Power Line Truck Hacking: 
2TOOLS4PLC4TRUCKS
Ben Gardiner (NMFTA), Chris Poore (AIS)
Agenda

• 50 minutes total
• Who are we?
• What is PLC? Generally & PLC4TRUCKS specifically
• Interfacing with PLC
• Tool 1: plc4trucksduck
• Tool 2: gr-j2497
• Adapters for PLC connection
• Issue & Impacts
• Future work
About Us

Ben Gardiner
- Senior Cybersecurity Research Engineer contractor
- at the National Motor Freight Traffic Association, Inc.
- Embedded systems dev, RE, CyberTruck™ Challenge Instructor, DC HHV & CHV volunteer, SAE volunteer

Chris Poore
- Senior Computer Engineer
- at Assured Information Security in Rome, NY
- degree in Social Engineering, is an active somnambulist, was King of the Pirates for three years, and frequently violates Pornhub’s terms of service.
About the Team

A great team

- AIS (Dan S, Chris P, Eric T)
- NMFTA

Plus a huge thank you to NMFTA motor freight carrier member sponsors
What is Power Line Communications (PLC)?
• In General: Power-line carrier, PLC, PDSL, main communications etc.
  • Communication of data on a conductor used also for power
  • e.g. ‘Green PHY’, ‘HomePlug’
  • e.g. IEEE 1901 interoperable family of technologies

• Found in SAE J1772 plugin-in electric vehicle charging.

• e.g. ... *PLC4TRUCKS*
Tractor & Trailer ABS circa 1997

**Need:**

- Trailer ECU
- Trailer ECU
- Tractor ECU

E.g. a Haldex AQ15463 (Finditparts.com)

By Ehsnils - Own work, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=28849516
Connector (J560)

Back of Cab:

By MobiusDaXter - Own work, CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=38288839
Tractor-Trailer Interface circa 1998

FMVSS No. 121 paragraph S5.1.6.2(b)
"... tractor electrical circuit must be capable of transmitting an ABS malfunction signal from the antilock brake system(s) on one or more towed vehicle(s)."

- “...[ATA TMC] approved PLC4Trucks in June 1998.”
  https://www.trucknews.com/features/tests-shedding-light-on-abs-warning-systems/
- SAE J2497 Published October 2002
  https://www.sae.org/standards/content/j2497_200210/
Power Line Carrier (for trucks)
Encumbered

“[June 2001] SAE withdrew its official sanction for the next PLC task force meeting and indicated that legal considerations concerning Intellon/VES patent and intellectual property rights might prevent it from setting and administering standards for PLC4TRUCKS.” –
"A second cable between the tractor and trailer was initially proposed by [NHTSA]. But NHTSA dropped it when fleet managers showed the malfunction warning could be done by multiplexing the existing single cable."

– Tom Berg, TTNews Apr 1999
SAE J2497

- Alt physical layer for J1708 (ish)
- Includes its own medium arbitration
- Always 9600bps
- Encodes J1708 payloads using spread-spectrum *chirps*

*By analogy (very loosely):*

- Diagnostics
  - J1587
  - J2497
  - J1708

- J1939
  - J1939/15
  - J1939/11

- DNS
  - UDP/IP
  - 802.11 Infra-Red
  - 802.3
J2497 Chirps

Specification:
• from 203 -> 400 kHz in 63us
• then 400 -> 100 kHz in 4us
• then 100 -> 203 kHz in 33us
• 100us total
• starting and ending at 0
• Amplitude between: 2.5 – 7 VPP

Two possible synthesized chirps @ 200 Msp
**J2497 Encoding**

**Preamble**
- Amplitude Shift Keying (ASK)
- Bit time 114us (14us silence after 100us chirp)
- Logic ‘0’ = chirp present
- Initial symbols (1-2 logic ‘0’)
- Start bit (logic ‘0’)
- MID bits (duplicated in body)
- Stop bit (logic ‘1’)

**Body**
- Phase Shift Keying (PSK), 180deg difference
- Bit time 100us
- Logic ‘0’ symbol is arbitrary per device, determined by the symbol transmitted in the preamble
- Sync symbols (5 logic ‘1’)
- J1708 Body Bytes. MID followed by Data
  - Start bit (logic ‘0’)
  - Data bits (8)
  - Stop bit (logic ‘1’)
- J1708 Checksum Byte
  - Start bit (logic ‘0’)
  - Checksum bits (8)
  - Stop bit (logic ‘1’)
- Gap (0-4 logic ‘1’) & End symbols (5 logic ‘1’)

![Diagram](image-url)
Designed for J1708

PLC4TRUCKS was accomplished by an integrated circuit: Intellon SSC P485.

