Cyber-Security of UAVs

BY: NATHANIEL HAMILTON

Acknowledgements

- I borrowed heavily from Andy von Stauffenberg's presentation UAV Cyber Security INCOSE with VSTAR Systems Inc. His original presentation can be found at http://www.sdincose.org/wp-content/uploads/2017/03/UAV-Cybersecurity.pdf

Agenda

- UAV Overview
- Types of Attacks
- Remote Attacks
- Hardware Attacks
- Current Prevention
- Questions?

UAV Overview

What is a UAV?

- UAV stands for Unmanned Aerial Vehicle
  - i.e. an aircraft without a human pilot onboard

http://insideunmannedsystems.com/air-force-replacing-rq-1-predator-remotely-piloted-aircraft/

https://newatlas.com/dji-phantom4-pro-v20-upgrade/54559/

https://atlasleisure.org.uk/clubs-socs/btrmac/

http://www.skymasterjets.net/index2.htm

Who uses UAVs?

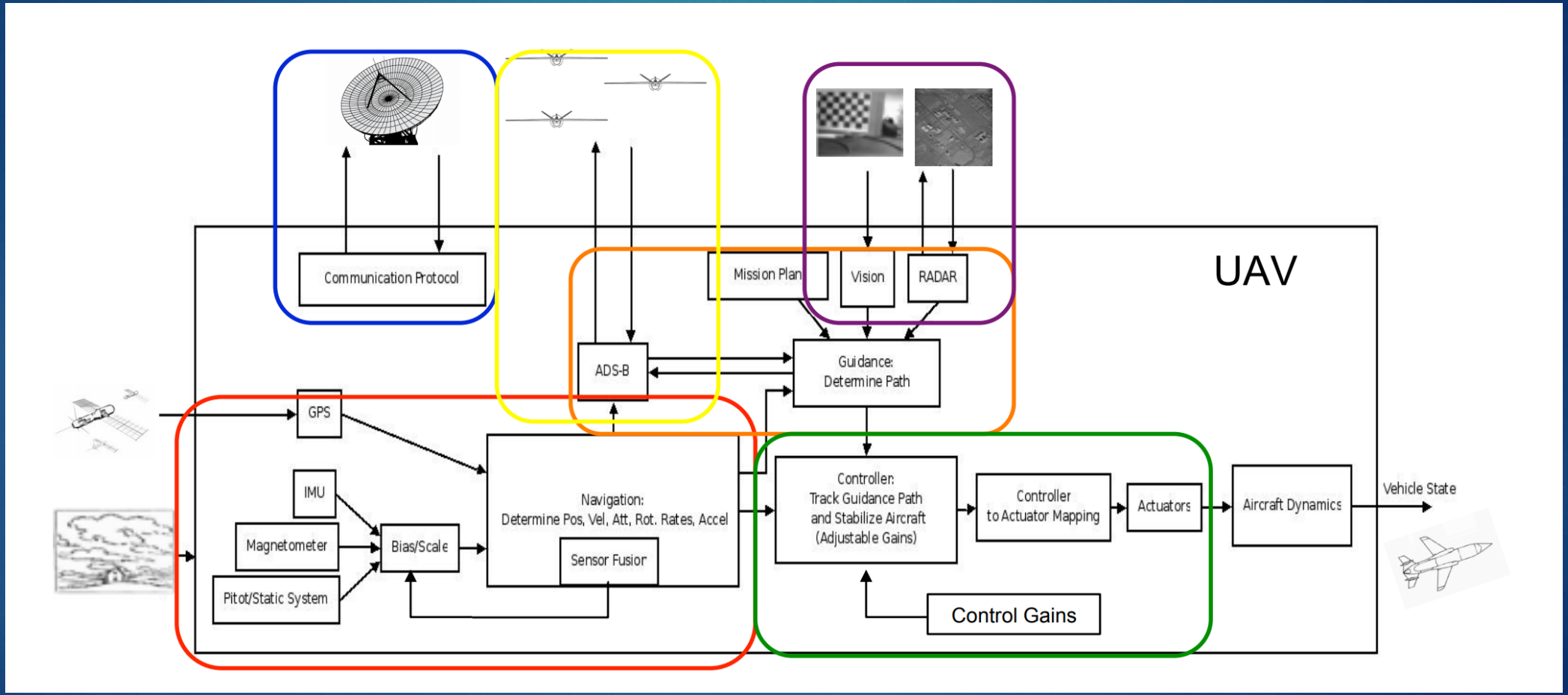
- The Government
- Emergency Responders
- Agriculture, Forestry, and Aquaculture
- Entertainment
  - Filmography and photography
- Hobbyists
  - If you are interested in becoming a hobbyist, I recommend joining the Academy of Model Aeronautics (http://www.modelaircraft.org/)

Why is Cyber-Security of UAVs Important?

