Earth, Wind on Fire: Adversarial Analysis of Avionics & Terrestrial Hybrid Systems

Maxwell Bland, UIUC

Goals for this Presentation

- Discuss the differences in hacking avionics and terrestrial systems
- Highlight trends in terrestrial and avionics research, future directions

Definitions

Vehicle:

Material coordinating itself in space

Adversary:

Causal prior to an attack

Attack:

An alternative potentiality

Reasoning

Counter-argument:

Federal Information Processing Standards defines a threat as **access, misuse, disclosure, modification,** or **denial of service.**

Rebuttal:

This introduces an *interpretive perspective* on attacks rather than a *scientific perspective*.

Air vs Ground CPS (call AAA)

1. **Access:** different abstractions, similar materials
    a. RF, Software Update, more to come
    b. ARINC/ACARS vs OnStar, CD Player vs data-loader device

2. **Architecture:** similar formal qualities, different materials
    a. Internals of complex CPS are distributed systems
    b. Components of distributed system constructed differently, different software

3. **Attack:** Different navigational software, sensors, etc.
    a. As air/ground CPS become more specialized, they become less similar (intra and inter)
    b. Infrastructural environment only similar in trivial cases
    c. Computations, attacks run are different (false data injection, for example)

Disclaimer: These categories are only one signification! The real difference is **physical.**

An Introduction to the Problem

Image Source: amazon

Strawman Example: Parrot AR.Drone

1. Subject of Rani et al. [1] UAV security analysis.

2. Sensor differences in Ravi paper are abstracted away.

3. Paper hacks the broadcasted 802.11 network used to control the drone.

4. *No discussion* of attack after access. Just used aircrack-ng.

Quote from another researcher on avionics vs terrestrials:

"Is there any difference?"

Two Sides of this Talk

"119 studies (i.e. 86.2%) do not explicitly consider any communication aspect or imperfection" - Lun et al [src]

Compromise

- Methods of **access** and **architecture**
- Will ignore consumer electronics, as the access protocols are standard and architectures are well-known
- Will receive greater focus:
  - Access, architecture is the first step
  - Closer to my current area of research
  - Pragmatic: sophisticated attacks on differential equations unnecessary *(and specific to the vehicle!)*

Control

- Methods of **attack**, such as modifying sensor values
- Consumer electronics are fair game
  - May model more complex systems
- Less Focus
  - Material attacks are specific to the vehicle
  - Abstract attacks (such as modifying a dynamic feedback controller) require compromise
  - Control systems are built on an understanding of the network architecture (Schenato et al.)

Source: Car-and-Driver Magazine

Compromising Civilian Transports

Passenger Aircraft

Transport aircraft have more systems (ticketing, ATC, flight) than cars, buses.

Watkins, Crow et al. [2, 3] define *modular* and *federated* avionics systems.

Federated avionics is the most common system today.

Federated aircraft operate via several Line Replacable Units (LRUs)

- **Assumption:** no sensitive information
- **Assumption:** air-gapped from passenger wifi, bluetooth

LRUs for sale online: Communication Management Unit (CMU): $2,500.

Passenger Aircraft Adversarial Model

Assumption: Not taking over the cockpit mid-flight, using a bomb, etc.

Assumption: We care about hacking the vehicle, not other systems.

Crow et al. fails to mention interconnected systems:

- Pre-takeoff fueling carts (personal experience).
- ATC attacks: in 2015 LOT Polish Airlines forced to ground flights [4].

Terrestrials have interconnected systems, such as traffic lights (Ghena et al. [5])

Categories of attack: *in-movement* or *pre-movement*

Hacking a Passenger Aircraft Mid-Flight

RF links: Radio altimeter, VHF NAV, GNSS,
Automatic Dependent Surveillance Broadcast (ADS-B).

