CIS 700/002 : Special Topics : CPS Attacks on Vehicles

Bipeen Acharya
CIS 700/002: Security of EMBS/CPS/IoT
Department of Computer and Information Science
School of Engineering and Applied Science
University of Pennsylvania

2017-01-20

Attacks: Past and Present

- Past
  - –Limited to war driving, war-flying
- Today
  - –Attractive targets for cyber attacks
    - for the size, some of the most complex and difficult to secure CPS
    - rely on impressive number and range of on-board computers, sensors and communication systems.

Unmanned Aerial Vehicles

- Applications in archaeology, policing, wildfire detection, film making etc.
- operate in hostile environments
- surveillance
- transporting supplies

Accidents

- Fire Scout (2010)
  - autopilot malfunctioning
- US Air Force found them most accident-prone (129 accidents between 1997 and 2012)

Communication

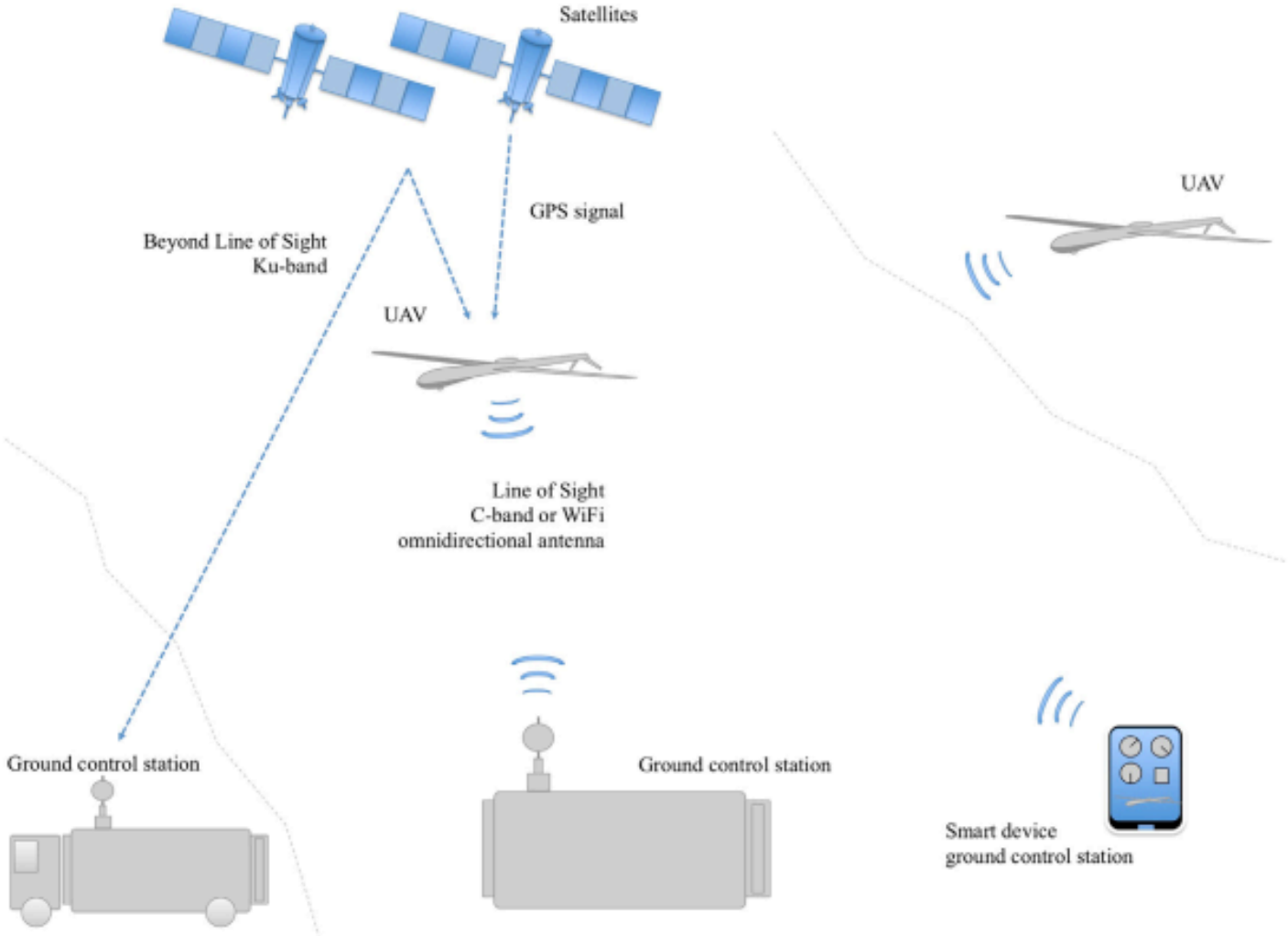

Figure 3.3 Some of the different types of communication involved in the operation of an unmanned aerial system. The example shows two UAVs that are able to communicate with each other, as well as three different ground control stations.

