

RQ-170 Drone Hacking

Chris Wozny

CS466: Computer Security

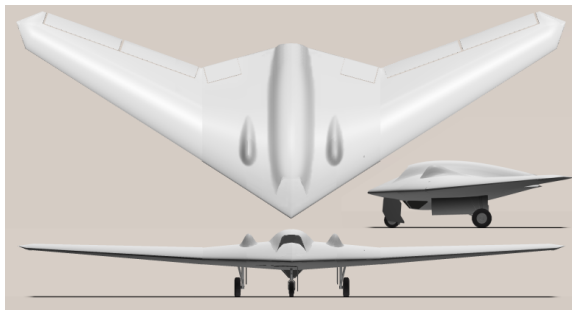
January 25, 2012

Introduction

From DailyTech article "Iran: Yes We Hacked the Drone and Here's How We Did It"



What is it?



- Produced by Lockheed Martin's Skunk Works
- High-altitude reconnaissance unmanned aerial vehicle
- Designated replacement for U-2 program
- Utilized in Afghanistan, Pakistan, and Iran

What was it doing there?

- High altitude weather research...

What was it doing there?

- High altitude weather research... (i.e. gathering intel on Iran's nuclear program)

Why is it interesting?

- "Stealthy" characteristics
- Cutting-edge technology
- The UAV that provided support in Operation Neptune Spear

Communications

- Loss of communication with ground station forces most drones into **back-to-base** mode
- Iranian Army's Electronic Warfare Unit capitalized on this by utilizing **radio jamming**

Radio Jamming

- A transmitter tuned to the same frequency as the opponents' receiving equipment and with the same type of modulation can, with enough power, override any signal at the receiver
- Makes receiver think that actual signal is just background noise by reducing **signal-to-noise ratio**
- Most decent receivers know when they're being jammed due to spike in amplitude of signal and will not accept the new signal as valid

Global Positioning System

- GPS satellites send information to unit which then determine location (courtesy of Einstein's relativity and time dilation)
- Iranian Army's Electronic Warfare Unit **spoofed** the GPS feed making the plane think it was close to Kandahar AB
- Iranian's couldn't find "perfect" match for landing strip so they made the UAV land at a slightly higher altitude (and caused damage)

Sanity Check & Dead Reckoning

- Verify that change in location is possible (i.e. the aircraft didn't just travel 500 miles in less than a second)
- Store the path that the UAV took and if it gets jammed use that route to go back to base

- President Barack Obama submitted a formal request to Iran to return the captured RQ-170

- President Barack Obama submitted a formal request to Iran to return the captured RQ-170
- Iranian defense minister Brigadier General Ahmad Vahidi asserted "the downed spy drone is now Iran's property, and our country will decide what steps to take about it."

This is what Iran sent to the White House:

This is what Iran sent to the White House:

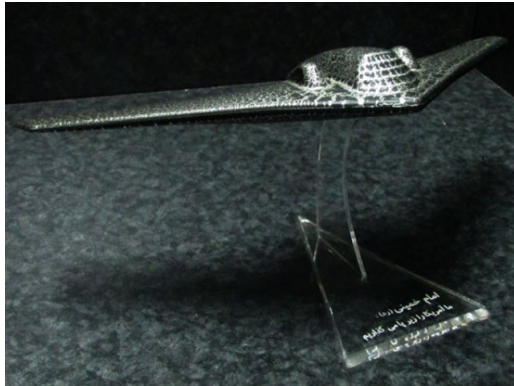


Figure: Inscription reads "We will put America under our feet"

Questions

- Should we have sent in a team to destroy the drone?
- Should we be using spy planes to overfly hostile territory?
- Why didn't the engineers foresee this hack?