- Wraps with preamble, sync and end bits
- Performs arbitration using preamble MID
- Uses very clever timing to synchronize J1708 and PLC

The rest is from J1708

- J1708 ~ RS485 so UART start and stop bits
- Performs arbitration on MID (first byte)
- Checksum byte at end
J1587 Highlights (from the spec)

• Fixed length at 21 bytes – except when vehicle is stationary
• A factory test MID that “should never be sent by any vehicle system.”
• A bridging and forwarding scheme
• Dynamic address claim
• Cold and warm restart commands
• Toll systems, display signage, climate

For more details and how to decode J1587 automatically, see our team’s presentation on github.com/ainfosec/pretty_j1587
Common PLC Messages (on Trailers)

• In our testing the messages we’ve seen are limited to:
  • ABS Fault Lamp on and off
  • Diagnostics

• 2005 FMCSA-PSV-06-001 report suggests that there should also be:
  • Axle weigh systems
  • Yaw sensors
  • Door latch sensors
Interfacing with PLC

• Traditional Diagnostics Adapters
  • Convert PLC <-> J1708 adapter pins
  • e.g. DG Technologies PLC TestCon 600USD
  • e.g. Nexiq 604020 330USD
  • Converts from PLC on power pins of DB15 to J1708 pins on another DB15

• These aren’t cheap.
• Intellon P485 becoming harder to source
• These also can’t do ‘weird’ things to PLC. They are limited by J1708 interface.


Nexiq PLC adapter (FindItParts.com)
Interfacing with J1708 (to interface with PLC)

• An RP1210 Adapter with J1708 support (most)
  • Needed for manufacturer diagnostics tools
  • E.g. DG Tech DPA4, DPA5, Nexiq USBLINK

• Truck Duck beaglebone cape(s)
  • by sixvolt & haystack, @DEF CON 24
  • Later revisions 1.5 YEET and MEGA
  • py-hv-networks for J1708 (and SocketCAN for J1939)
PLC Writing Tool Goals

• Low cost
• Open
• Capable of doing weird things
• Arbitration optional, frame detect likely needed
• No read for now

Approach: Truck Duck Modifications

• Small changes to Truck Duck; ideally just PCB rework
• Open source code and feed board and BOM changes back to sixvolts
• Create arbitrary chirp-trains by bitbanging PWM using the PRU
Bitbanging PWM on PRU

- Bitbanging = toggling GPIOs from software
- Programmable Realtime Unit (PRU) gives jitter-free code at 200MHz
- Need to find a GPIO that can be used on
- PRU is already used on Truck Duck for J1708 Channels 1 and 2
  - Realtime frame detect and back-off for J1708 transmit (not arbitration)
- Truck Duck J1708 Channel 2 is (fortunately for us) broken
  - We can use the PRU for J1708_2
- We need to find a GPIO for bitbanging PWM
  - Ideally also can be later migrated to use PWM peripheral instead
Selecting Some Pins

- Beaglebone has lots of pins but not all have the same capabilities
- PLC Output needed to be both PRU-capable and also PWM-capable
- Can’t conflict with other Truck Duck pins
- Settled P9.28; P9.29 as a backup
- We also want to plan for (later)
  - Frame Detect: P9.32, P9.35 or .40, and P.34
  - PLC Read via ADC: P8.39-46, P9.31, and P8.30
Two Main Pieces: PWM Synthesis and Coupling

Truck Duck:

- Beaglebone ARM
- 'J1708'
- Beaglebone PRU

Numbers:
1
2
Synthesis

The dumbest PWM method @ 200MspS
Coupling

Great filtering for coupling!

Dumbest filtering
PLC GPIO PWM Results

• Using PRU speed and deterministic execution
  • Wrote python to write PRU C-code to do PWM
  • PRU GPIO @ 25 MHz
  • Discovered some undocumented and unexpected instruction cycle counts and adjusted

Tuning edge delays

PWM result after receiver filtering (left: orange / right: purple)
The Code: PLC4TRUCKSduck

- MIT Licensed
- Improves J1708 PRU ‘server’ for Truck Duck
- Adds PLC write PRU ‘server’
  - as a J1708 interface
- Adds J1708 command line utilities
  j1708dump.py and j1708send.py
- All compatible with haystack’s py-hv-networks
- Truck Duck PCB rework instructions included

github.com/TruckHacking/plc4trucksduck
Adapters for PLC Write
Adapter 1:  
J560 to DB15 and Deutsch-2pin

• DB15 connector is on many Truck Ducks.

