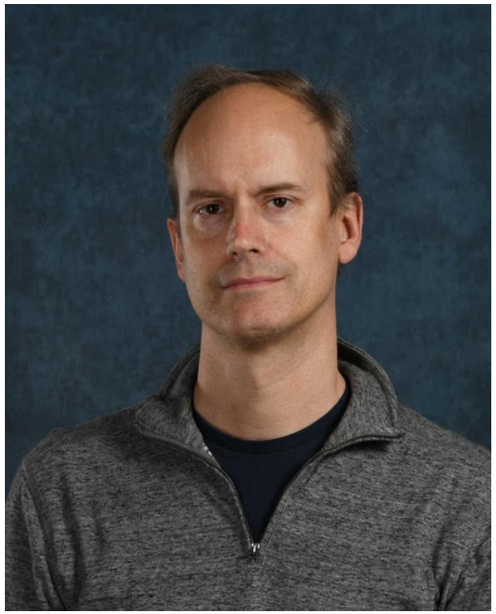

black hat®
ARSENAL
AUGUST 7-8, 2024
MANDALAY BAY/LAS VEGAS

RF Hacking on the Road

Logging Tire Sensors

Paul Clark

Paul Clark



Chief Engineer, Factoria Labs

Electrical Engineer - SDR
Author
Instructor

github.com/paulgclark/arsenal_tpms

Black Hat History

Trainer, since 2019
Arsenal, since 2022

TPMS

- Pressure and temperature
- Unique ID
- Very low power
- Very low duty cycle
- Mandated 2007 (US)

RF Data Logging

- Security and Monitoring
- Reverse Engineering
- Autonomous RF Systems

Capture

Find the signal

Capture to disk

Reverse

Tune

Demodulate

Estimate timing

Clock sync -> data bits!

Logging/ID

Payloads -> code!

Display/save

Apply filtering/alerts

Building a Full System

Software:
- Smart receiver
- Catalog major vehicles

Hardware
- Directional Antenna
- Hardware Filter
- LNA

Step 1 - Capture

Step 2 - Reversing

Step 3 – Extract Payloads

Step 4 – Logger Test

Step 5 – Logger Live

RF Hacking on the Road

Logging Tire Sensors

Paul Clark