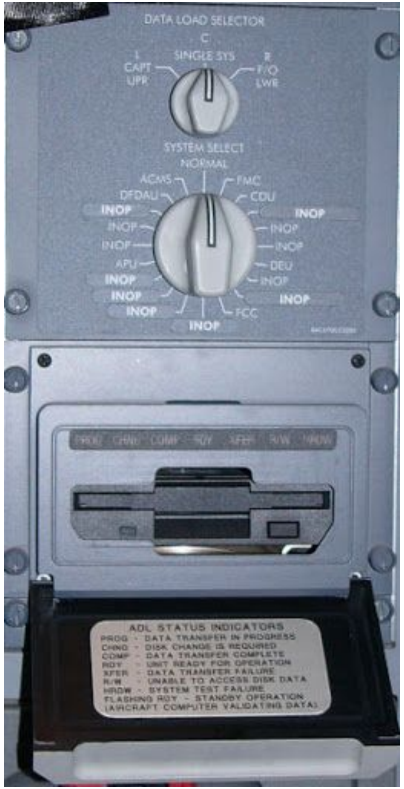
- **ACARS** forwarded from VHF receiver to CMU

Dataloader, Implant Attacks: Requires physical access.

- Cabinet on plane used to store LRUs, privileged access

ARINC: defines a set of standards for ACARS and bus comms for LRUs such as the Flight Management Computer

Sources: (Crow et al., Hauss et al.)


DATA LOAD SELECTOR
C
SINGLE SYS
L
CAPT
UPR
R
F/O
LWR
SYSTEM SELECT
NORMAL
ACMS
DFDAU
INOP
INOP
INOP
APU
INOP
INOP
INOP
INOP
FMC
CDU
INOP
INOP
INOP
DEU
INOP
INOP
FCC
PROG
CHNG
COMP
RDY
XFER
R/W
HRDW
ADL STATUS INDICATORS
PROG - DATA TRANSFER IN PROGRESS
CHNG - DISK CHANGE IS REQUIRED
COMP - DATA TRANSFER COMPLETE
RDY - UNIT READY FOR OPERATION
XFER - DATA TRANSFER FAILURE
R/W - UNABLE TO ACCESS DISK DATA
HRDW - SYSTEM TEST FAILURE
FLASHING RDY - STANDBY OPERATION
(AIRCRAFT COMPUTER VALIDATING DATA)

Source: b737.org.uk

Taking Down Passenger Aircraft Mid-Flight

LRUs run RTOS: Typically with several applications,

- Collins CMU900 runs Ready System's VRTX.
- *Privilege escalation, ACARS CFI violation!*

Manual overrides: *Adversary would still need to "fool" the human pilots.*

- Realistic attack scenarios understudied: future work.
- FMC based autopilot landing typically only used in foggy conditions

Common alternative, spoofing:

- Many, many papers. One example: spoof GNSS systems for UAVs [6].

A Remote Attack

- ACARS RF message -> CMU -> ARINC -> (optionally MCDU, etc) -> FMC

Similar to the Checkoway et al. comprehensive automotive attack paper [7]:

- aqLink -> ECU -> CAN bus -> other ECU or ECM

Differences:

Protocol used, computer used, attack then dependent upon software design, e.g. differential equations + automata model in hybrid systems (RE needed!) [8].

- *No short-range RF attack surface, unless you implant it!*

Passenger Cars

Sensitive information: market for *calibrations (.a2l files)!*

Long Range RF Links: From Checkoway et al.: GPS, Satellite Radio, Digital Radio, TMC, many others …

- But notable difference: several short range links, e.g. Bluetooth, RKE, TPMS!

Physical Attacks: CD Players, OBD-II …

- adversary model much less privileged

ALDL, CAN Bus: ECU communications (active community!)

Source: CBM

Taking Over a Passenger Car Mid-Drive

First notable difference from a passenger airplane:

“Where are the long-range spoofing attacks?”

Newer automobiles have few manual overrides (from experience).

- An attacker with control over the ECM can change fuel injection entirely

ECUs have their own operating systems and applications

- The primary ECM handles reading from sensor values, such as crankshaft position, adjusting timings based upon loaded calibration files

Sources: Contag et al. [9], Le et al. [10]

A Key Difference: Updates

From conversations with Boeing security team:

We can't really work with the code on the Collins CMU900: the support contract for that LRU expired.

