Team Threat Modeling Exercise #2-
Actors personas

Participant #1 37 Participant #2 55
Participant #3 46
Date _____ Course Info Security managment

Instructions for Persona-Non-Gratae Threat Modeling Study

1. Please start by reading the short article entitled "Keeping Ahead of our Adversaries". This article introduces an example of the Implantable Cardioverter Defibrillator (ICD). It summarizes the use of Security Cards and introduces the idea of using personas for threat modeling instead of using Security Cards.

2. Take a look at the two examples of Persona-non-Grata (PNGs) for the ICD system (shown in pages 2 and 3 of this document). Note that a PNG tells us something pertinent about the person who intends to maliciously attack the system. We learn about his/her motivation, goals, and skills. We then see a list of specific misuse cases that the attacker will follow in order to achieve his/her goals.

3. There are several ways in which you could systematically identify PnGs for a system. For purposes of this exercise we will use a brainstorming activity as follows:

    a) First, individually try to think of 4-5 PnGs for the system. Just give them a short description (e.g. Bitter and revengeful competitor who plans to give the ICD a bad reputation through random attacks).

    b) As a group – evaluate all of the PnGs. Identify similar/redundant ones. Select 5-7 most representative and most critical PnGs.

    c) Within your group assign 2-3 PnGs to each person to develop (following the examples of Marvin and Angela).

    d) Try to be as specific as possible about the misuse cases. For example "Angela will hack the system to modify the therapy patterns" is not very precise; whereas the example PnG gave more specifics about specific logs that she planned to purge and/or modify.

    e) Check each other's PnGs for quality and then submit.

Justin
UAV Test Engineer
Disgruntled and malicious

Justin is a UAV Test Engineer, who works for the company that is building and supplying the drones. After losing a job promotion to a co-worker that Justin felt was less qualified, he became increasingly disgruntled with his boss and feels unmotivated. Justin does not feel valued and no longer has loyalty to the company.

Goals:

- Damage the company's reputation by causing disruption to the drones during missions.
- Cause damage to the fleet of drones.
- Threaten the safety of people in the surrounding areas.

Skills:

- UAV Test Engineer/flight plan and operations skills
- Drone security hacks

Justin's Misuse Cases which Threaten Correct Operation of the Drones	
1.	Spoof the UAV's GPS signal in order to take control of the leader craft and send coordinates that redirect the drones away from the mission.
2.	Spoof the UAV's GPS signal to take control of the swarm of drones and deliberately crash them. The can cause damage to the fleet, ruin customized equipment on board, and potentially harm people in the surrounding areas.
3.	Interfere with the wireless connection in order to disconnect the leader craft from the base control station and gain control of the drone.

Maria
Computer Science Graduate Student
Part-time Hacker

Maria is in her final year of graduate school as a Computer Science major. In order to sharpen her computer science and security skills, she researches hacking techniques and then practices it in real life. Maria loves a challenge and gets a thrill whenever she can hack into something successfully. Recently, she came across an article about drones and was intrigued by the potential security concerns.

Goals:
- Identify security breaches
- Deepen understanding of security threats

Skills:
- Background in computer science
- Hacks for fun in her spare time

Maria's Misuse Cases which Threaten Correct Operation of the Drones	
1.	Deploy application software on a drone to look for smartphone signals while it is searching for a Wi-Fi network, allowing Maria to potentially steal the victim's data (user credentials, credit card numbers, location data).
2.	Use a channel hop attack to jam the Wi-Fi network, allowing Maria to gain complete access of the drone. She can cause potential harm if she loses control and crashes it.
3.	Use a signal jammer to emit radio frequency waves to prevent the drones from making or maintaining their connections.

Name: Aqib

Role: Talented MIT Graduate Mechanical Engineering Student

Moniker: Bitter, Resentful and Radicalized.

Aqib is a second generation Muslim born and raised in the United States. Growing up he is always being teased and picked on because he doesn't fit in. Attending MIT John is facing an identity crisis. He is still He is lost in life and attempting to find his identity. He feels rejected by the culture that surrounds him and beginning to develop resentment and raged. Where then he encounters ISIS operatives that make him feel included and valued. They legitimized and reinforced his resentments for the western culture.

Goals:

•To steal drones by jamming radio signal and sending wrong GPS coordinates.

•Mount with explosives then redirect drones to heavy civilian traffic area and detonate while remain invisible.

•Cause maximum damage civilian and surrounding infrastructures to satisfy his resentment.

Skills:

•Knowledge of machines, aircrafts, drones including their designs, uses, repairs and maintenance.

•Well versed in Computer and Electronics, including circuit board, processors, GPS chips, electronic equipment, and computer hardware and software, including applications and programming.

• Well versed in Chemical composition, structure and properties of substances and chemical processes.