• This adapter would let you connect to the back of a tractor with J560

• Can be used for trailer also if you have battery <-> Deutsch 2pin

• Whole set comes with DGTech PLC TestCon
Adapter 2: Battery Clips to DB15 and ‘Stuff’

• DB 15 connector is on many Truck Ducks
• This adapter lets you connect to PLC right at the battery
• These are available in ‘Nexiq’ adapter sets
• Can be used with Tractor+Trailer Connected
Adapter 3: J560 Y Adapter to Deutsch 9pin

• Deutsch 9pin is on the UTulsa Truck Duck variation
• Could also use any DB15 to Deutsch 9pin adapter
• Can be used with Tractor+Trailer Connected
• WARNING: Some of these adapters are passive and some are active (contain an J1708<->J2497 adapter). Active ones will filter PLC signals.

www.ebay.ca/itm/Bendix-ABS-Trailer-Remote-Diagnostic-Unit-TRDU-PLC-Adapter-9-pin-Connection
Adapter 4: J560 inline, power breakout

- Brings out the power connector to hooded connector that can be probed easily
- Banana jacks are on the Truck Duck 1.5 and MEGA
- Can be used with Tractor+Trailer Connected

Adapter 5: Custom Umbilical Cable Tap

- Build one by soldering or joining onto power lines inside the shroud of a J560 cable (‘umbilical’)
- Deutsch 2pin here for easy connect to DG Tech PLC Testcon. Could use DB15 or Banana plugs
- Can be used with Tractor+Trailer Connected
A PLC Reading Tool
The Chirps (Again)

- These are spread-spectrum signals
- 100us chirp duration
- 100-400kHz

Most SDRs have minimum receive frequencies much higher than this
Solution: Upconverter

- Upconverters ‘move’ low freq signals ‘up’ into the higher frequency receive range of your SDR

- Upconverter options
  - Ham it up [https://www.rtl-sdr.com/tag/ham-it-up/](https://www.rtl-sdr.com/tag/ham-it-up/)
  - Spyverter [https://www.itead.cc/spyverter-r2.html](https://www.itead.cc/spyverter-r2.html)

- Tip: because the target frequency range (100-400kHz) is so close to ‘DC’ (0Hz) it is better to tune the SDR to 126MHz and filter to receive at (-900) - (-600)kHz
Alternative Solution: Direct Receive

- Theoretically: LimeSDR (wasn’t sensitive enough in our tests)
- Direct-receive modified RTL SDRs
- RTL-SDR blog v3 dongles (have direct-sampling built in)
- Airspy HF+
- ADALM2000 or other oscilloscope with GNU Radio support
Our Setup

We used an RTL SDR and Ham It Up and developed a GNU Radio custom block and flowgraph for receiving the J2497 frames.

We built some coupling adapters to ensure the upconverter wasn’t exposed to 12VDC. Although it may have been OK as many are AC-coupled on their input already.
GNU Radio Receivers

- Phase Measurement
- Correlation Measurements
Receive by Phase

- Using Quadrature Demod and measuring the phase-angle of the signal
- Changes in phase results in phase discontinuities
- Ignore the ASK preamble
- ‘method3’ in repo
Receive by Correlation

• Phase angle measurement and detecting spikes doesn’t work well in moderate to high noise environments.

• Correlate with a reference signal
  • Works best at 203kHz

• Ignore the ASK preamble

• ‘method1’ in repo
Receive Correlating against two Symbols

- Correlating against a whole chirp is good
  - But doesn’t readily distinguish between 0 and 1
- Do both:
  - Corr whole signal to detect burst start and stop
  - Corr 200kHz snippet to decode 0 and 1 in the body PSK
- Works good in medium levels of noise
- Ignore the ASK preamble
- ‘method2’ in repo
The Code: gr-j2497

• [github.com/ainfosec/gr-j2497](https://github.com/ainfosec/gr-j2497)

• gr-j2497 contains flow graphs with custom blocks for reading PLC4TRUCKS traffic.

