<Interrupting Satellite Communications>

# Identification

Use Case ID: <assigned by Cyber M&S SG>

Description:

Domain: Training

Table 1. POCs

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Organization** | **Role** | **Email** |
| Jonathan Harris | NAWCTSD |  | Jonathan.T.Harris@navy.mil |
|  |  |  |  |

Table 2. Change Log

|  |  |  |
| --- | --- | --- |
| **Version #** | **Date** | **Changes** |
|  |  |  |

Relationship to other use cases:

* <use case ID> - <Description of relationship>

# Goals and Measures of Performance (MOPs)

The goal for this use case is to assert superiority over a nation by interfering with its ability to patrol and maintain its maritime trade routes. This use case is designed to showcase the might of a nations cyber abilities as a method to pressure other countries to support and enforcement their sanctions.

## Goals

1. Impact ability to track the commerce vessels in a heavily traveled trade route
2. Impact the maritime vessels data link to higher level headquarters on its assigned mission
3. Cause panic and confusion and lack of confidence of the vessel’s crew by deploying some countermeasures without the crew intending them to be deployed

## Measures of Performance (MOPs)

1. Show at least 10 additional AIS tracks on displays that don’t actually exist in the water that might represent undocumented (untaxed) commercial traffic and change random commercial vessels to personal watercraft.
   1. Can be measured with senor mismatch from radar tracks
      1. e.g., a 1000ft personal watercraft vessel
      2. e.g., large vessel showing no radar footprint
2. False orders are sent via compromised data link to investigate an oil tanker believed to be carrying oil from sanctioned nation but it turns out the vessel is a passenger cruise ship.
3. Without warning the defensive countermeasure of anti-missile chaff and flairs are deployed

## Goal / MOP Crosswalk

Table 2. MOPs for Measuring Achievement of Goals

|  |  |
| --- | --- |
| Goal 1 | * MOP – Sensor failure - add false AIS Tracks |
| Goal 2 | * MOP – Spoofed Mission Assignment |
| Goal 3 | * MOP – Deploy countermeasure without user interaction |

# Scenario Exemplar

A coast guard ship is patrolling national waters to ensure compliance with laws and orderly flow of goods through their trade routes. While on patrol, they notice a larger than normal number of yachts in shipping lanes and stationary tankers in the bay areas. Upon further investigation, the AIS tracks aren’t matching radar readings. At the bridge while trying to investigate the sensor readings mismatch, a data link message comes in to investigate a suspected oil tanker originating from an adversarial nation illegally transiting national waters. When the coast guard intercepts the ship, they realize the vessel is a commercial passenger cruise ship. Once the captain relays back to headquarters the information, they realize they are under a cyber-attack and attempt to head back to port. The crew is confused and second guessing everything. While securing the ship for docking in the bay, a bridge warning goes off that they have an inbound attack and the chaff and heat flairs are automatically deployed. In the panic and confusion, the captain orders the ship to power off and secure all weapon systems and wait for a tow in to the port.

# Conceptual Model

The attacks consists of integrality issues for various sensors and a MITM injection of false orders from the ships chain of command. It also includes an unauthorized and not-initiated use of defensive countermeasures. By spoofing AIS signatures and adding in noise (additional non-existent tracks) to the system, the crew is left confused and concerned about the reliability of their data. This is further amplified by the ship being given (MITM injected) data link orders to intercept a rogue ship. When this is revealed to to be another issue, the captain starts to be concerned and doesn’t have trust in his ability to operate safely. He orders a return to port for investigation. That’s when the crew is alerted to the ongoing cyber-attack. The crew should reduce attack vectors by shutting down external network access and that is when a system is triggered from an external entity to fire off flairs and chaff.

* Attacks –adding/modifying sensor feeds, injecting modified data link traffic,
* Effects – Spoofed AIS, execute a modified mission, unintended trigger of flairs
* Network – wireless AIS, encrypted Data Link

Describe level of resolution necessary for entities, e.g. aggregate, packets, effects. Consider representing actions graphically as vignettes or interactions.>

# Potential components

The components that will be needed is (1) High fidelity simulation of a ship with ability to control (2) sensor feeds such as AIS & Radar (3) intercept and modify Data Link messages (4) and ability to control countermeasure systems like flairs and chaff.

* + Simulation assets (with LVC categorization)
    - Ship with AIS, Radar, Data Link
    - Ship that can model flairs and chaff

# Derived Data Exchange Model (DEM) Requirements

* Spoof data and ability to impact integrity
* MITM attack of data link streams (for modified mission)
* Trigger countermeasure effects

# Notes, Anomalies, Challenges

* Challenge to find a model of a constructive ship to support AIS, Radar and Data link
* Representing Chaff and flairs may be a challenge in a constructive simulation

# References

# Acronyms

AIS - Automatic Identification System

IP – Internet Protocol

MITM – Man-in-the-Middle

MOP – Measures of Performance

NAWCTSD - Naval Air Warfare Center Training Systems Division