Attacking Electric Motors For Fun and Profit

Matthew Jablonski
Duminda Wijesekera, Ph.D.
About Us

Matthew Jablonski
• Ph.D. Student in IT
• Engineer and penetration tester
• Safety and security of cyber-physical systems

Dr. Duminda Wijesekera
• Professor, CS
• 250+ Publications

RARE Lab
• Areas of Focus:
  • RF Off. and Def.
  • Cyber Physical Systems
  • Computer Vision
  • Risks in algorithms, HW/SW, etc.

• Collaborations:
  • Government
  • Transportation
  • Medical
  • Industrial
Abstract & Caveats

• Comprehensive technical evaluation of attack objectives and offensive strategies focused on electric motor (EM) systems

• Introducing the Motor Threat Model

• We do not:
  • target a specific product or endorse any products
  • follow safety warnings (but you should and we are not responsible for your actions)
Quick Overview

(Got to keep this presentation MOVING...)
Hypothetical Problem Scenario

• Your next risk assessment target:  
  A Proprietary Drone System

• Thousands deployed worldwide for package delivery
  • 30 different drone models were dev’ed
  • Hundreds of operators...
  • With physical and remote access...
  • And... background checks aren’t required.
  • Over the Internet.

• WHAT IS THE ATTACK SURFACE?
  (and we need your response NOW!)
Safety First!

• Rules, Regulations, Standards
  • Designed to address **accidents**

• Protect against risks through:
  • Operational requirements
    • i.e. air traffic control
  • Power requirements
    • i.e. overcurrent, low voltage, etc.
  • System calibration requirements

• Security... Second?
  • What about **intentional threats**?
The First Security Problem...

• Possible nightmare scenario...
Unacceptable Security Recommendation

YEAH, BUT YOUR SCIENTISTS WERE SO
PREOCCUPIED WITH WHETHER OR NOT THEY COULD,

THEY DIDN’T STOP
TO THINK IF THEY SHOULD.
System Review: What’s Inside?

- **Brushless Motor**
- **Controller**
- **Mission Control (operator)**
- **Handheld Throttle (operator)**
- **Sensors:**
  - Accelerometers
  - Inertial measurement
  - Magnetic
  - Optical
  - GPS
- **4G LTE**
- **2.4GHz FHSS**
- **Linux; AI apps**
The Start: Find Similar Threat Models?
How do Electric Motors Work?

- Every motor connected to a **drive**
  - Embedded controller
  - ESC, VSD, VFB

- Voltage fluctuated at **pin** by HW switch
  - Current flows to motor when $V>0$
  - Pulse Width Modulation

- **Clock** and **duty cycle** controlled by HW & SW

![Diagram showing voltage levels and duty cycles](image-url)
How do Electric Motors Work?

- **Input**: electrical energy
- **Output**: torque, speed, mechanical energy

- **Rotor**: free-moving
- **Stator**: stationary

- **Many different types**:  
  - DC vs. AC power  
  - Rotary vs. linear  
  - Selection based on LOAD
How do Electric Motors Work?

Torque vs. Speed

- Stall Torque: $\tau_S$
- No-Load Speed: $\omega_N$
- Max Power: $P_{MAX}$
- Low Power Slope: $\tau = \tau_S - \omega \tau_S / \omega_N$
- Optimal Operation Zone
- Intermittent Duty Zone
- Continuous Duty Zone

Effects on Power Output

- Stall Torque: $\tau_S$
- Max Power: $P_{MAX}$
- $\tau_{NP} = 0.5 \tau_S$
- $\omega_{NP} = 0.5 \omega_N$
- $\omega_R$
- $\tau_R$
- $\omega_{NP}$
Control Theory: The Recipe for Digital Movement Control

Open loop systems:

Closed loop systems:
Another Security Problem...
Yet Another Security Problem...

Movement is continuous (usually)

Digital control requires discrete commands
Maybe Similar Threat Models?
Threat Modeling... Gaps...

• Let’s get away from drones.

• **Common issues:**
  - Cyber vs. physical attacks
  - Physical attack outcomes
  - Multiple control layers
  - Digital commands are discrete

• **Possible models?**
  - ICS Cyber Kill Chain (Stage 2) [1]
  - Mitre’s ICS ATT&CK Framework [2]

---

The Motor Threat Model (MTM)

Our proposed model:
The MTM Stack

• Simplified 7-layer stack

• Key takeaways:
  • Attacks at higher layers allow better control for attacker
  • Attacks at lower layers take control of movement from higher layers
  • Can understand access needed for C v. P attacks
High Level Attack Objectives

• Control
  • Steal control to achieve some goal
  • Cyber attacks
  • Easiest at layers 4-7

• Disrupt
  • Stop movement or prevent operational controls
  • Cyber or physical attacks
  • All layers

• Data Exfiltration
  • IP or privacy theft by tracking movement data
  • Cyber attacks
  • Easiest at layers 5-7
## Layer Descriptions