- When is Cyber-Security not important?
- In the Government, they use drones to store a wide range of information ranging from troop movements to environmental data, to strategic operation.
- This makes them a target for theft and manipulation.
- UAVs can also be very expensive and some exploits can be used to takeover and/or destroy them.

Why is Cyber-Security of UAVs Important?

UAV System Architecture



https://pdfs.semanticscholar.org/1a95/4775dd9a2596b7543af7693d70741 5077289.pdf

Types of Attacks

General Attacks

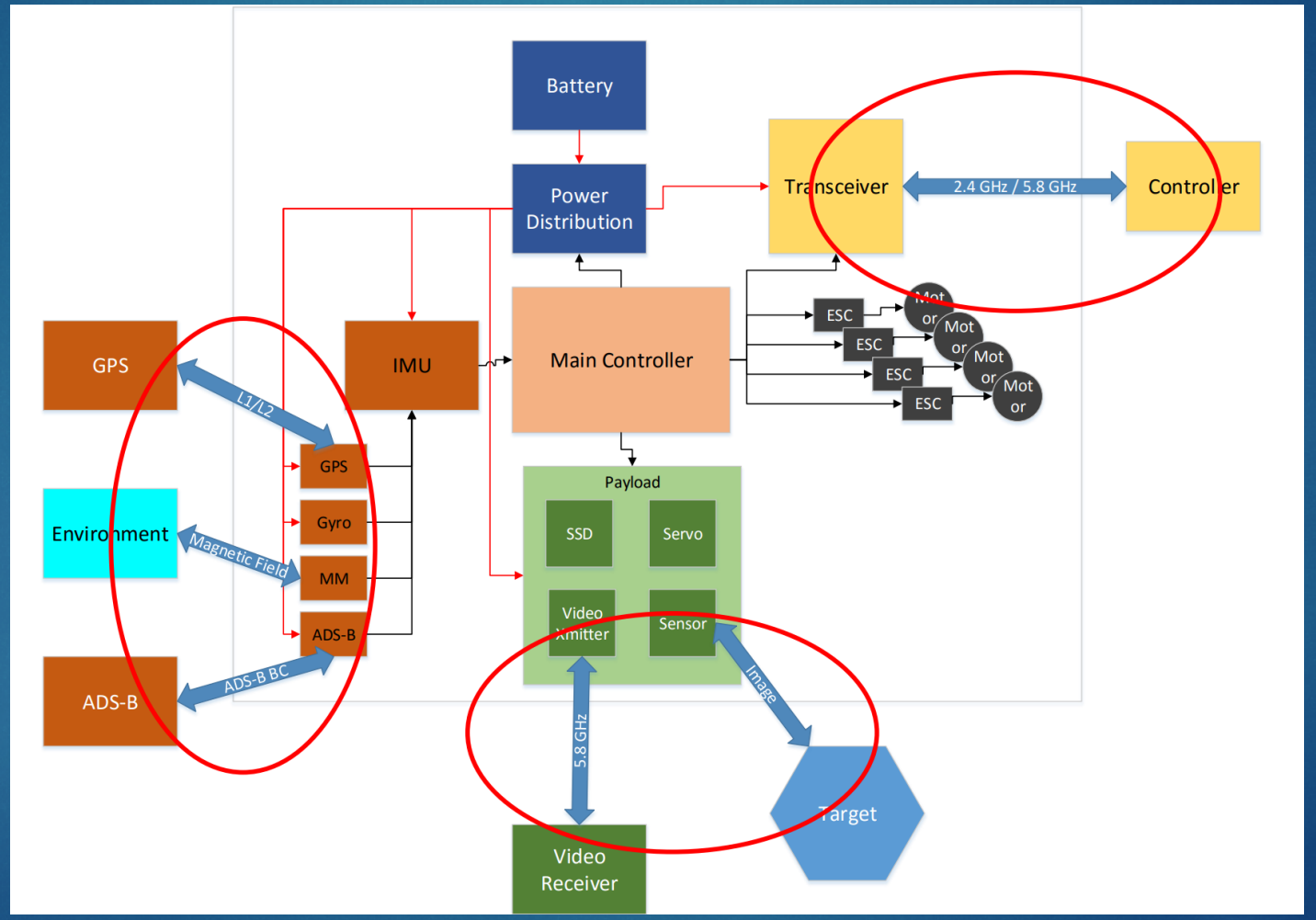
- Remote Attack (A.K.A. Wireless Attack or Sensor Jamming/Spoofing)
  - Via
    - Sensor manipulation
    - Communication channel interruption or recording
  - Easy to do, but only affects one UAV at a time
- Hardware/Subsystem Attack
  - Access components directly
  - Harder to do, but more severe consequences