Future direction: binary rewriting?

Meanwhile, August 2020:

"Tesla CEO Musk Trumpets Upcoming Suspension and Autopilot Upgrades" (source)

Alternative Adversary: The Manufacturer

Of course Boeing could take down an airplane, and Ford could crash a car.

This adversary model simply needs manufacturer **Motivation**.

Contag et al. [9] demonstrated Volkswagen *defeat devices.*

- ECM for Volkswagen contained logic to detect and adjust fuel injection during emissions test cycles

EPA has similar standards for commercial aircraft [11]

- *Aircraft are more expensive & complex to study!*

Source: afrc.af.mil

Compromising Military Transports

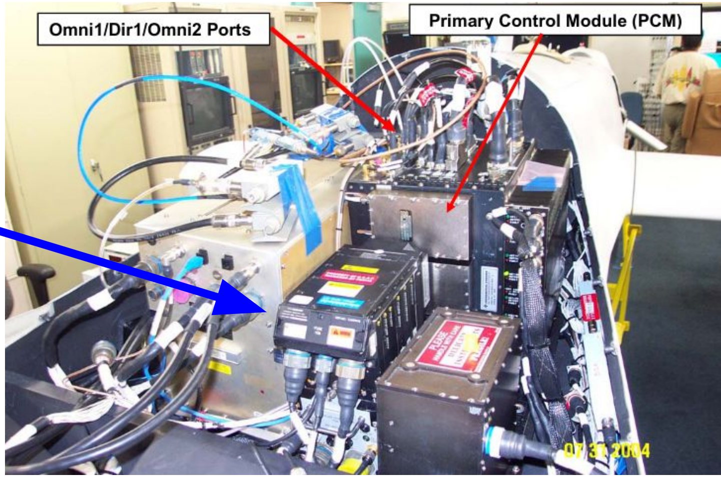
Attacking a MQ-1 Predator Drone

Control [dtic.mil, ukrainian armed forces]**:**

- C-band line-of-sight data link or a Ku-band satellite data link for beyond-line-of-sight operation
- AN/AAS-52 Multi-spectral Targeting System

ARC-210 Radio with SINCGARS:

- Anti-jamming, frequency hopping systems!
- Bus comms over MIL-STD-1553 data bus (The military version of ARINC 429!)



source

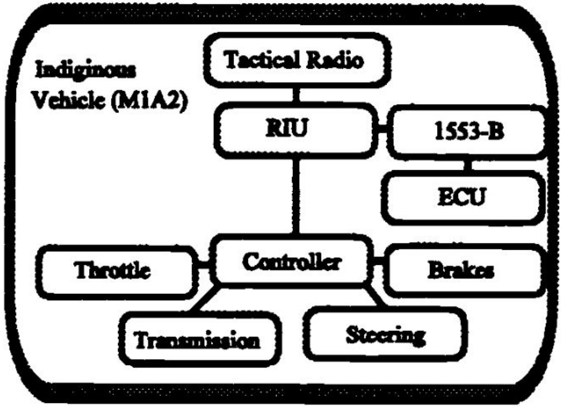
Attacking an M1 Abrams Tank

> *“Internal systems and components on the Abrams are integrated with the vetronics architecture” [dtic.mil]*

- Vetronics is a GE-headed technology that “now enables each warfighter and military asset to become a battlefield sensor” [ecrin systems]

Communications are standardized:

- VHF also handled via SINCGARS
- Also uses the MIL-STD 1553-B serial bus standard



Source: [Vertrionics Technical Group]

A Different Adversary Model

Similarities:

- Anti-jamming, anti-spoofing capabilities
- Accessible via the same general VHF systems (SINCGARS)
- Attack goals: leak sensitive info, change position, change function
- Data bus protocols used!