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Level 1 Access Description</th>
<th>Level 2 Access Description</th>
<th>Types of Attacks (C, P)*</th>
<th>Attack Objectives (C, D, DE)**</th>
</tr>
</thead>
<tbody>
<tr>
<td>7 - OPERATOR</td>
<td>Unprivileged motor control</td>
<td>Operator interface</td>
<td>OPERATOR-CONTROL channel</td>
<td>C, P</td>
<td>C, D, DE</td>
</tr>
<tr>
<td>5 - CONTROL</td>
<td>Root system control</td>
<td>System controller</td>
<td>CONTROL-DRIVE channel</td>
<td>C, P</td>
<td>C, D, DE</td>
</tr>
<tr>
<td>4 - DRIVE</td>
<td>Modify motor configuration</td>
<td>Motor drive controller</td>
<td>DRIVE-MOTOR channel</td>
<td>C, P</td>
<td>C, D</td>
</tr>
</tbody>
</table>

* Cyber (C) or Physical (P)  ** Control (C), Disrupt (D) or Data Exfiltration (DE)
## Layer Descriptions

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Level 1 Access Description</th>
<th>Level 2 Access Description</th>
<th>Types of Attacks (C, P)*</th>
<th>Attack Objectives (C, D, DE)**</th>
</tr>
</thead>
<tbody>
<tr>
<td>3 - POWER</td>
<td>Prevent or degrade movement</td>
<td>Power system access</td>
<td>N/A</td>
<td>C, P</td>
<td>D</td>
</tr>
<tr>
<td>2 - MOTOR</td>
<td>Source of mechanical movement</td>
<td>Motor physical access</td>
<td>N/A</td>
<td>C, P</td>
<td>D</td>
</tr>
<tr>
<td>1 - LOAD</td>
<td>Prevent movement by overload</td>
<td>Output LOAD access</td>
<td>N/A</td>
<td>P</td>
<td>D</td>
</tr>
</tbody>
</table>

* Cyber (C) or Physical (P)
** Control (C), Disrupt (D) or Data Exfiltration (DE)
OPERATOR Attack Ex. 1
Wireless Control

Example Target:

Controller

Operator

Forward
Reverse
OPERATOR Attack Ex. 1
Wireless Control

Results: Control and Disrupt
OPERATOR Attack Ex. 2
Remote Pin Control

Example Target:

- RPi Controller
- Raspbian
- pigpiod with Remote GPIO
- LiPO Battery
- ESC
- Brushed DC Motor
- Dynanometer

This physical setup is used in most attack examples, unless noted.
OPERATOR Attack Ex. 2
Remote Pin Control

**Fingerprint on network**

- Attacker has network access and observes remote GPIO
- Executes attack script: `PIGPIO_ADDR=192.168.1.4 python3 attack.py`

**Attack script**

```
from gpiozero import PWMOutputDevice
from time import import sleep

motor = PWMOutputDevice(18)
motor.frequency = 250

while True:
    motor.value = 0.3
    sleep(3)
    motor.value = 0.4
    sleep(3)
```
OPERATOR Attack Ex. 2
Remote Pin Control

Results:
Control and Disrupt

RPM vs. Time
SENSOR Attack: Accelerometer Data Injection

Example Target: ADXL345 accelerometer used to control servo angle
SENSOR Attack: Accelerometer Data Injection

- Capture and decode I2C, 6 bytes sent for X, Y, Z
- Connecting attack Pi – observe I2C address 0x53
SENSOR Attack:
Accelerometer Data Injection

• Set attack Pi as I2C slave
• Control bytes

Results:
Control and Disrupt
CONTROL Attack 1:
Timing Impacts of Discrete Command Injections on Motor Control

• Inject changes to duty cycle during operation

Results: Control and Disrupt; RPM vs. Time
CONTROL Attack 2: Hardware Implant Targeting PWM Channel

Example Target:
CONTROL Attack 2: Hardware Implant Targeting PWM Channel

- When PWM used as control signal, typically a 3-wire cable is used:
  - Black wire = ground
  - Red wire = current
  - White or yellow wire = control
CONTROL Attack 2: Hardware Implant Targeting PWM Channel

Results:

Control and Disrupt

RPM vs. Time
DRIVE Attacks: Pin Control and Configuration Attacks

• Attacks modify pin registers in Rpi 3 B+ SoC, Broadcom BCM2837
• Memory map physical memory locations using BCM2837 spec
DRIVE Attacks: Pin Control and Configuration Attacks

• Attack 1: Change pin to INPUT during operation

Results: Control and Disrupt

RPM vs. Time
DRIVE Attacks: Pin Control and Configuration Attacks

- Attack 2: Modify PWM CLOCK and DATA on BCM2837 to identify behavioral changes to motor
- Target:
DRIVE Attacks: Pin Control and Configuration Attacks

Results:

Control and Disrupt

DATA vs. CLOCK w/ Static RANGE
 DRIVE Attacks:
Pin Control and Configuration Attacks

• Attack 3: Record and playback PWM registers

Results:
Control and Disrupt

RPM vs. Time
POWER Attack: Motor Performance due to Low Voltage

• Test run with low voltage LiPO battery

Results:

Disrupt

RPM vs. Time

NOTE: LiPO batteries should never be used in low voltage (may overheat or worse)
POWER Attack:
Motor Performance due to Low Voltage