Specific Attacks

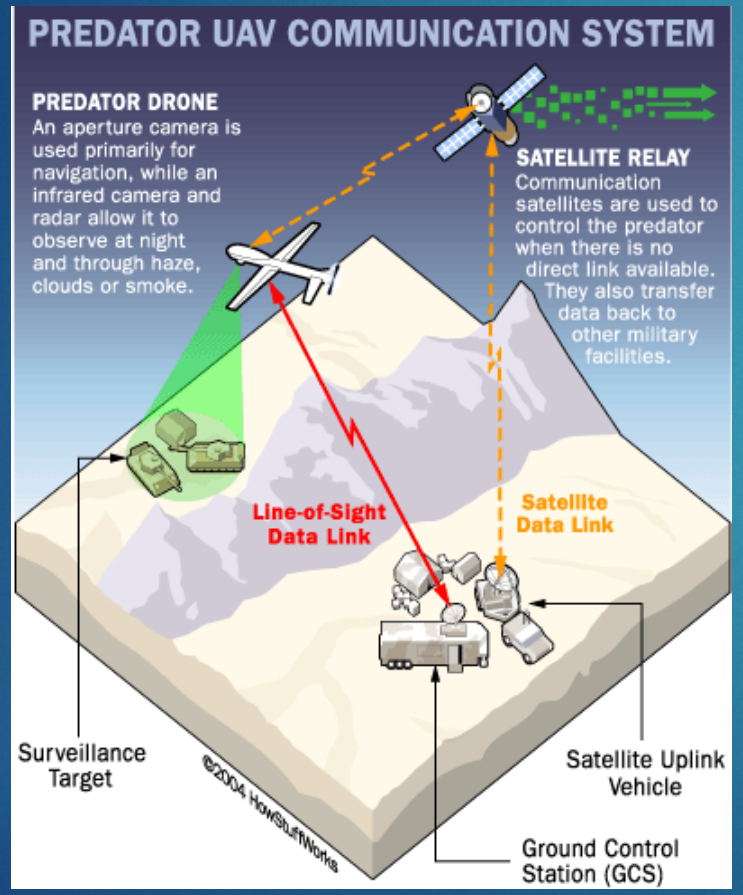
- Payload/Remote Control Data Attack
  - i.e. Stealing sensor data
  - High likelihood, but low severity
- Direct Payload Attack
  - Damage is done to the payload
  - High likelihood and high severity
- Control System Attack
  - Not likely to occur do to the difficulty, but would cause catastrophic problems
- Application Logic Attack
  - Altering the data being fed to the control system

Remote Attacks

External Interfaces



Communications Architecture



https://science.howstuffworks.com/predator6.htm

- How the Predator drone's communications system works is roughly similar to how most UAV communication systems work
- Predator is more sophisticated and expensive with a couple extra redundancies
- There is a ground station with some control over the drone and info is sent between the 2

Payload/Remote Control Data Attacks

- Prevalent and easy to do type of attack
- Involves gaining access to the data stream to get "free" intelligence
  - Exploits the lack of encryption on these data streams
- Typically "annoying", but could be used to reveal critical and/or private information

Insurgents Hack U.S. Drones

- This event is from 2009
- Originally reported on by the Wall Street Journal but I can't get that video, so here is CBS News on it
- https://www.youtube.com/watch?v=uFK0bdBjgwM

Direct Payload Attacks

- This is more difficult, but can cause serious problems
- Can disrupt or destroy the payload
- The payload can be things like a camera for recording information or weapons
- It could be possible to launch a missile at the command center instead of the intended target
- Luckily, there are no reported cases of this happening

