RSAConference2020
Asia Pacific & Japan

A Virtual Learning Experience | 15–17 July

HUMAN ELEMENT

SESSION ID: **GPS-F05V**

Drone Penetration Testing And Vulnerability Analysis Framework

Dr. Vivek Balachandran

Assistant Professor
Singapore Institute of Technology

Drone Attack

- Drones are the future
  - Cheap and cost effective
  - Easier to deploy
  - Great tool for surveillance
  - Limited hindrance
  - Limited danger
- RIE 2020
  - A focus area is Urban Mobility
  - Fusing traditional transport engg with autonomous technology
  - New set of vulnerabilities and challenges

Drone Challenges

- Drone Deployment challenges
  - Integrating safely into the airspace
  - Reliability of the aircraft
    - Communication modules, OS vulnerabilities, RF jamming etc.
- Operational level
  - Needs a comprehensive vulnerability map
  - Manufacturers may not divulge the information
  - Counter drone signal jammers
  - Existing Vulnerabilities

Examples of known vulnerabilities

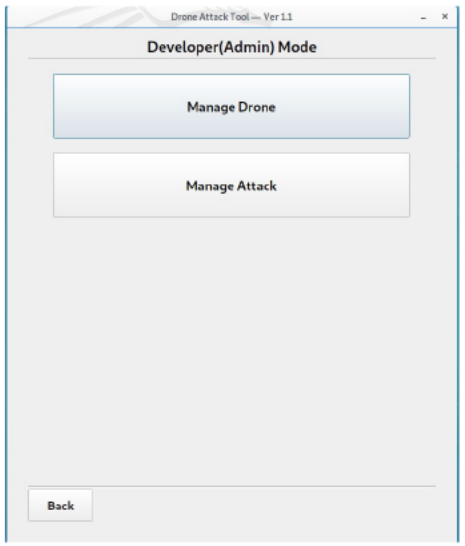
- Swann
  - hardcoded password and an authentication bypass (2017)
- DJI Phantom
  - GPS Spoofing
- Parrot AR
  - WiFi attack using Aireplay-NG
  - Deauthentication

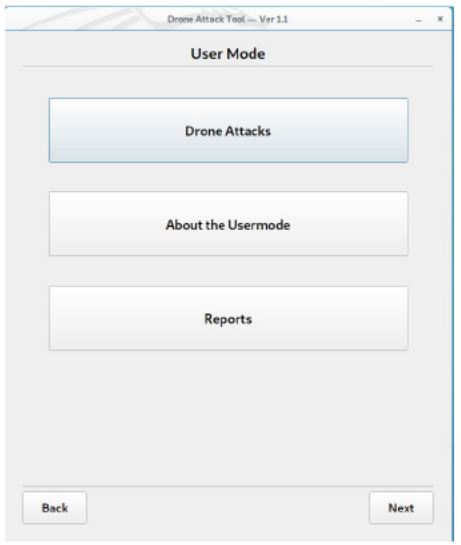
Our Solution

- No centralized framework for Drone PT
  - Independent works exist in literature
  - Mostly as academic pursuits
  - And in forum discussions
- Goal
  - Open source platform for drone attacks
  - Easy to launch attacks on different types of drones
  - Easy to add new attack modules
  - Local and server database