Communication

- Satellite communication for GPS geolocation and navigation.
- Civilian aircraft rely on civilian GPS signals
- Military aircraft rely on military GPS signals (protected with encryption and resistant to interference)

Group communication

- UAVs form a network
- Extend communication range
- Complete group missions
- Requires additional wireless communication link

CPS Attack on UAVs

- Theoretically straightforward:
  - Disruption of communications
  - Interception of communications
  - Feeding false data
- Practically, not so
  - but feasible

Interference with signals

- Widely employed to disrupt communications, radio broadcasting, missiles (World War II)
  - Adversary transmits random noise at the correct frequency
  - Jam communication with ground control station
  - GPS signals are very weak and vulnerable to jamming

GPS Spoofing

- Generating fraudulent signals (via GPS simulator)
- UT Austin and Northrop Grumman
  - Custom made device that combined GPS spoofer and GPS receiver
  - Receiver receives authentic signals and spoofer generates fraudulent but similar signals
  - Increase power slowly and control

GPS meaconing

- Rebroadcast legitimate data with a slight delay
- Distance from satellite is estimated based on the time it takes for signal to arrive.
- A delay of microseconds could cause large errors.

Middle of the Earth

- Fake signal reports a position in the middle of the earth (value of 0 for one spatial axis)
- GPS receiver unable to process (presumably due to division by 0)
- Infinite reboots!

Attacks on UAV networks

- Rogue UAVs connect to enemy's network
- Smaller UAVs without enough computation power susceptible
- carry out jamming, man-in-the-middle

“SMART” UAVs

- UAVs run by smart handheld devices
- Flooding attacks exhaust battery
- Malware

Military UAVs

- Supply chain risks
  - infiltrate networks
  - vulnerabilities in design, implementation or production phase

Automobiles

- Mechanical parts replaced with software and electronic parts
- Vulnerabilities in software
- Intentional cyber-physical attacks

Electronic Control Unit (ECU)

- Basically a small computer
- Communicates with other ECUs
- Runs the sensors and actuators to which it is connected.
- ~70 ECUs in modern vehicles

Controller Area Network (CAN)

- Network for communication of ECUs
- Every node receives all information transmitted on the bus
- Low-speed and high-speed CAN
- Gateway exchanges messages
- All nodes share one communication medium
- Trusts all nodes are legitimate

CPS attacks through CAN

- Unencrypted communication
- Rogue ECUs generate spoofed messages
  - report fake readings
  - request unsafe actions
- All nodes receive all transmission
  - Replay

Fuzzing

- Bombarding network with random data
- Since CAN payloads are relatively small, eventually find valid data
- disable engine, lock individual brakes, prevent braking

Denial of Service

- Mess with CAN's priority system
- Rogue ECU blocks valid messages by sending its messages at higher priority

No Authentication

Figure 3.6 The structure of the standard CAN frame with up to 64 bits of data and 44 bits of overhead (identifier, error detecting code, etc.).

Wireless Attacks

- Tire Pressure Monitoring System (TPMS)
- Broadcast air pressure and temperature
- Eavesdrop on information
- Feed fake information
- Trigger warning light
- Affect Battery consumption

Telematics Unit

- OBD Dongles
- Information is made available to users through the internet
- Introduce malware in the form of updates
  - later, generate CAN messages and control car

Immobilization system

- Immobilizers: Anti-theft devices
- Through cryptography and a transponder in the key
  - Transponder transmits distinct identification
  - lately, also ensure that physical key contains secret key
  - very weak crypto
  - techniques to find secret key in less than 6 minutes

Smart Keys -- relay attack

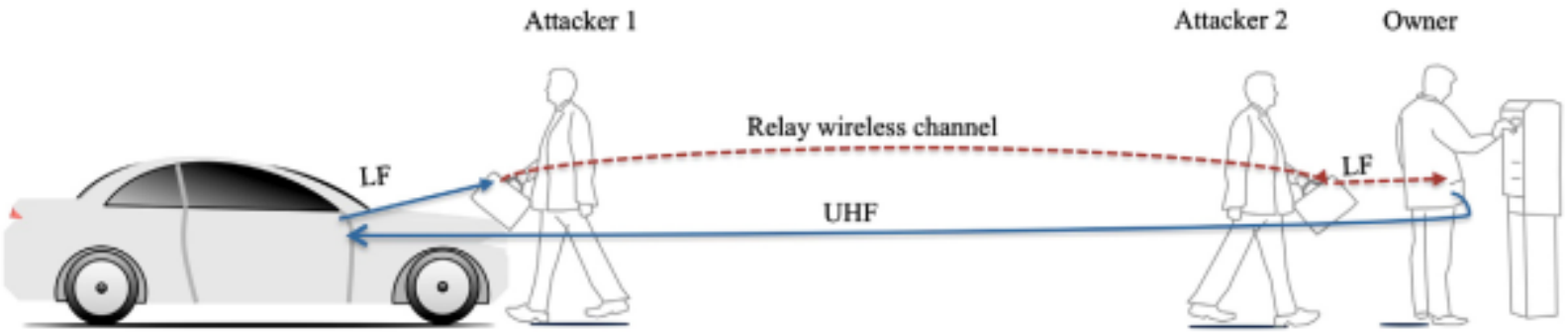

Figure 3.8 A pair of attackers activate the smart key and unlock the car's doors by relaying signals between the car and the smart key in the owner's pocket.

GPS jamming/spoofing

- Similar as to UAVs
- More prevalent when driverless cars become prevalent.

Radio Data System-Traffic Message Channel (RDS-TMC)

- Transmit traffic related messages to users
- supports lightweight cryptography
  - "to deter all but the most determined hacker"
- Barisani and Bianco, 2007
  - schematics of a custom RDS-TMC
  - generate fabricated events

Other attacks

- through ECUs that sit on both networks
- Miller and Valasek

Summary