

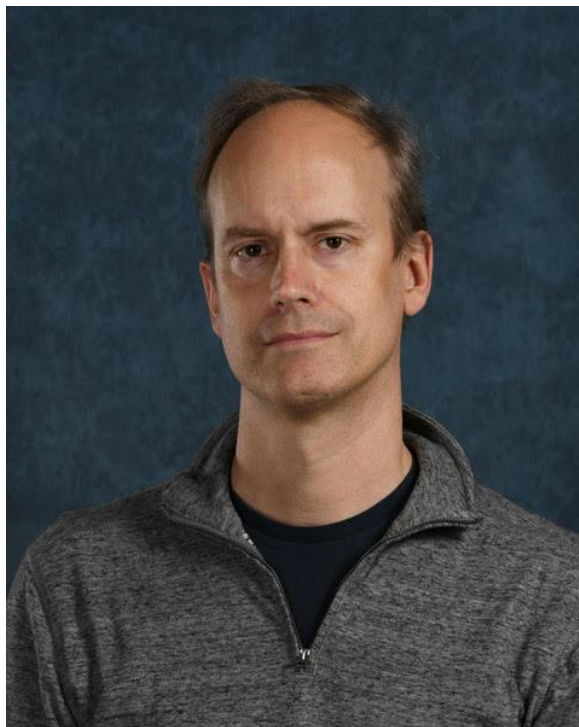


Hands-On RF Hacking

Your Table is Always Ready

Paul Clark

Paul Clark



Chief Engineer, Factoria Labs

Electrical Engineer - SDR
Author
Instructor

github.com/paulgclark/burger-pager-bhat

Black Hat History

Trainer, since 2019
Arsenal, since 2022

Restaurant Pager

- Relatively simple protocol
- Unique ID
- Haptic/LED Parameters



Capture

Find the signal

Capture to disk

Demod and Decode

Tune

Demodulate

Estimate timing

Clock sync -> data bits!

Decode Raw Bits

Reverse Protocol

Payloads -> Bit Function

Take over target!

Building a Full System

Software:

- Universal Radio Hacker (URH)
- SDR Drivers

Hardware

- Any TX-capable SDR
- Antenna
- Laptop



Thanks to the efforts of Johannes Pohl and Andreas Noack!

<https://github.com/jopohl/urh>

(use pipx!)

Universal Radio Hacker: A Suite for Analyzing and Attacking Stateful Wireless Protocols ^[SEP]

- 12th {USENIX} Workshop on Offensive Technologies ({WOOT} 18)

- <https://www.usenix.org/conference/woot18/presentation/pohl>

Step 1 – Find Signal

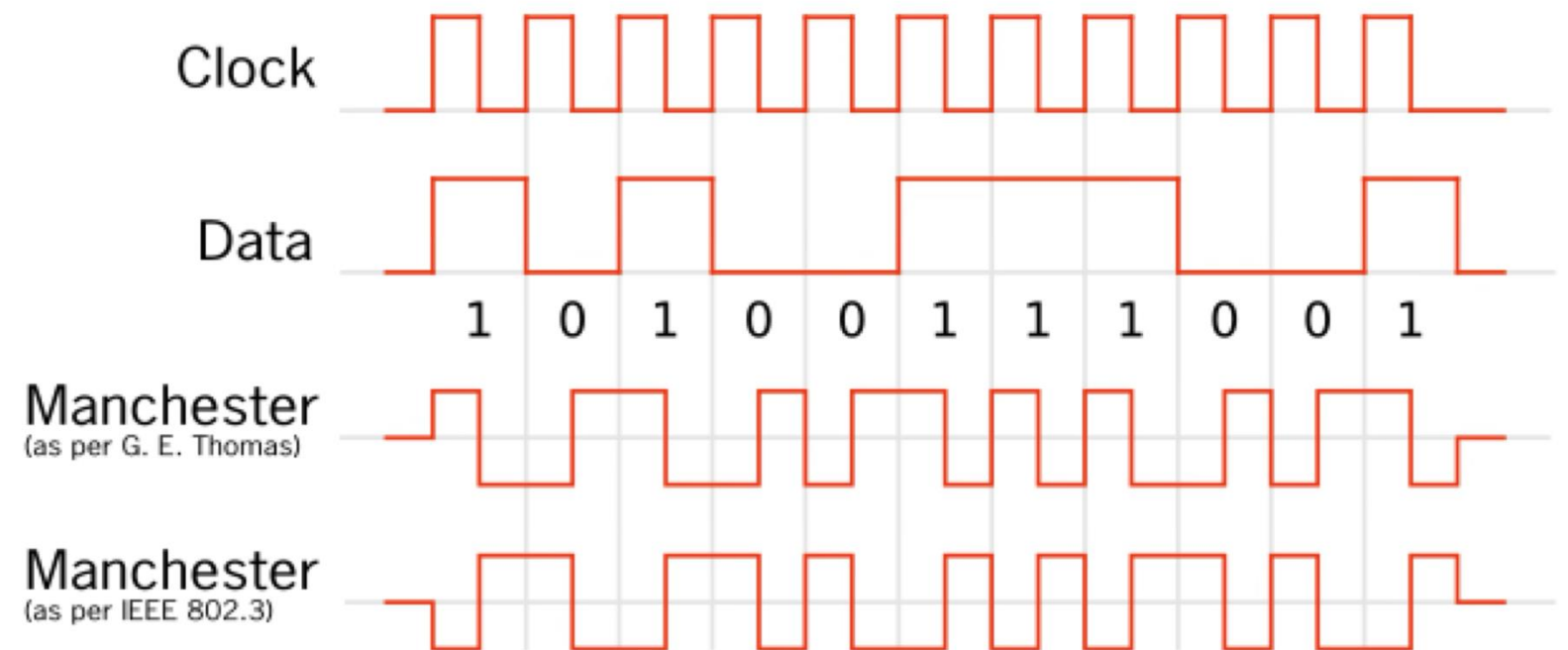
Step 2 - Capture

Step 3 – Demod

Step 4 – Decode

Encoding

- May not see data 1s and 0s
- Repetition -> Timing Errors
- Numerous schemes



Step 5 – ID Payload

Step 6 – Checksum

Step 7 – Takeover

Thank You!

Hands-On RF Hacking
Your Table is Always Ready
Paul Clark