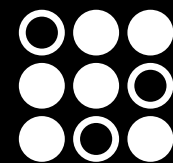


Trailer Shouting

Talking PLC4TRUCKS Remotely with an SDR
DEF CON 30

NMFTA

*National Motor Freight
Traffic Association, Inc.*



ais

ASSURED
INFORMATION
SECURITY

Agenda

45 mins

- What is PLC4TRUCKS?
- The patented chip & patent shenanigans
- What we've discovered & CVEs
- What is this RF stuff? / WhAt iS hApPeNing?
- How did we discover this?
- How can you do this?
- A Largely Unexplored Network
- Why disclose this?
- Demo

About Us

- **Ben Gardiner**

- Senior Cybersecurity Research Engineer contractor at NMFTA
- Director at Yellow Flag Security Inc.
- Experience: Embedded systems dev, reverse engineer
- CyberTruck™ Challenge Instructor
- DC HHV & CHV volunteer
- SAE volunteer

- **Chris Poore**

- Senior Reverse Engineer at AIS
- Discovering vulnerabilities in wireless systems
- Gaining access to systems via RF
- Reverse engineering RF protocols
- Forensically testing cybersecurity systems
- Administering RF collection events
- Developing open-source software for RF applications



About the Team

A *great* team

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

Plus a huge thank you to
NMFTA member carriers



Lounging

What is PLC4TRUCKS?

NMFTA

*National Motor Freight
Traffic Association, Inc.*



ais

ASSURED
INFORMATION
SECURITY

What is “Power Line” Communications?

Generally:

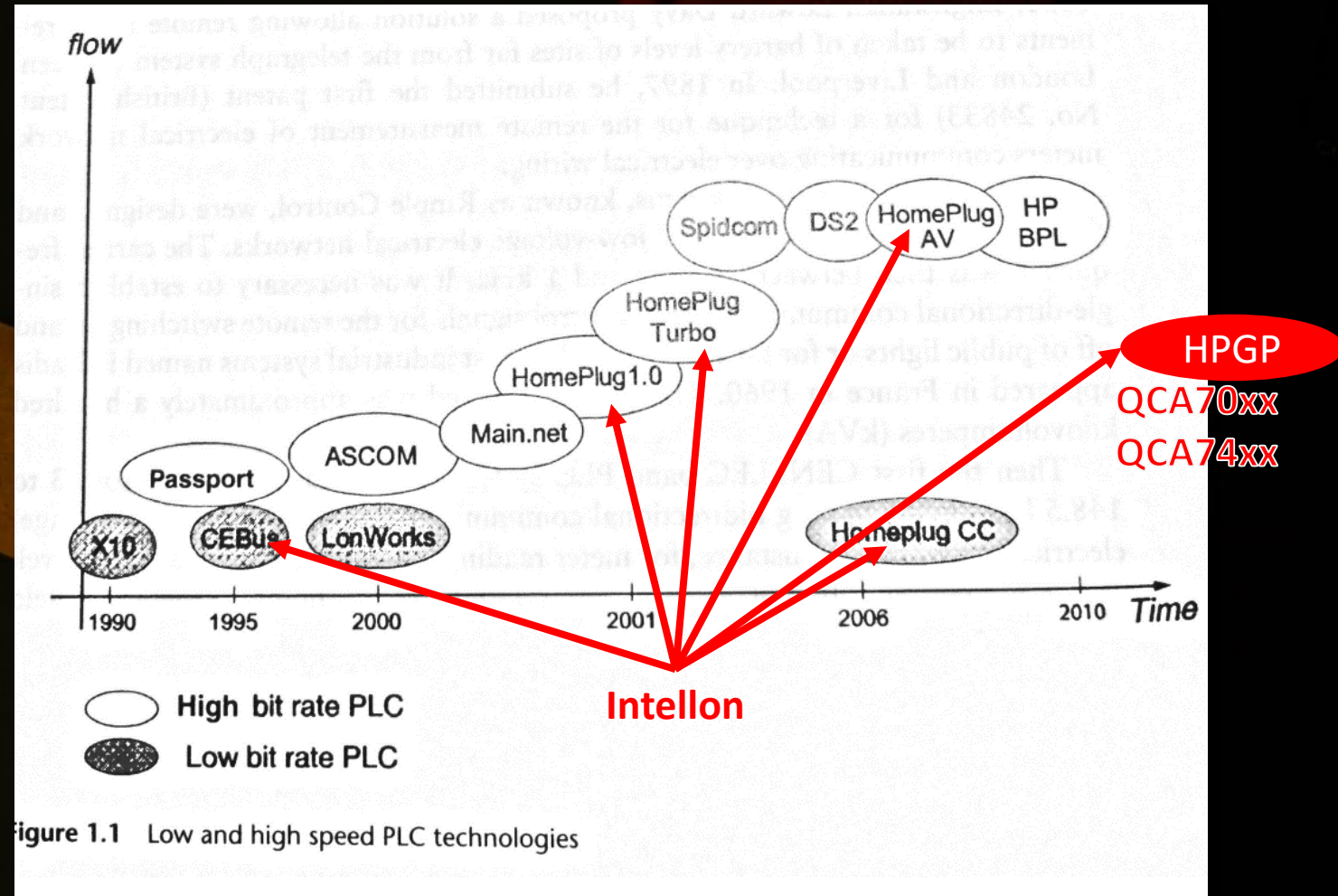
- Adding digital signaling to existing power-supplying wires. Adds communications without new connectors, allocating pins or adding wires.

