remote Code Execution	3G Protocol	Medium	Open	01/17/2017
IMSI paging attack	3G Protocol	Critical	Open	01/17/2017
Authentication and Key Agreement AKA protocol attack	3G Protocol	Critical	Open	01/17/2017
Spoofing	Cellular Tower	Critical	Open	01/17/2017
Dictionary-based Password Attack	Wi-Fi	High	Open	01/17/2017
Password Brute Forcing	Wi-Fi	High	Open	01/17/2017
Man in the Middle Attack	Wi-Fi	Critical	Open	01/17/2017
Password Cracking	Wi-Fi	Critical	Open	01/17/2017
WiFi Credentials Exposed	Wi-Fi	Critical	Open	01/17/2017
Hardcoded Crypto Keys	Wi-Fi	Critical	Open	01/17/2017
