GPS Spoofing of UAV Case Study

Carol Woody

April 2021

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.
The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

DM21-0352

GPS Spoofing of UAV Case Study

Background

The root causes of vulnerabilities are a challenge to determine. Available information points to activities that occur in the operational system and tracking this back to the code is one level of abstraction. Tools can be useful in reengineering some of this information. However, tracking it back to design decisions that created weaknesses requires another level of abstraction from the code and there is only context and subject matter expertise that can help piece this together. One level of support that can point to possibilities is the Common Attack Patterns and Enumerations (CAPEC) but these are not specific to any design.

This case should be used in conjunction with threat modeling and risk analysis to provide an understanding of the impact of poor design choices on operational systems. Too frequently designers are so far removed from the actual operational environment that they fail to notice choices the make that lead to security issues.

To prevent these design weaknesses, systems requirements must include scenarios for misuse and abuse that the system is not to allow to happen. These become constraints on the design to ensure that unwanted behaviors are not allowed.

Case Study Overview

This case study is designed to give the student practice in reviewing available information to determine if design adjustments are needed to address a vulnerability. Materials from an actual incident (news reports and assessment documents) to provide a context but it will be up to the student to determine what design changes, if any, would be helpful in addressing the vulnerability.

Student Instructions

1. Review the media reports and develop a use case that describes the threat scenario.

   Media reports – Lockheed Martin RQ-170 Incident
   - http://www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer-Video
   - http://www.nytimes.com/2012/04/23/world/middleeast/iranians-say-they-took-secret-data-from-drone.html?_r=1&

   Humphreys, Todd. *Statement on the Vulnerability of Civil Unmanned Aerial Vehicles and Other Systems to Civil GPS Spoofing*. http://homeland.house.gov/sites/homeland.house.gov/files/Testimony-Humphreys.pdf (2012).
   Tippenhauer, Nils O.; Pöpper, Christina; Rasmussen, Kasper B.; & Capkun, Srdjan. "On the Requirements for Successful GPS Spoofing Attacks," 75–85. *Proceedings of the ACM Conference on Computer and Communications Security (CCS*). Chicago, IL, Oct. 2011. ACM, 2011.
2. Analyze the scenario to identify potential design flaws that allowed the incident to occur
   a. Map these to the relevant Common Weakness Enumerations (CWEs)

   b. Identify possible CAPEC attack patterns exploited by the attack
3. Identify mitigations such as controls and alternate design decisions that could be used to remove the weaknesses.

Instructor notes

This exercise can be used in teaching the topics of threat modeling and risk analysis to help the students understand the complexity in connecting threats and vulnerabilities to systems design.

The resulting scenarios can be structured for misuse and abuse scenarios which would be part of requirements a system engineer should be given for a system design. Unfortunately, too many systems are designed without consideration of these scenarios which results in design choices that provide weaknesses for attackers.

This example shows that knowledge of both the possible threat and how the system is designed to operate work together to provide a weakness for a successful attack.

Example solution

Threat If a malicious attacker gains control of an UAV
Consequence Then the UAV could be used to attack US forces
Attack Steps

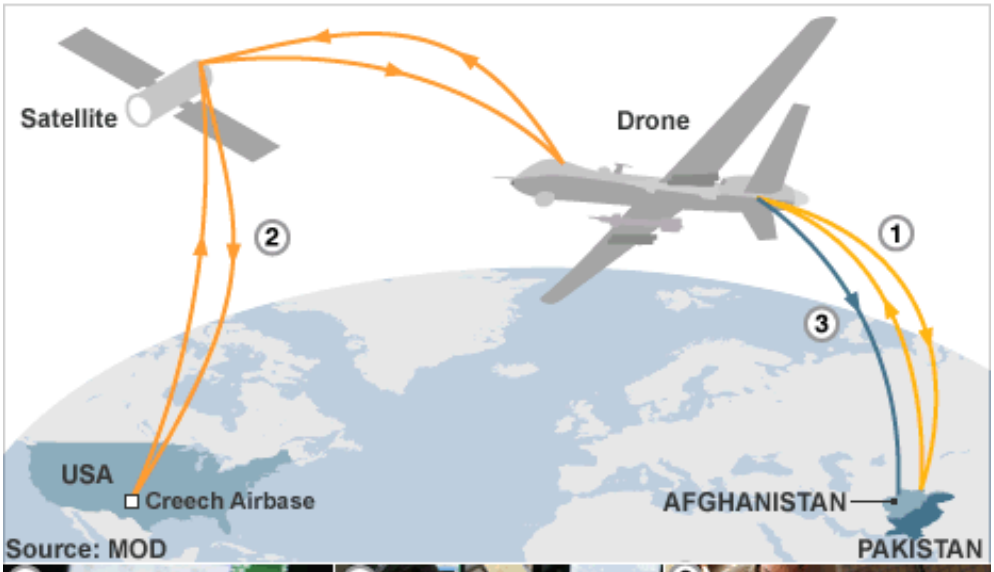
1. Encrypted GPS signal is jammed.
2. Navigation system fails over to an unencrypted civil GPS.
3. Authentic GPS signal is overpowered.
4. UAV is under the control of a malicious attacker.

Mitigations

M1: Include a redundant navigation system that is not reliant on GPS
M2: Ensure that navigation system does not fail over to an unencrypted civil GPS when jammed

Additional background information to show communication links

How drones work



Drone take-off and landing controlled locally

Drone flown remotely from US airbase

Images relayed to troops on the ground

References

Alexander, I. "Misuse cases: use cases with hostile intent," in IEEE Software, vol. 20, no. 1, pp. 58-66, Jan.-Feb. 2003, doi: 10.1109/MS.2003.1159030.

Common Weakness Enumerations https://cwe.mitre.org/

Common Attack Pattern Enumeration and Classification https://capec.mitre.org/

Humphreys, Todd. *Statement on the Vulnerability of Civil Unmanned Aerial Vehicles and Other Systems to Civil GPS Spoofing*. http://homeland.house.gov/sites/homeland.house.gov/files/Testimony-Humphreys.pdf (2012).

Nataliya Shevchenko, Timothy A. Chick, Paige O'Riordan, Tom Scanlon, Carol Woody, PhD, *Threat Modeling: A Summary of Available Methods*, August 2018, White Paper, HTTPS://RESOURCES.SEI.CMU.EDU/LIBRARY/ASSET-VIEW.CFM?ASSETID=524448

Tippenhauer, Nils O.; Pöpper, Christina; Rasmussen, Kasper B.; & Capkun, Srdjan. "On the Requirements for Successful GPS Spoofing Attacks," 75–85. *Proceedings of the ACM Conference on Computer and Communications Security (CCS*). Chicago, IL, Oct. 2011. ACM, 2011.