Contemporary:

- IEEE 1901 HomePlug AV and HomePlug GreenPhy (used in CCS for Plug-in Electric Vehicles)

History:

- 2000: *HomePlug* alliance selected Intellon as baseline
- Intellon was bought by Atheros, was bought by QUALCOMM

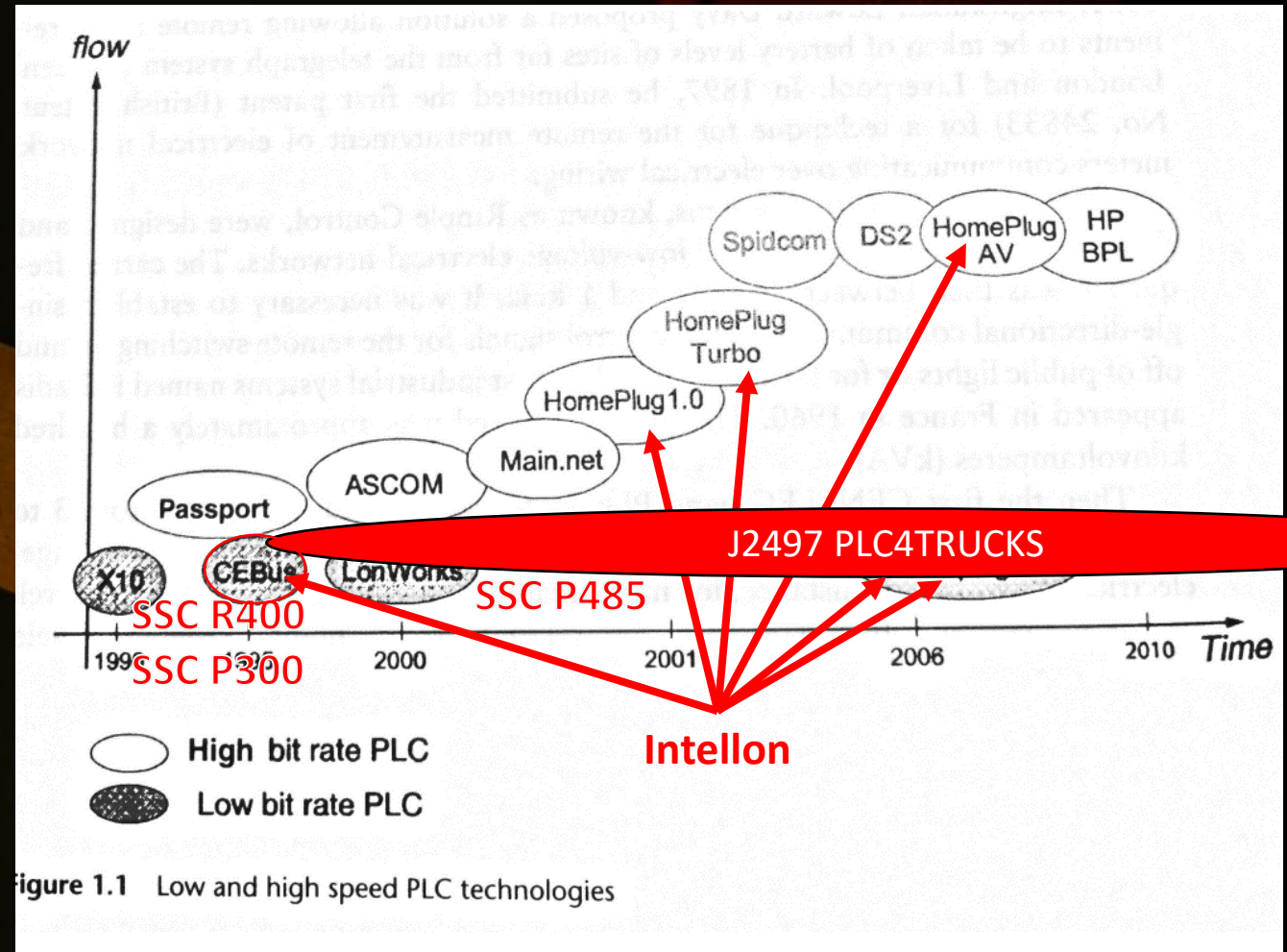


Carcelle, Xavier *Power Line Communications in Practice* Arctech House 2006

