UAV CYBER SECURITY
INCOSE

Andy von Stauffenberg
Agenda

• VStar Systems Overview
• What is Cyber Security?
• UAV Overview
• Broad types of Cyber Attacks
• Remote Attacks
• Subsystem Attacks
• Suggestions
• References
About VStar

What we do?

VStar Systems Inc. is an unmanned systems integrator that creates innovative and effective solutions for Government and Commercial Clients.

Areas of Expertise

- Unmanned/Autonomous Vehicles
- Intelligence, Surveillance, Reconnaissance (ISR)
- Data/Communication Systems
- Command and Control (C2) Systems/Ground Stations
- Remote Sensing
- System of Systems/Distributed Systems
- Storytelling & Problem Solving
What is Cyber Security?

Definition:
Cyber security, also referred to as information technology security, focuses on protecting computers, networks, programs and data from unintended or unauthorized access, change or destruction.
Why UAV Cyber Security?

• They store a wide range of information from troop movements to environmental data and strategic operations.
• The amount and kind of information enclosed make UAVs an extremely interesting target for espionage and endangers UAVs of theft, manipulation and attacks.
• In the future, could (and will) be used for nefarious purposes.
UAV Overview

UAV’s are becoming very common – need to think about Cybersecurity NOW!!
UAV System Overview

UAV
- Power
- Propulsion
- Comms
- Main Processing
- GNC
- Flight Control
- Payloads

GS
- Processing
- User Interfaces
- Comms
- Data Storage

VSTAR SYSTEMS INC.
sUAV System Architecture

- Battery
- Power Distribution
- IMU
- Main Controller
- Transceiver
- Payload
  - SSD
  - Servo
  - Video Xmitter
  - Sensor
- ESC
- Motor
- GPS
- Gyro
- MM
- ADS-B
- Actuators
- GPS
- Boot Loader
- Reset
- Manual Flight Control
- Main Program
- Processor
- Power System
- Ground Station Comm
- UAV Wireless Comm
- Magnetometer
- Airspeed/Acc

Diagram showing the system architecture with various components and their connections.
General Attacks

• Remote Attack (Wireless Attack or Sensor Jamming/Spoofing)
  – Attack through one of the sensor or comms channels
  – Easy, but single system infiltration

• Hardware Attack
  – Access to components directly
  – Harder to accomplish, but effect greater
Specific Attacks

1. Payload/C2 Data Attack
   • “Stealing” Sensor Data

2. Direct Payload Attack
   • Temporary or Permanent damage to Payload

3. Control System Attack
   • Attacking the Control System SW or HW

4. Application Logic Attack
   • Altering data to the Control System
Remote Attacks
Payload/C2 Data Attacks

---

**Diagram Details:**

- **Battery**
- **IMU**
- **Main Controller**
- **Power Distribution**
- **GPS**
- **Gyro**
- **MM**
- **Transceiver**
- **ESC**
- **Mot**
- **Xmitter**
- **Controller**
- **Environment**
  - **ADS-B**
  - **L1/L2**
  - **GPS**
  - **Gyro**
  - **MM**
  - **ADS-B**
- **Payload**
  - **SSD**
  - **Servo**
  - **Video**
  - **Sensor**
- **Video Receiver**
- **Target**

---

**Communication Frequencies:**

- 2.4 GHz / 5.8 GHz
UAV Comms Architecture

Difficult because different comms paths have different owners/stakeholders
Payload/C2 Data Attacks

• Prevalent type of Attack – very easy to do

• Gaining Access to the Datastream in order to get “free” intelligence
  – Most streams poorly, or not at all encrypted

• Reports of wide range of U.S. UAV’s hacked by Iraqi Insurgents
  – Rovers widely used – Video Streams intercepted or jammed

• Typically “annoying”, but could also reveal critical intelligence
Direct Payload Attack

• Bit more difficult, but could seriously interrupt operations

• Disrupting or destroying the Payload

• EO/IR Cameras, SIGINT/EW Systems, etc.
Subsystem Attacks
UAV Subsystem Attacks

• Difficult to do, but great impact if accomplished.

• Control System Attack
  – Prevent H/W or CPU from behaving as programmed.
    • Buffer Overflow Exploits
    • Forced Resets to load malicious code
    • H/W Changes or additions

• Application Logic Attack
  – Manipulation of sensors or the environment to provide false data.
    • Sensor Data Manipulation
    • Vehicle/Component State Manipulation
    • Nav Data Manipulation
    • C2 data communication
Example of Attacks

4 December 2011 - RQ-170 Sentinel downed by Iran

Accomplished through GPS Spoofing (according to Iran)
System Attack Scenarios
Gain Schedule Attack
Actuator/Sensor Attack
GPS Attack
ADS-B Attack
Update Rate Attack
What to do about it?

• Keeping up with new Security Standards!
• Trusted Vendors
• Strong Quality Assurance Standards/Testing
• Strong Encryption
• Redundant subsystems
• Specific systems to counter external attacks
  – Receiver Autonomous Integrity Monitoring (RAIM)

UAV Cybersecurity is gaining traction – high costs associated!
BUT – Systems Engineering MUST think about it
References

• FAA Unmanned Aircraft Systems (UAS) Cyber Security Initiatives
  – Stephen George, FAA Airworthiness Manager

• Cyber Attack Vulnerabilities Analysis for Unmanned Aerial Vehicles
  – Ian Kim, Brandon Wampler, James Goppert, Inseok Hwang

• The Vulnerability of UAVs to Cyber Attacks – An Approach to the Risk Assessment
  – Kim Hartmann, Christopher Steup

• A Study on Unmanned Vehicles and Cyber Security
  – Emy Rivera, Robert Baykov, Guofei Gu
END TO END UNMANNED AND ROBOTIC SYSTEMS INTEGRATION