# ISM FINAL PRODUCT
# PRODUCT PROPOSAL AND CALENDAR

MANAV SOOD, AKASH BASKARAN

***Introduction and Statement of Purpose***

For our ISM Final Product, we propose to create the Danger Drone in order to test the vulnerabilities of networks, security technology, and devices from a remote distance. The Danger Drone is an unconventional penetration testing tool first displayed at the DEFCON whitehat/blackhat hacker conference in 2016. Our goal is to create an improved, customized version of the Danger Drone by 3D printing originally designed parts and components as well as implementing a Raspberry Pi core running Kali Linux, which is a Linux distribution designed for digital forensics and penetration testing. Currently, we intend to set up an “IoT Village” with multiple IoT devices and routers in order to deploy and test our Danger Drone to exploit and exhibit the vulnerabilities of the world’s most common IoT consumer devices. Through this demonstration, we hope to display cybersecurity-related skills gained through research, observation, and hands-on learning and follow in the path of the original Danger Drone in educating the masses of the threats apparent in the new wave of cyber terrorism.

***Review of Skills and Research***

The core object of our Original Work Project, which was the revision of the IoT Security Improvement Act of 2017, centered specifically around IoT devices. The objective of the Danger Drone would take the knowledge gained from research during the creation of the Original Work project and apply that information in a more technical and pragmatic approach. Furthermore, industry-related skills will come into play when designing and installing the Raspberry Pi core, Kali Linux operating system, and IoT Village upon which we intend to deploy the drone. This project will also assess and display our understanding and skills with the large number of tools and programs catalogued in the Kali Linux distribution, which is an industry standard in the field of cybersecurity.

### ***Methodology***

In order to create our variation on the Danger Drone as well as the IoT Village it will be tested in and upon, we will need to follow a carefully designed procedure. In order to make the drone, the skeleton of our proposed methodology includes the following:

1. Acquire the supplies required, including an environment to 3D print as well as motors to allow drone flight and the Raspberry Pi core.
2. Design the body of the drone, as well as the physical systems upon which we will mount the tools used for penetration testing.
3. Carefully research the ideal routers and related devices to be used in our network topology in creating the IoT Village and the Danger Drone.
4. Design and implement the test network, as well as implementation of the drone’s capabilities.
5. Attempt to conduct penetration testing on the test environment with the configured Danger Drone.

### ***Materials***

Due to the large numbers of devices in this product, some expense will be required to gather all the supplies needed. Including motors, 3D printing, a Raspberry Pi and penetration testing accessories, as well as some of the Internet of Things devices to be used in the testing environment, the total cost could accumulate to roughly $500 to $700 dollars.

### C***onclusions***

We anticipate the outcome of this product to be an originally designed, well-implemented, and successful Danger Drone, capable of flight, penetration testing, and other exploitation services. In creating this product, we aim to become well-versed in the tools and programs used by many professionals in the industry today and develop our knowledge and understanding of fundamental cybersecurity concepts such as IoT device protection, penetration testing, encryption, and end-user best practices among others. The original Danger Drone served to educate companies and warn consumers and workplaces of the threats prevalent in a new age of cybersecurity to usher in directed and focused development of security tools, practices, and education as to better protect businesses and users. We hope our Danger Drone implementation will serve a similar purpose, while also displaying a culmination of our knowledge and experience in a creative and tangible manner.

***Development of Product Calendar/Timeline***

| **Date** | **Task** |
|---|---|
| 1/31 | Share product proposal with mentors, receive feedback and revise. |
| 2/1<br>to<br>2/9 | Research construction of danger drone, schematics, penetration testing, internet of things devices, construction of testing environment |
| 2/15 | FInalize drone plan, devices to be used in topology, begin securing materials |
| 3/1 | Continue experimentation with Kali Linux penetration testing tools, complete gathering all materials needed |
| 3/1 | Begin construction of drone portion, design testing environment |
| 4/1 | Completed construction of drone without penetration testing capability, complete construction of testing environment |
| 4/5 | Begin penetration testing of test network without drone, finalize testing methodology, begin integrating penetration testing technology with functional drone |
| 5/1 | Complete final Danger Drone, conduct penetration testing on network, document results and begin analysis |
| 5/5 | Complete extensive analysis of penetration testing with Drones on IoT networks and popular routers |