What is “Power Line” Communications?

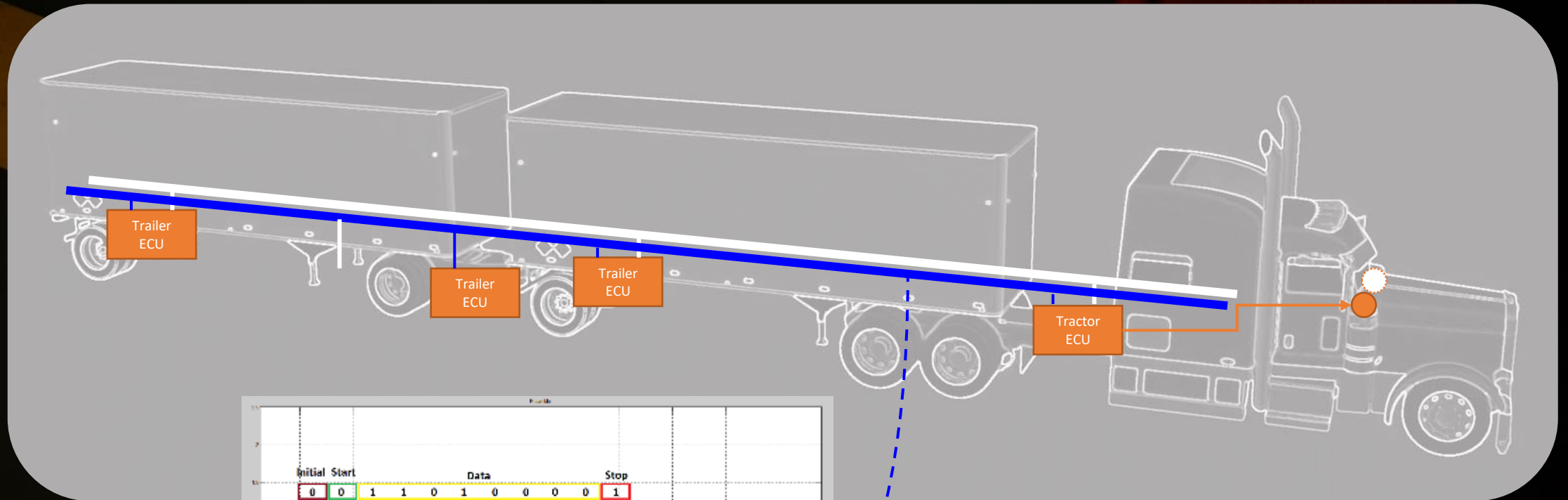
This talk: the **SSC P485**

- Introduced ~2000: as the only way to implement J2497 / PLC4TRUCKS
- As of 2007: 7E6 ‘legacy’ [sic] SSC P485 sold on 6 continents [IEEE ISPLC *Intellon* Keynote]
- Today: is sometimes emulated but otherwise implemented with SSC P485