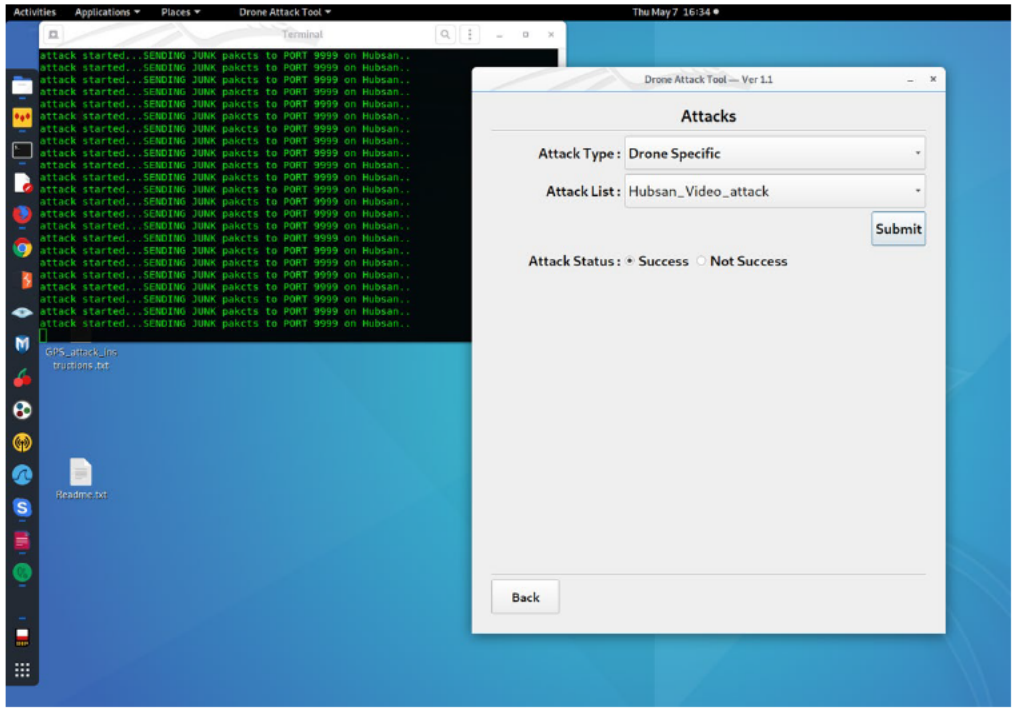
Framework

- DRAT (Drone Attack Tool) has been developed in Kali Linux as Penetration testing tool and vulnerability analysis tool for Drones. It has local database with search function and report creation feature.
- User Mode
  - Launch existing attacks
  - Generate reports
- Admin Mode
  - Enables to add new attack modules