Hardware Attacks

Hardware/ Subsystem Attacks

- More difficult to accomplish but more dangerous if successful
- Control System Attack
  - Prevent the control system from behaving as programmed.
    - Buffer overflow exploits
    - Forced resets
- Application Logic Attack
  - Manipulation of sensors or environment providing false data.
    - Sensor manipulation
    - State manipulation
    - Navigation data manipulation
    - Control data manipulation

Application Logic Attacks

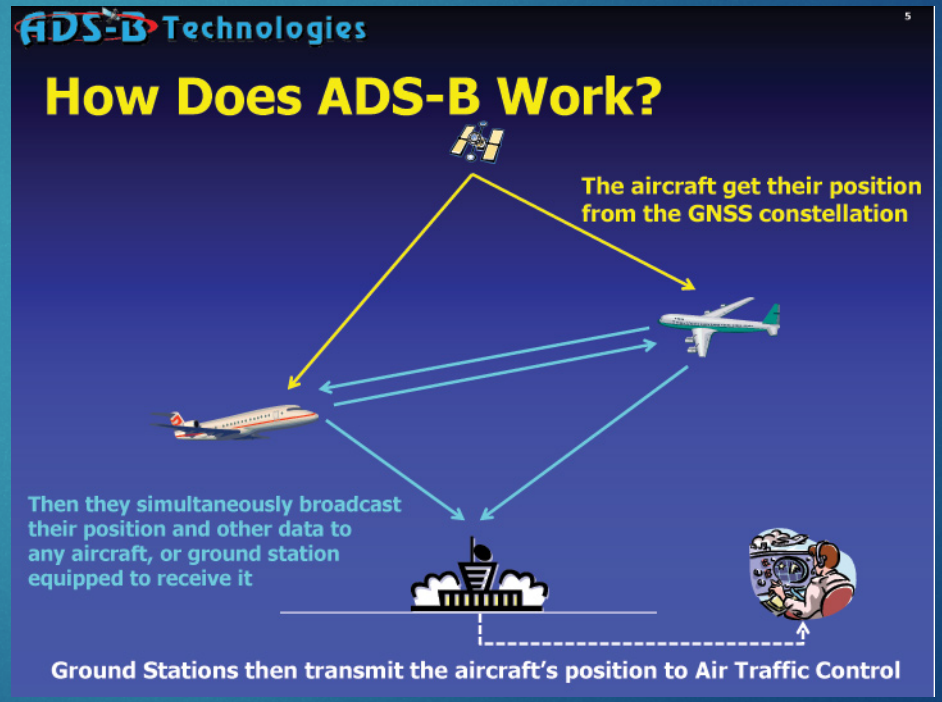
- This is becoming much more prevalent with things like GPS spoofing, control takeover, and falsified ADS-B reports
- I have videos about the first 2 in the next slides, but ADS-B examples are harder to find
- And what is ADS-B?

ADS-B

- Automatic – It's always ON and requires no operator intervention
- Dependent – It depends on an accurate Global Navigation Satellite System signal for position data
- Surveillance – It provides "Radar-like" surveillance services, much like RADAR
- Broadcast – It continuously broadcasts aircraft position and other data to any aircraft, or ground station equipped to receive ADS-B