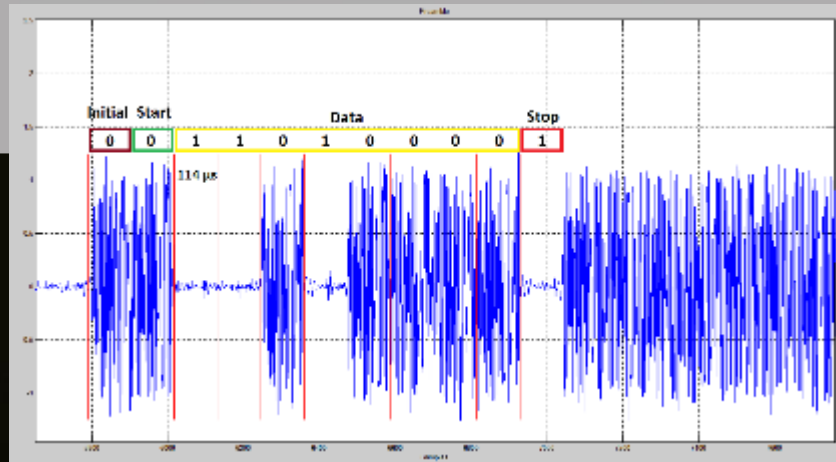


Carcelle, Xavier *Power Line Communications in Practice* Arctech House 2006

Power Line Carrier (for trucks)



12VDC

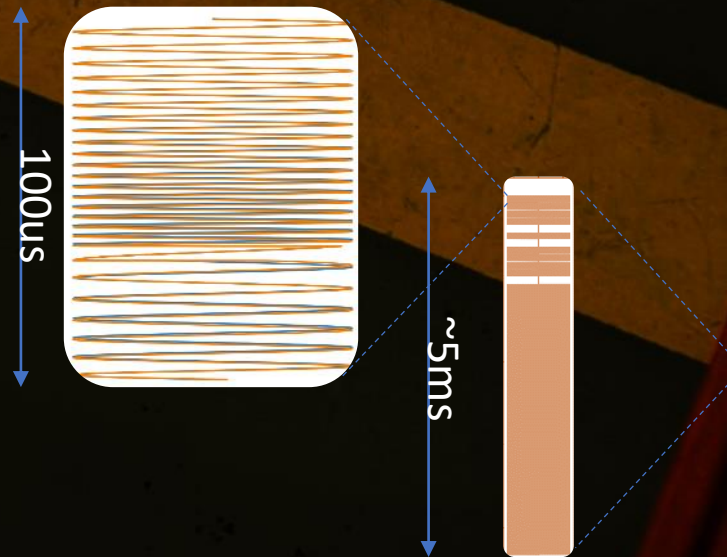


J2497 / PLC4TRUCKS Spread Spectrum

Spread spectrum using chirp symbols.