Results:

Disrupt

Torque and Power Output vs. Speed

NOTE: LiPO batteries should never be used in low voltage (may overheat or worse)
MOTOR Attack 1: Motor Performance in Presence of External Electromagnet

- Introduced electromagnet (500N suction) to target during run to observe behavior
MOTOR Attack 1: Motor Performance in Presence of External Electromagnet

Results:

*Disrupt*

RPM vs. Time
MOTOR Attack 1: Motor Performance in Presence of External Electromagnet

Results:

*Disrupt*

Torque and Power Output vs. Speed
MOTOR Attack 2:
Reprogramming Digital Servo Motor

- Digital servo manufacturers provide programming tools
- Identify motor type and procure programmer – no auth!
- Target and programmer:
MOTOR Attack 2: Reprogramming Digital Servo Motor

• Expected behavior (top, CW) vs. reprogrammed (bot, CCW):
LOAD Attack: Overheating and Stalling a Motor

• Target desk fan:
LOAD Attack: Overheating and Stalling a Motor

- Overheated to ~180°F and motor died at 61-min mark

Results: Disrupt
LOAD Attack: Overheating and Stalling a Motor

- Brushless motor comparison between dead and good fan
- No visual difference
Motor Threat Model Redux
Start Over: Hypothetical Problem Scenario

• Your next risk assessment target:
  A Proprietary Drone System

• Thousands deployed worldwide for package delivery
  • 30 different drone models were dev’ed
  • Hundreds of operators…
  • With physical and remote access…
  • And… background checks aren’t required.
  • Over the Internet.

• WHAT IS THE ATTACK SURFACE?
  (and we need your response NOW!)
Attacker Model for Drone System

• Nation State – C & P; Offensive campaigns directed at accomplishing some mission; Many resources

• Cybercriminal – C; Motivated by data collection

• Terrorist – C; Motivated by spreading fear

• Insider – C or P; Disgruntled employee or social engineering victim
Refined Attack Objectives for Targeting Drone Movement

• **Control** –
  • Steal property
  • Alter predictable movements

• **Disrupt** –
  • Physical damage
  • Physical harm
  • Prevent movement

• **Data Exfiltration** –
  • Privacy Invasion
Movement Focused Attack Trees

Control
- 7-OPERATOR
  - C
  - P
- 6-SENSOR
  - C
  - P
- 5-CONTROL
  - C
- 4-DRIVE
  - C*

Data Exfiltration
- 7-OPERATOR
  - C
- 6-SENSOR
  - C
- 5-CONTROL
  - C

Disruption
- 7-OPERATOR
  - C
  - P
- 6-SENSOR
  - C
  - P
- 5-CONTROL
  - C
  - P
- 4-DRIVE
  - C*
  - P
- 3-POWER
  - C*
  - P
- 2-MOTOR
  - C*
  - P
- 1-LOAD
  - P
MTM Application for Finding Movement Threats

Sensors: Accelerometers; inertial measurement; magnetic; optical; GPS;

Controller - Linux; AI apps

6-SENSOR

7-OPERATOR

2-MOTOR

4-DRIVE

DRIVE

2-MOTOR

4-DRIVE

Sensors: Accelerometers; inertial measurement; magnetic; optical; GPS;

Handheld Throttle (OPERATOR)

2.4GHz FHSS

Mission Control (OPERATOR)

4G LTE

Controller

3-POWER

1-LOAD

5-CONTROL

2-MOTOR

Brushless Motor

Brushless Motor

Brushless Motor

Brushless Motor

DRIVE

DRIVE

DRIVE

DRIVE
Experimental Boneyard
Thanks!
Backup Slides
The OPERATOR Layer

• *Unprivileged* motion control (most of the time)

• **2 levels of access:**
  1. Operator interface
  2. OPERATOR-CONTROL channel

• **Type:** cyber and physical

• **Objectives:** control, disrupt, data exfiltration
The SENSOR Layer

• Provides input data about physical environment

• 2 levels of access:
  1. Sensors
  2. Out-of-Band Safety Systems (TRITON)

• Type: cyber and physical

• Objectives: control, disrupt, data exfiltration
The CONTROL Layer

- Privileged motion control (root!)

- 2 levels of access:
  1. Controller
  2. CONTROL-DRIVE Channel

- **Type**: cyber and physical

- **Objectives**: control, disrupt, data exfiltration
The DRIVE Layer

- Modify motor properties during operation

- 2 levels of access:
  1. Controller
  2. CONTROL-DRIVE Channel

- Type: cyber* and physical

- Objectives: control and disrupt

* With limited physical access
The POWER LAYER

• Prevent or degrade motor performance

• 1 level of access:
  • Targeting power input

• Type: cyber* and physical

• Objective: disrupt

* With limited physical access
The MOTOR Layer

• Disruption of movement at the source of mechanical power

• 1 level of access:
  • Targeting the motor

• Type: cyber* and physical

• Objective: disrupt

* With limited physical access
The LOAD Layer

• Movement prevention by overloading the system

• **1 level of access:**
  • Targeting the output system

• **Type:** physical

• **Objective:** disrupt