B.Tech Project Evaluation-2, VIIIth Sem

PORTABLE VULNERABILITY ASSESSMENT SYSTEM FOR WIRELESS AS DATA TRANSITION ANOMALY IN IOT

Presented by :-

UDIT PRABHAKAR, 2018007643
ABHISHEK SHARMA, 2019643445
ASTHA AGRAWAL, 2018014082
SHUBHAM JHA, 2018011469

Under the Supervision of:-

Mr. AVINASH KUMAR
Assistant Professor, Department of Computer Science and Engineering, Sharda University, Gr. Noida
M.Sc, Cyber Security, United Kingdom.
Certified Ethical Hacker.

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING
SCHOOL OF ENGINEERING AND TECHNOLOGY
02, April, 2022

Approval from guide for the evaluation

Workload distribution of the team

Task	Udit	Abhishek	Astha	Shubham
Literature Survey	Y	Y	Y	Y
Problem Formulation	Y	Y	Y	Y
System Modelling/Costing	Y	Y	Y	Y
Scripts	Y	Y		
Simulation/Hardware	Y	Y	Y	Y
Patent Writing	Y	Y		
Report Writing and Other Paperwork	Y	Y	Y	Y

Why it is needed to hack drones :

To monitors, stop and capture unauthorized drones which is flying in surveillance area which may be a potential threat to organization or government agencies that may carry explosives or might have intentions to steal sensitive information.

Subdomain of our main problem statement :

Drone uses Two Transmission medium for communication

    i) Wi-Fi Signals

    ii) Radio Frequency
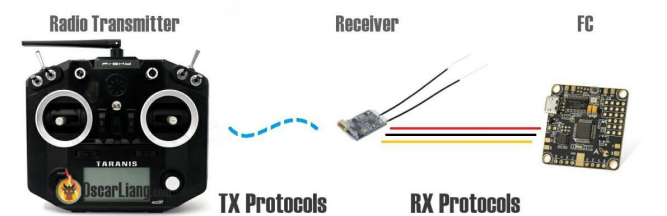
WiFi operated drones -

Solution - Wifi adapter with monitor mode is the best solution for deauthenticating a drone wifi signals from the operator

Supported hardware :- Tplink 722n, Alpha wifi cards

Radio Frequency

Solution - RTL SDR is the solution for drones which works on radio frequencies for receiving live radio signals
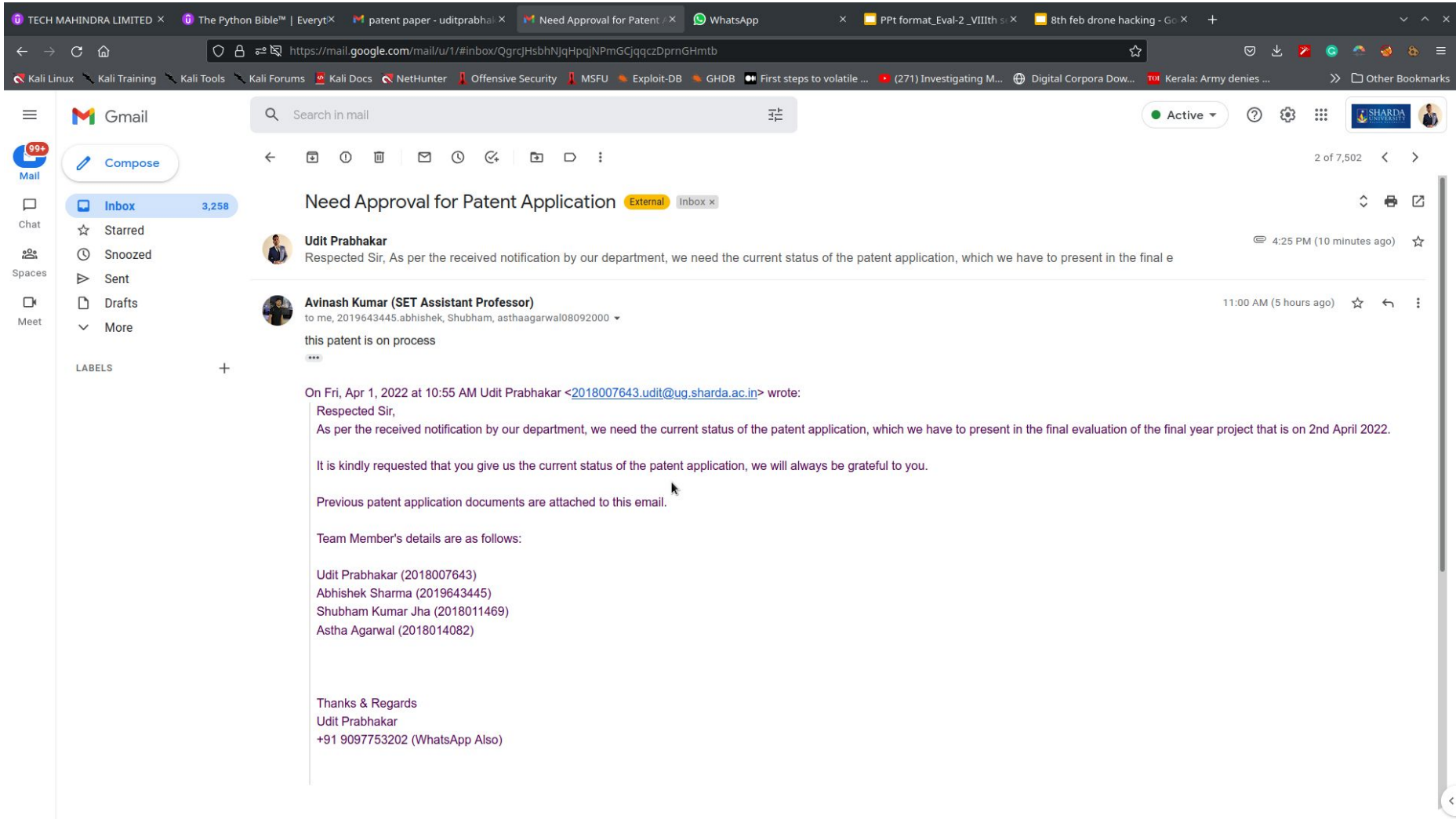
Supported Hardware:- RTL SDR

Improvement/Work done from the last evaluation

- Manually monitors and deauthenticated the target and solved wifi drones problem

- Radio drones solution is still in testing

- Tested for 2.4 Ghz drones

- Automated Script (.ssh) is partially working, Further improving it.

Project overview:

- The project tries to hack the drones which are not legitimate. It aims at monitoring and identifying the unfavourable drones which are being controlled by the intruders or the hackers who are meant for causing some form of destruction or harm.

- The project consists of a wifi gun and the deauthentication code. The wifi gun monitors all the available wifi signals within the system range to keep track of any unwanted drone in the area. It detects all the wifi drones and distinguish them as the favourable drones and the unfavourable drone (which is being controlled by the hacker). Whenever any hacker or an intruder enters into the range with his drone, the system identifies it and deauthenticate that drone such that it no longer remains under the control of the hacker and is taken down. The drone is now under the control of the system.

- This project is a part of smart security and surveillance of the city. It basically targets the public places where some form of events are being organised, like festive functions, public rallies etc, or in the risky areas which requires security services.

Proof of paper accepted or communicated/ Hackathon/ Patent