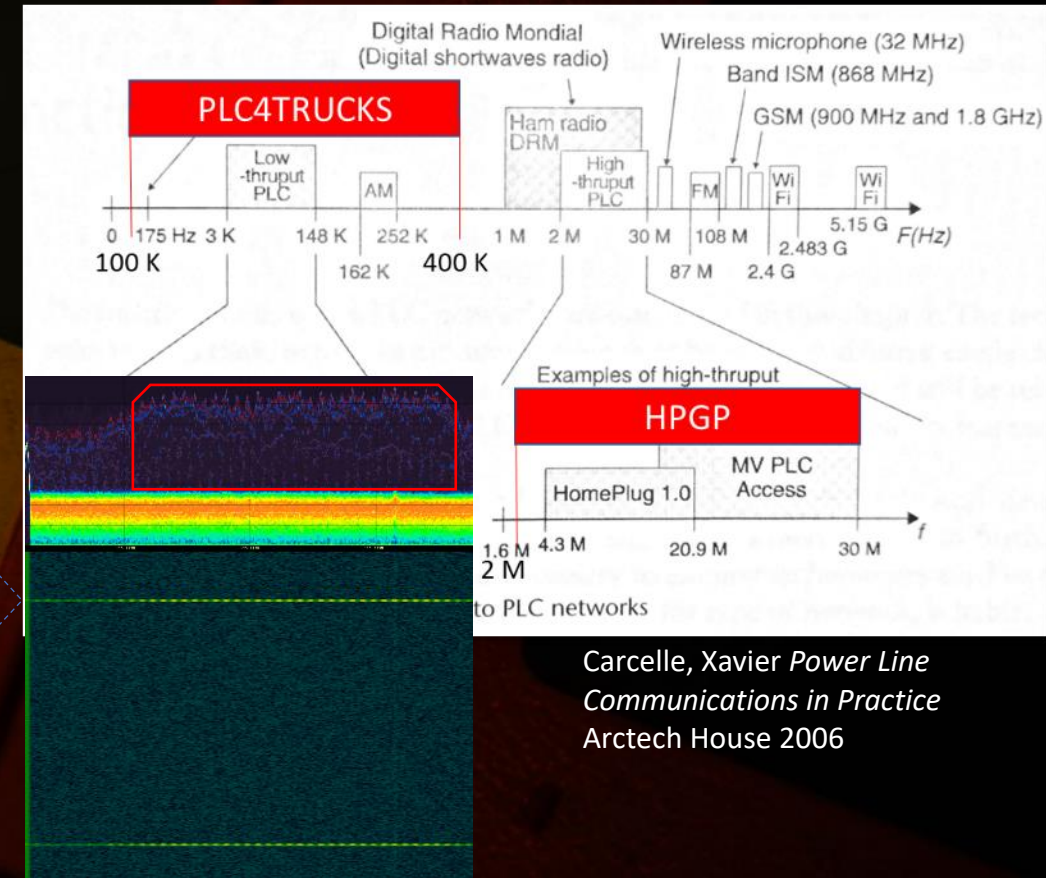
The chirps are 100us in duration, between 2.5 and 7V peak-peak

The chirps sweep from 203KHz through 400KHz (63us) then to 100KHz (4us) and back to 203KHz (33us) to finish



By analogy:

HPGP: ethernet over powerline
PLC4TRUCKS: UART over powerline

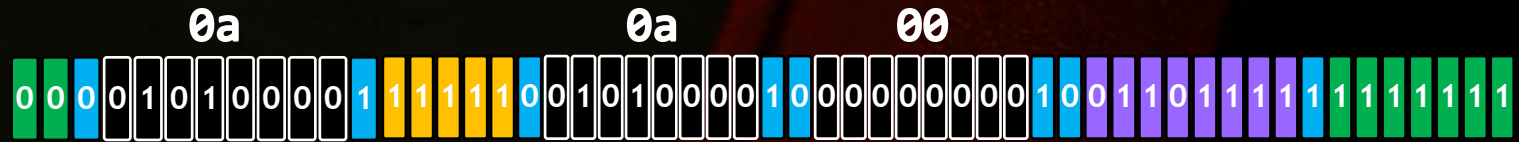
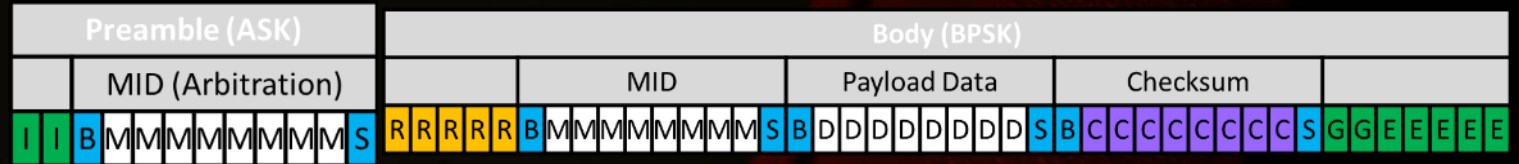


Carcelle, Xavier *Power Line Communications in Practice*
Arctech House 2006

J2497 Specifics

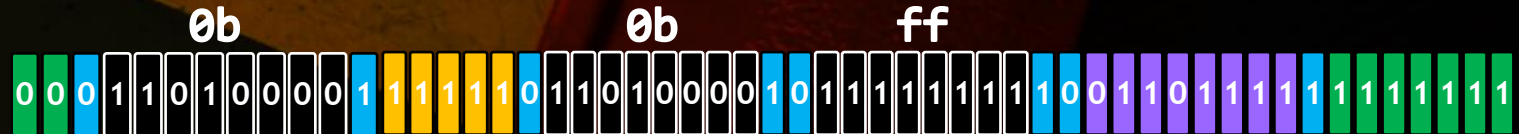
Preamble

- 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')