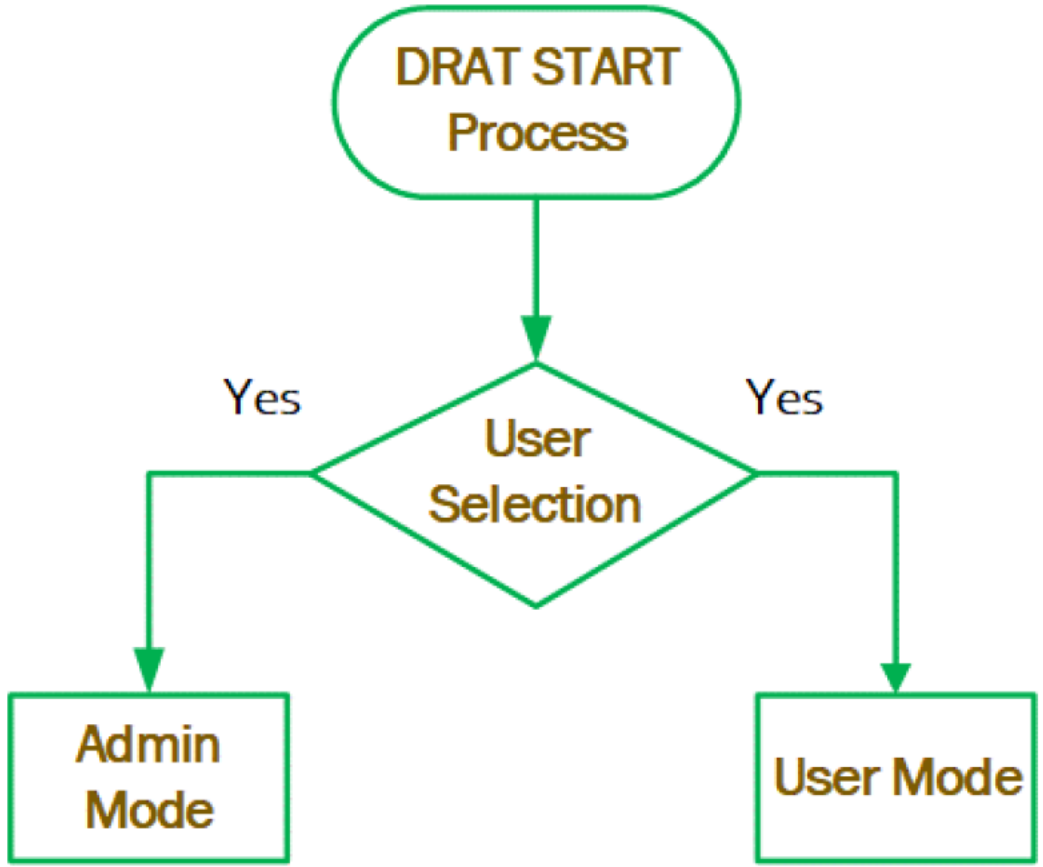


DRAT

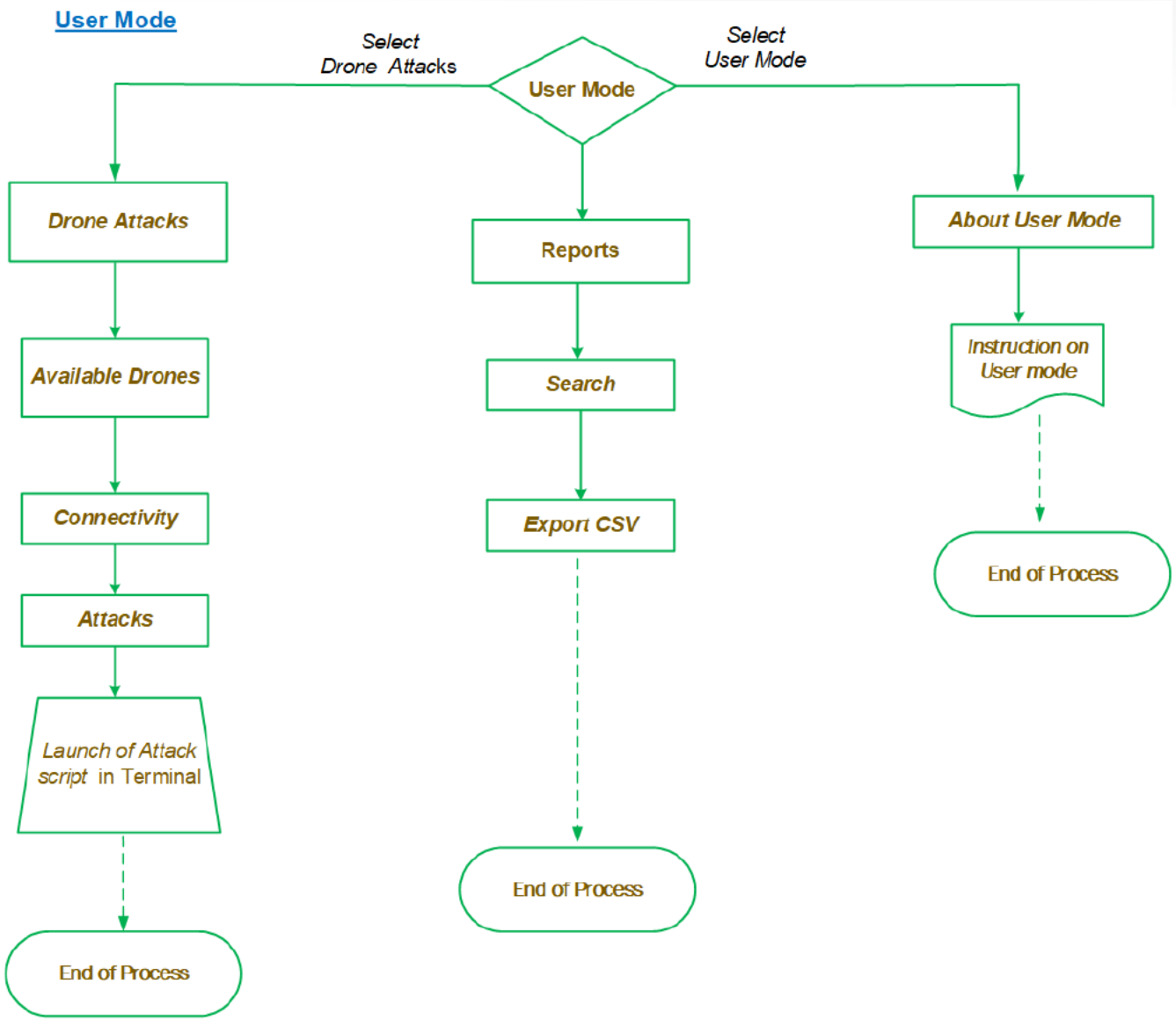

Activities
Applications
Places
Drone Attack Tool
Thu May 7 16:34
Terminal
attack started...SENDING JUNK pakcts to PORT 9999 on Hubsan..
Drone Attack Tool — Ver 1.1
Attacks
Attack Type : Drone Specific
Attack List : Hubsan_Video_attack
Submit
Attack Status : Success Not Success
Back
GPS_attack_Ins truction.txt
Readme.txt