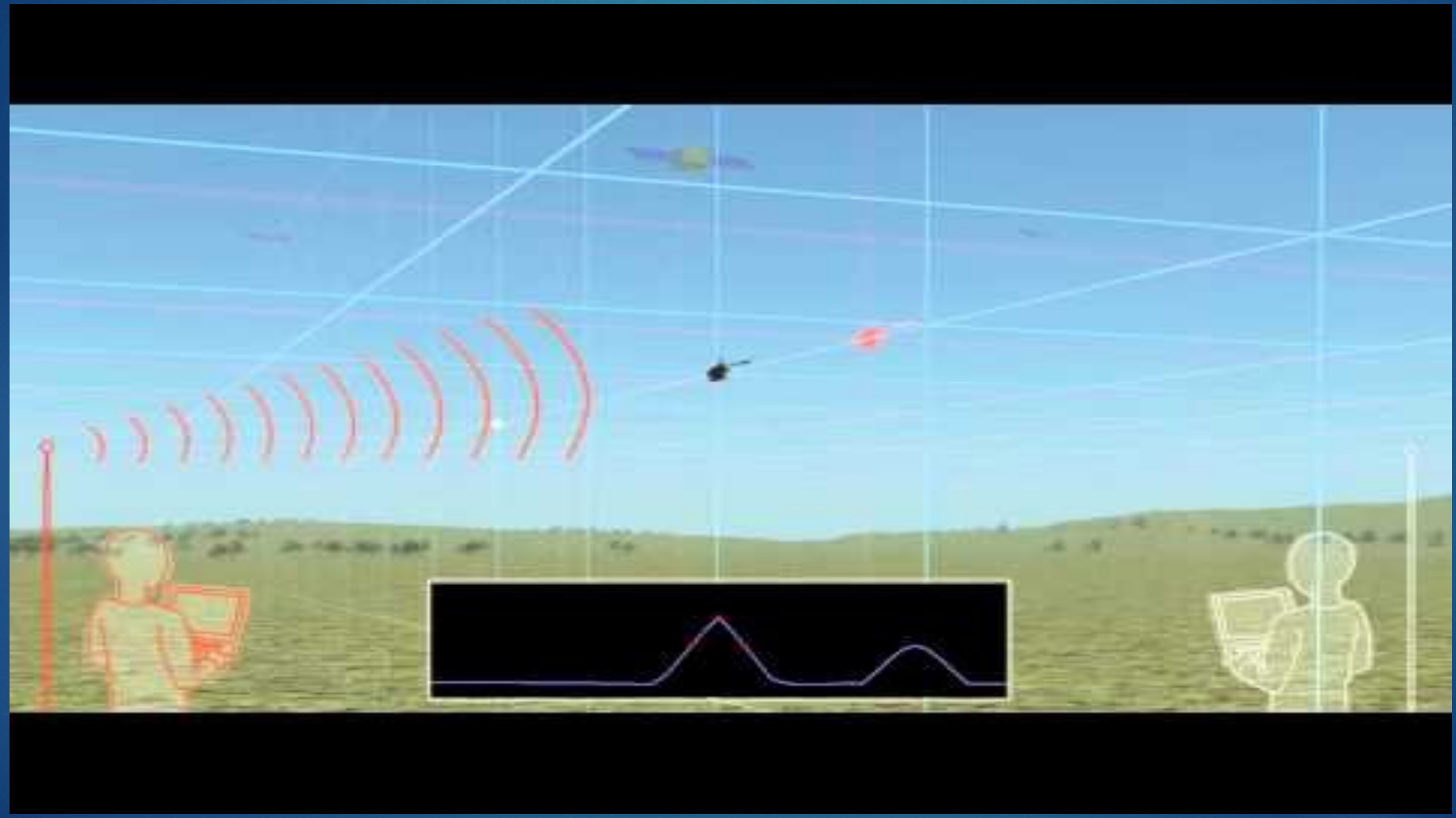
ADS-B

- The device gives the UAV a sense of who else is around it
- Used for aircraft avoidance
- According to [Rivera, Emy et al] it is "a device that every flying device will soon be equipped with"