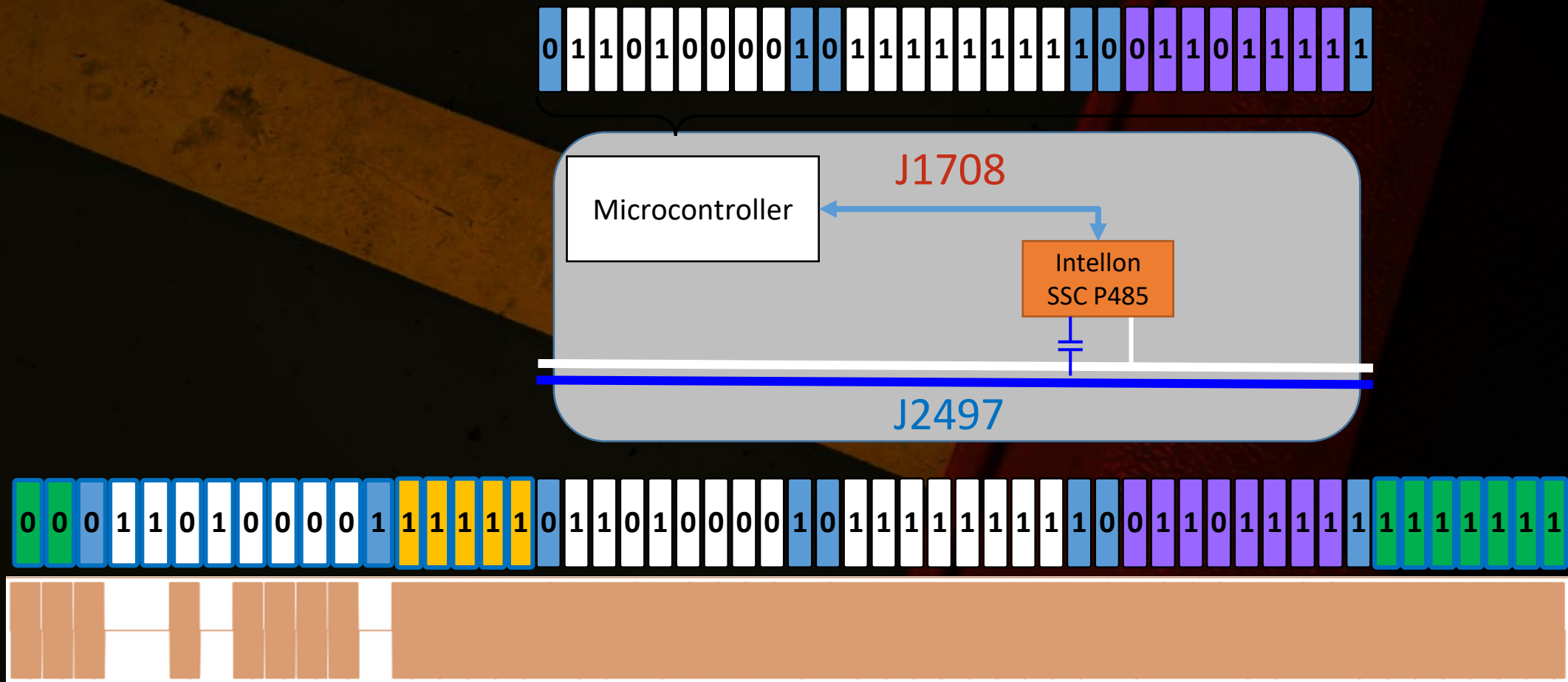
Body

- 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')



J2497 Specifics

- J1708 ↔ J2497
 - Implemented almost exclusively by the Intellon SSC P485 chip



J1708/J1587 Specifics

- Predates J1939 by many years. Sometimes still found in the tractor. Always still found in the Trailer as J2497.
- 9600bps 8N1 UART (RS-485); First byte is arbitration and source address (MID)
- J1587 standard defines the signal encodings
- and: proprietary messages in Data Link Escape (DLE)
- By analogy:

Diagnostics

J1587

J2497

J1708

Diagnostics

J1939

J1939/15

J1939/11

DNS

UDP/IP

802.11 Infra-
Red

802.3



Patents & Patent Shenanigans

NMFTA

*National Motor Freight
Traffic Association, Inc.*



ais

ASSURED
INFORMATION
SECURITY

- 1991 Vehicle Enhancement Systems (VES) formed from some Freightliner employees when Freightliner moved headquarters
- 1992 NHTSA lets the industry know that Trailer ABS fault dash indicator will be required by 1995, requests second cable, fleets reject
- SAE and ATA TMC task forces for tractor-trailer comms over 50s era J560 connector formed
- 1998 ATA TMC approves PLC4TRUCKS as the method



CC BY-SA MobiusDaXter

Although several competing devices could also multiplex the cable and send the warning signal, the mostly unproven PLC4Trucks won the industry's acceptance because it is a "generic" method that would avoid possible licensing fees. It also less costly than the other devices, Menig asserted.

<https://www.trucknews.com/features/tests-shedding-light-on-abs-warning-systems/>

- A VES founder was active in the ATA TMC and SAE Task Forces and filing patents around the developing technologies of tractor-trailer comms
- 1999 SAE withdraws J2497 due to the patents

NEWS

PLC4TRUCKS Hits A Snag

June 1, 1999

Plans for trailer data network threatened as deadline nears. It seems like a relatively minor technical issue - light a warning light in a tractor cab if a trailer's ABS system fails. For a variety of reasons, some technical and some competitive, a federal safety requirement mandating such a light has turned into a major headache for vehicle manufacturers and their ABS suppliers. And now the agency

Jim Mele

<https://www.fleetowner.com/news/article/21664669/plc4trucks-hits-a-snag>

- VES is purchased by Morey but the patent was assigned to a VES individual; Morey needs to make an agreement with the individual
- 2001: Suppliers, OEMs and Intellon all make agreements with VES individual
- 2002: SAE issues first J2497

NEWS

PLC4Trucks Dispute Settled

April 11, 2001

Makers of ABS equipment have recently started signing licensing agreements with the inventor of a required electronic circuitry. The \$1.50-per-tractor-trailer fee will be far less than the initial \$10 PLC4Trucks inventor Al Lesesky and his company, Vehicle Enhancement Systems Inc. (VES), first asked for, but much more than manufacturers claimed the technology was worth. PLC4Trucks allows trailer ABS