• MIT Licensed

• Outputs received PLC frames as J1708 to UDP compatible with both haystack’s py-hv-networks and the j1708dump.py / j1708send.py tools in PLC4TRUCKSduck
Adapters for PLC Read
Just a 100nF Capacitor

- This (again) works well enough
- 100V just to be safe

- Then, you need a way to connect it to the wires of PLC
- All the Adapters for PLC Write apply here too for getting to the power lines;
Adapter 6: Converted Balun One Nine

- Balun One Nine has nice wire spring clips, an SMA connector and is inexpensive
- Remove transformer, replace with cap
- Cut center tap ground on rear
- Bridge grounds
- Add solder resist to avoid touching 12VDC at Truck battery currents

https://www.nooelec.com/store/balun-one-nine.html

Mod Plans (red)

Result
Adapter 7: It’s an Antenna

- Any 2200m or LowFER antennas should be suitable for picking up PLC
- We tested out a few portable options (loops, whips, mini whips)
- Best was this style of active mini-whip:

Pictured eBay.com,
There multiple options < 30USD
Distance: 6 feet
Why Does this Happen?

1/2λ: 12MHz

Shouldn’t be a good radiator. But it is good enough.
Why Does this Happen? (cont’d)

• Long contiguous wires in the trailers acting as radiating elements
• High transmit voltages (>7Vpp) contributing to this effect

• Conducted emissions: the PLC transmitters are left alone to be noisy.

7.4 Conducted Emissions Limit

The PLC signal must be considered when testing for the Electro-Magnetic Compatibility. The emissions from the PLC transmitters will exceed recommended limits in the PLC frequency range. Therefore, exceptions to the limits must be made for the PLC frequency range.

The appropriate tests to consider for measuring electromagnetic emissions are defined in CISPR 25 except Section 5, Annexes B, C, D, and H.

• Radiated emissions: FCC e-CFR §15.103 exempts the system from ‘unintentional radiator’ status as a “digital device utilized exclusively in any transportation vehicle...”
Impacts
Wireless Read of PLC: Impacts

Present:

• On Trailers MINOR impact
  • If trailer uses a PLC air weigh axle, then impact is higher
• (On other PLC applications: unknown)

Future:

• On Trailers (potentially) MODERATE impact
  • ATA TMC FutureTruck next generation Trailer interface is proposing to do key exchange over PLC
  • Could be a problem if not implemented correctly

Wireless Read of PLC: Mitigations

Present:
• **For fleets:**
  What PLC traffic is on your trailers?
  Consider loss of confidentiality:
  • e.g. air weigh axle
  • e.g. trailer ECUs configured to stream readings like wheel speed

Future:
• **For ATA TMC FutureTruck next gen. tractor-trailer interface:**
  Reduce emissions
Mitigations, Future:

Should mitigate remote PLC read.

- Shorter radiating elements
- Enables lower voltage transmit
Wireless Read: Disclosure

• Throughout this process (past 8mo) we had coordinated disclosure with:
  • Trailer equipment manufacturers (all 3 major ones)
  • Trailer builders (only 1 response though)
  • The NMFTA members
  • CISA Vulnerability Disclosure Program (previously called ICS CERT)

• CISA VDP has assigned CVE-2020-14514
  • A CISA advisory on Trailer Power Line Communications to raise awareness of this issue is forthcoming.
Future Work
Future Work

Transportation
• improve Truck Duck features
• try other DC block mods
• find new maximum distance with improved receiver code
• Look at Intermodal
  • Trailer on Flatcar (TOFC)
  • Trains
  • Ships

Industrial Control Systems
• Developing new GNU Radio transceivers for other ICS Power Line Communications Technologies:
  • G3-PLC
  • IEEE® P1901.2
  • ITU G.9903
  • PRIME (PoweRline Intelligent Metering Evolution)
Conclusion
Conclusion

• Tool plc4trucksduck enables Truck Ducks to write PLC
  • 1bit PLC chirps
  • Arbitrary PLC frames
  • Compatible with haystack’s py-hv-networks

• PLC traffic can be read remotely with < 100USD in tools from a distance of 6ft (so far)
  • ICS-VU-227452

• Tool gr-j2497 enables reception and decoding of PLC frames
  • Compatible with haystack’s py-hv-networks
DEF CON 28 Safe Mode
Virtual CHV

Trailer ABS ECU setup in the virtual Car Hacking Village.

We connected the trailer ABS exhaust port to NERF darts for... you. Enjoy!
Thanks!

NMFTA Members
CyberTruck™ Challenge
Trailer Equipment Manufacturers
ATA TMC Working Groups
Andrew Wallner
Dr. Jeremy Daily
Sean Bumgarner
Thomas Hayes
Thomas M. Forest
sixvolt
haystack
atlas
Urban Jonson

DEF CON 28 SAFE MODE,
Aug 2020