Differences:

- Components, internal architecture

Feedback Control Systems

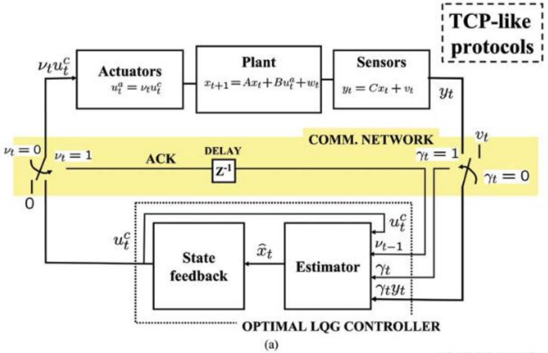
The Role Control Systems Play

Schenato et al. [12] was the first to acknowledge the interplay of networked systems in feedback control systems

- Also provides a good introduction to the problem

What is a feedback control system?

1. Environment is read through sensors
2. System state is estimated
3. Modifications are made to physical devices
4. The cycle repeats



Source: Schenato et al.

Clearly **similar** between autopilot in airplanes, fuel injection in cars.

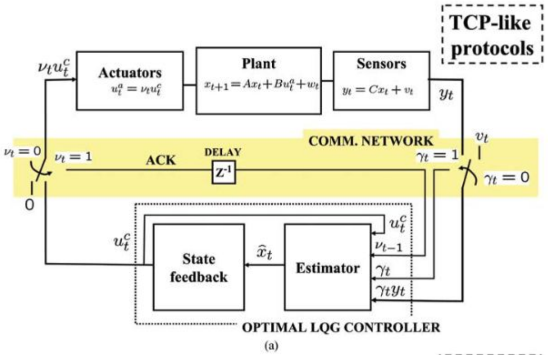
The Role Control Systems Play

Schenato et al. [12] was the first to acknowledge the interplay of networked systems in feedback control systems

- Also provides a good introduction to the problem

What is a feedback control system?

1. Environment is read through sensors
2. System state is estimated
3. Modifications are made to physical devices
4. The cycle repeats



Source: Schenato et al.

Clearly **similar** between autopilot in airplanes, fuel injection in cars.

PIDs, IMUs, Control Loops

Many, many papers on defenses and attacks against control loops.

Attack structure (but not the math) are shared between avionics and terrestrials

Any portion of the control loop is at risk

- Sensors get spoofed
- State estimation equations may be fallible (FDI attacks)
- Actuators may be turned off
- You can shoot missiles at the vehicle (plant).

Need to know the details of the system being used:

PID: Proportional-integral-derivative, IMU: Inertial Measurement Unit, etc.

Avionics Control Systems

Attitude (Roll, Pitch, Yaw), an Example

Me et al (2019) [13] surveys the defenses against quadrotor UAVs

- State estimation requires estimation of nonlinear, complex dynamics
  - Potential for FDI attacks

Large amounts of noise present in certain parts of the system (generalized FDI!)

- E.g. position estimates of accelerometers in IMU require double integration

Defenses include:

- Systems defenses (encryption, etc.)
- Non-linear control techniques for state regularization
- Intelligent control systems (ANNs) for detecting deviations

Terrestrial Control Systems

Main Terrestrial Difference: Dynamics

“Traditionally developed rigorous mathematical theories ... are mostly based on static or low-mobility environment assumptions” (Liang et al [14])

I.e. you can go from a highway environment to a downtown environment

- Stability-based control techniques must account for rapid state change
- Example: Zeng et al 2018 [15], road segments in downtown areas used to attack GPS navigation
- Shen et al. 2020 [16] use noise from multiple sensor fusion to identify points at which attacks will occur

The Future

We still aren't there yet.

For example, "precision agriculture", automatic drone-based analysis of crops [16] is an active area of research.

As more complex control systems emerge, so will attacks and defenses.

We can't even secure multiple sensor fusion!

We can leverage cutting-edge techniques in cryptography, AI, the whole of computer science, but let me end with some mythology …

Daedalus, Wayland, and von Braun