Aqib's Misuse Cases which Threaten Correct Operation of the Drones	
1.	Jamming radio signal between lead drones and base station, which will disconnect it from ground controller.
2.	Via spoofing - send the lead drone wrong GPS coordinates tricking it into believing that it was near base station and landing the entire swarm in an area where they can easily be retrieved.
3.	Re-equip drones with homemade explosives and reprogram GPS destination coordinate on lead drones
4.	Sending swarm equipped with explosive crashing into passenger planes causing explosion and loss of lives.
5.	Sending swarm equipped with explosive crashing into heavy pedestrian area (music events, sport events killing and injuring innocent lives.

Name: Peter
Job title or role: Poacher
Moniker: Obsessed with hunting and guns, gets pleasure from others misfortunes

Peter likes to spend time in the country and woods, and makes his own guns and weapons as a hobby. He enjoys killing endangered animals for personal pleasure and profit, and has been doing this for many years. Recently he has encountered drones that pass by him while he is hunting and they have become more frequent. He now has the idea that it would be fun and useful to shoot these drones down. He has a friend named Jack who is experienced in aviation and GPS technology.

Goals:
- To make money, commercial gain
- To feel accomplished and have a thrill.

Skills:
- Expert hunter
- Access to weapons, can make his own weapons
- Connections to underground markets

Peter's Misuse Cases which Threaten Correct Operation of the Drones	
1.	Peter can shoot down the drones that pass by causing them to be damaged or destroyed. It would be a loss to the people funding the drone operations and to the beneficiaries.
2.	Contact his friend Jack who has the ability to patch into the drone GPS system. Peter will then know where the drones are and when they will be coming. He would be able to shoot down the drones more easily.
3.	Peter can steal parts from the drones and the supplies that the drones are carrying and sell them in underground markets. These items would not be retrievable.

Alfred is a software engineer who is scared of drones. He watches a lot of sci-fi movies and has watched videos on new drone technology (such as “The Attack of the Drones” documentary). He has become fearful that drones may go out of control and cause damage or kill him and other people. He wants to help those who are also scared of drones, and he leads a group of supporters called the DPC (Drone Phobia Coalition).

Name: Alfred
Job title or role: Software Engineer
Moniker: Fearful, has drone phobia

Goals:

- To hack the drone system or get unauthorized access to the system and the ability to control the drones
- Have more peace of mind to know he and his supporters will not get attacked by drones

Skills:

- Expert engineer
- A lot of experience in software development and security
- Ability to be a strong leader and persuade people

Alfred’s Misuse Cases which Threaten Correct Operation of the Drones	
1.	Alfred hacks into the system by obtaining signing keys. He is able to control the drones and access private information about operations, such as where the drones might go. He gives this information to his supporters
2.	Alfred diverts the drones if the operation would require them to go near one of his supporters. This may end up causing the whole mission to fail, because of the delayed route.
3.	Alfred phobia of drones may become more severe and he may want to just destroy the drones altogether so that he would not have to worry about them at all. With access to control these drones, he could crash them in a remote location.
3.	Interfere with radio signal between lead drones and base station so that operation of mission could not happen at all.

Name: Antonio
Job title or role: Experienced UAV Pilot working at Controller Base
Moniker: Financially distressed. Looking for ways to earn extra income.

Antonio is a talented UAV pilot. He has been working at the controller base for 15 years and had successfully completed numerous mission. Over the years Antonio had become acquainted with all the different geographical terrains and GPS locations. In recent year he develops a taste for gambling and becomes heavily indebted. Running out of money and option to satisfy his gambling habit, he turns to the drugs cartels back home. With the promise of cash rewards, he agrees to assist the cartels in smuggling drugs across the border using the UAV's that he piloted. With each successful job he will receive a substantial cash reward.

Goals:

- To make as much money as possible by using drones swarm to make illegal deliveries.
- To make as many illegal deliveries as possible while without doing any harm to the swarm and its surrounding while remain undetected.
- Successfully make all deliveries attempt in order to get paid.

Skills:

- In-depth knowledge of standard aviation (including UAV) practices and procedures
- Experienced and well versed in UAV navigation utilization GPS coordinates.
- Well experienced in navigating UAV through difficult terrains and international borders.

Antonio's Misuse Cases which Threaten Correct Operation of Drones	
1.	Abusing job title by using government's property to deliver illegal goods for personal gain. Tarnishing and jeopardizing the reputation of the organization if discovered.
2.	Manually overwritten GPS coordinates to send UAVs to Mexican drug cartels in remote location to pick up drug packages and make delivery back to drug deals in the US.
3.	Deviate UAVs from mission critical assignment in order to make more time for illegal deliveries. This will tarnished the reputation of the organization and may cost lives and other unforeseen damages due to mission failure.
4.	Erasing/modifying GPS logs in order to cover up any traces of UAVs GPS coordinates that are not authorized.