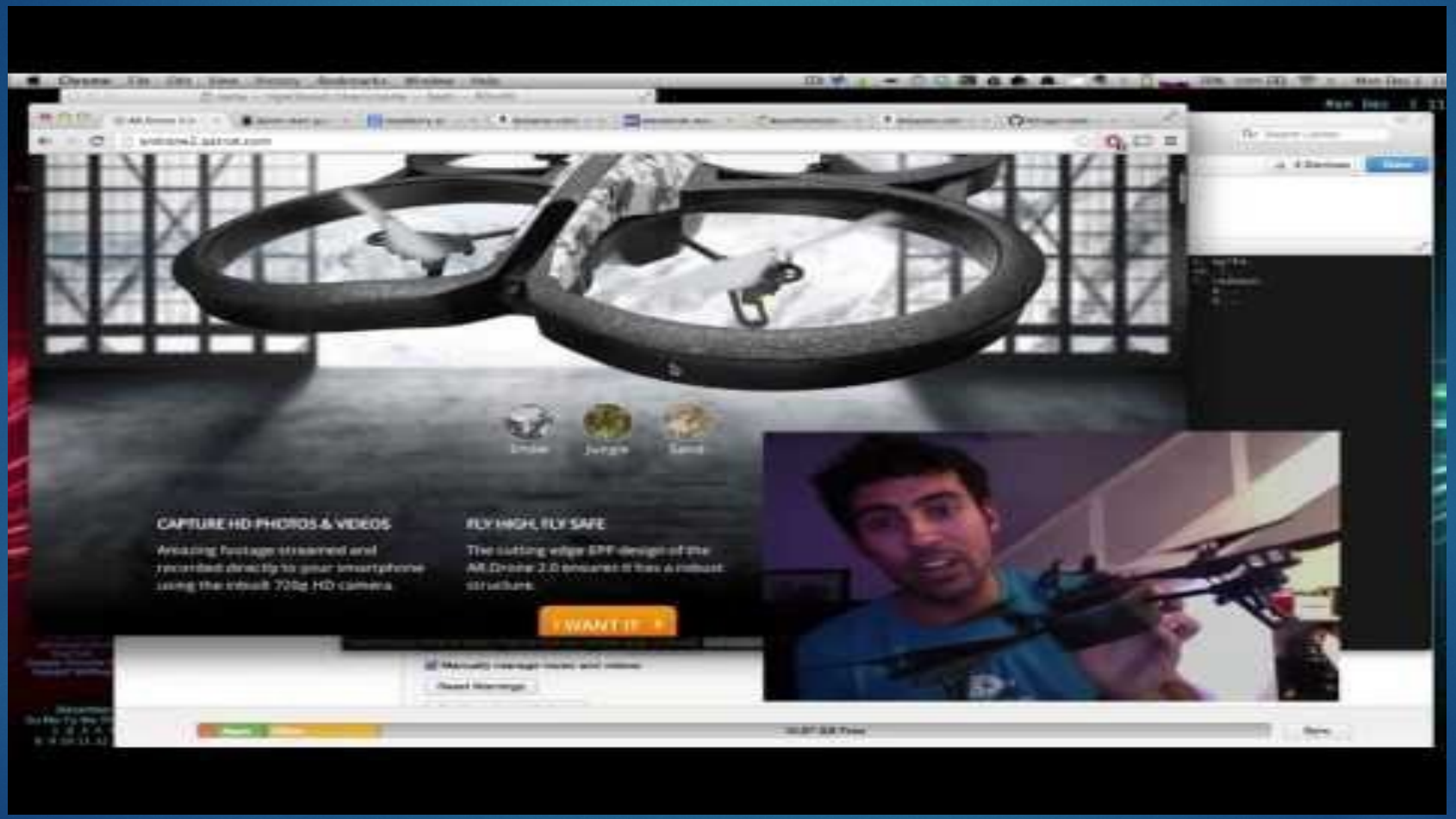


http://www.ads-b.com/

GPS Spoofing



SkyJack Software for Control Takeover



Current Prevention

Current Prevention

- Keeping up with security standards
- Only using trusted vendors
- Strong encryption
  - Many groups are arguing for civilian GPS encryption, but that would be very expensive to implement
  - Video, at the very least, should be encrypted
- Redundant subsystems
- Specific systems that counter external attacks
  - Receiver Autonomous Integrity Monitoring (RAIM)
  - Others being worked on here at ISIS and more can be found in this paper [https://onlinelibrary.wiley.com/doi/full/10.1002/rob.21513]

Questions?

References

- Gorman, Siobhan, et al. "Insurgents Hack U.S. Drones." *The Wall Street Journal*, Dow Jones & Company, 18 Dec. 2009, www.wsj.com/articles/SB126102247889095011.
- Hartmann, Kim & Steup, Christoph. "The Vulnerability of UAVs to Cyber Attack – An Approach to the Risk Assessment." Ccdcoe.org, https://ccdcoe.org/publications/2013proceedings/d3r2s2_hartmann.pdf.
- Kim, Alan et al. "Cyber Attack Vulnerabilities Analysis for Unmanned Aerial Vehicles." *Infotech@Aerospace* (2012), https://pdfs.semanticscholar.org/1a95/4775dd9a2596b7543af7693d707415077289.pdf.
- Rivera, Emy et al. "A Study On Unmanned Vehicles and Cyber Security." (2014), https://pdfs.semanticscholar.org/521c/2dd41bd7de10cb514f4e9d537fd434699cb7.pdf.
- Von Stauffenberg, Andy. "UAV CYBER SECURITY INCOSE." *Sdincose.org*, www.sdincose.org/wp-content/uploads/2017/03/UAV-Cybersecurity.pdf.

fin.