Denial of Service
Line Of Sight (LOS)
Drone Hijacking
Cracking of Drone Password

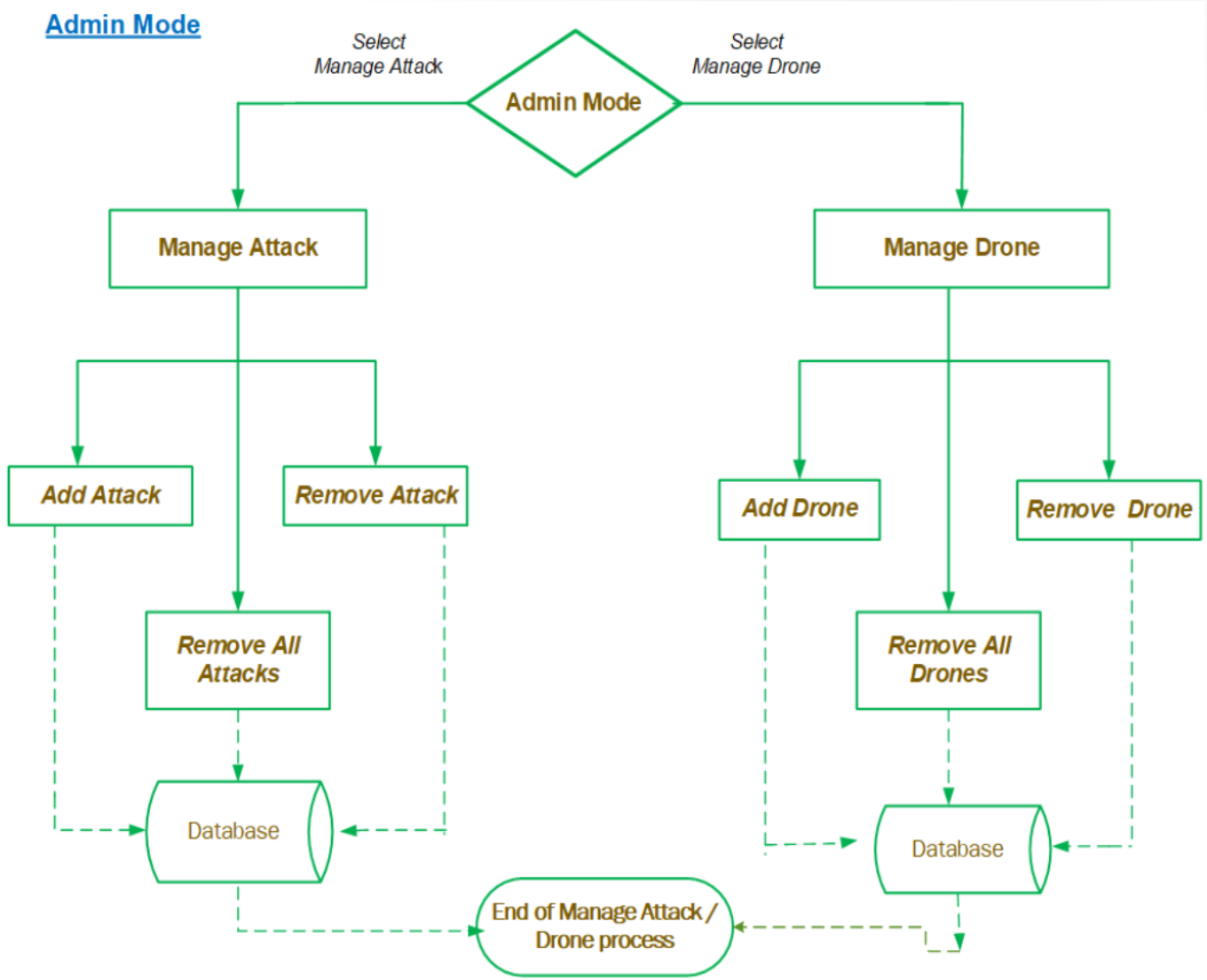
DRAT Control Flow Diagram



DRAT Control Flow Diagram: User Mode



DRAT Control Flow Diagram: Admin Mode



Attacks currently available in the framework

- Tello attacks:
  - Video Disruption
  - Wi-Fi password crack (WPA2)
  - Denial of Service (DoS)
  - Disrupting the Line-of-Sight
- Hubsan attacks:
  - Wi-Fi password crack (WPA2)
  - Authentication Request Flooding
- Mavic2 Pro/Enterprise attacks:
  - GPS Spoofing
  - Firmware Modification
  - Reverse Engineering

Tello Attacks

- Video Disruption
  - Froze video
  - Junk packets send to the udp port 9999
  - Need to know Drone's IP address
- Wi-Fi WPA2 password crack
  - Dictionary attack
  - Using Aircrack-NG
- DOS
  - Disrupts the command from the controller
  - Deautheticating the controller
- Line of Sight
  - Disrupts video transmission
  - Controller has to navigate without video stream
  - ARP poisoning

Hubsan Attack

- WiFi- WPA Attack
  - Dictionary attack
  - Using Aircrack-NG
  - Similar to Tello
- Authentication Flooding
  - MAC Spoofing
  - Tool has the same MAC as client controller
  - Multiple reconnection to the drone

Mavic Enterprise/Pro

- GPS Spoofing
  - Using HackRF h/w
  - No fly zone emulated to land the drone
- Firmware modification
  - Internal configuration values tweaked
  - brake sensitivity from 0.6 to 2
- Dji App reverse engg
  - Bypassing authentication
  - Offline Login
  - Remove Online Function
  - Remove Update Force
  - Remove Firmware Upgrade Service
  - Allow 'unsupported drones' on App

Work under progress

- More drones to be included
  - DJI Mavic Mini
  - Codrone
  - DJI Phantom 4 Pro v2
- More attacks are under development
  - GPS Jamming
  - Replay Attack
  - GPS Spoofing with rooted smartphone
  - Sniff the USB traffic between RC and Mobile phone
  - Attacking the video streaming RTSP (Real Time Streaming Protocol)

Release Status

- Where can we find it
  - Soon on github public
  - After the review with our collaborator and user
- What can you get
  - A drone pen testing framework
  - Readily available attack modules
- How can you contribute
  - Can add your own attack modules once published

RSAConference2020 APJ

A Virtual Learning Experience

Thank you