Tim Parry

<https://www.fleetowner.com/news/article/21680063/plc4trucks-dispute-settled>



What We've Discovered & CVEs

NMFTA

*National Motor Freight
Traffic Association, Inc.*

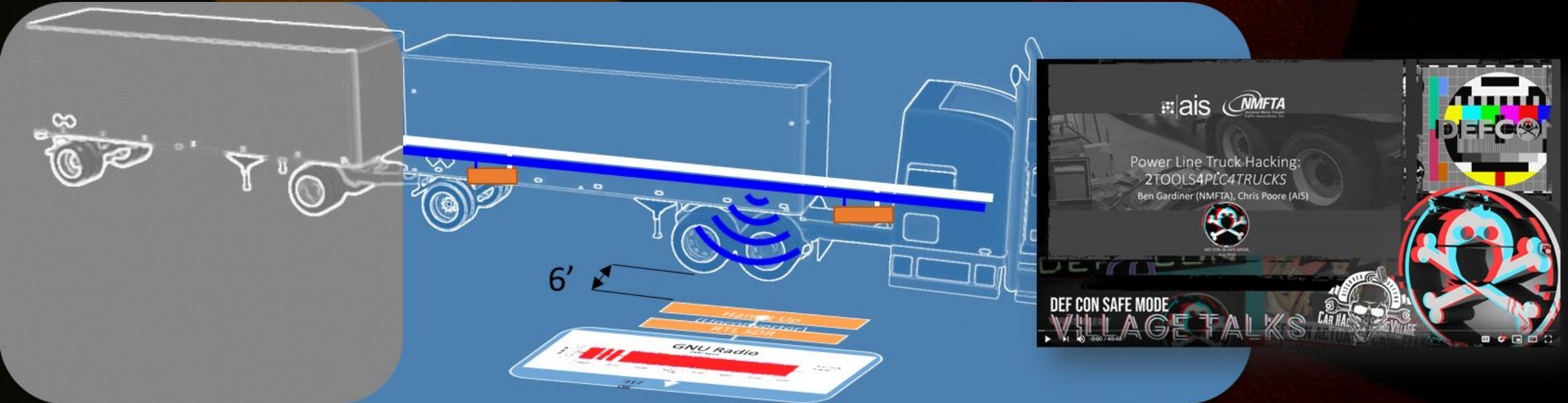


ais

ASSURED
INFORMATION
SECURITY

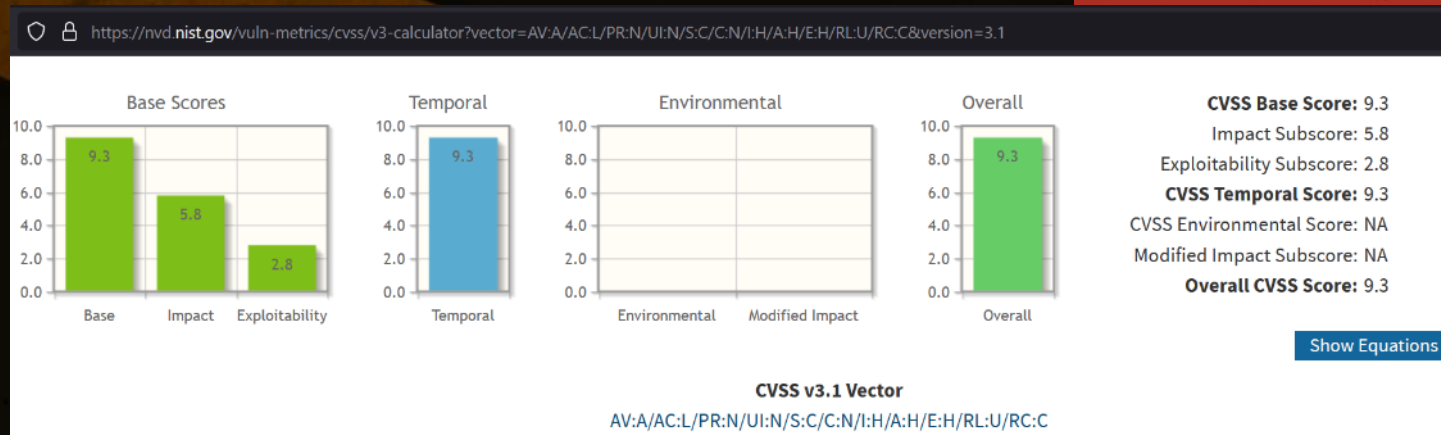
Previous Work: Remote Read

- PLC4TRUCKS can be read ~6ft from tractor-trailer using mini-whip antennas and SDRs
- CISA Advisory ICISA-20-219-01
- [CVE-2020-14514](#)



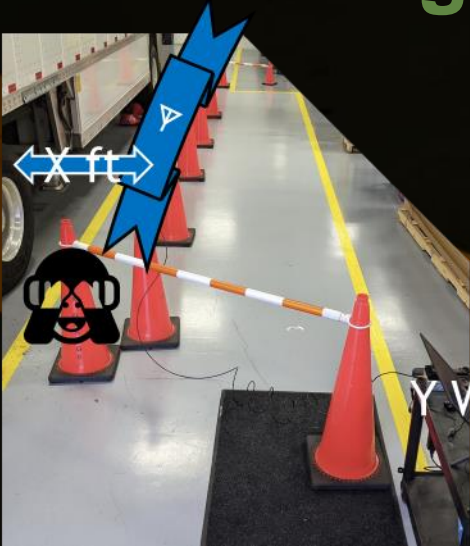
Inducing J2497 by Transmitting RF

- Our CVSS v3.1 estimate of this attack: **9.3**



- Severity in CVE-2022-26131: **9.8**
- Category: CWE-1319 Improper Protection against EM-FI 🧐

Induced Signal Testing Results



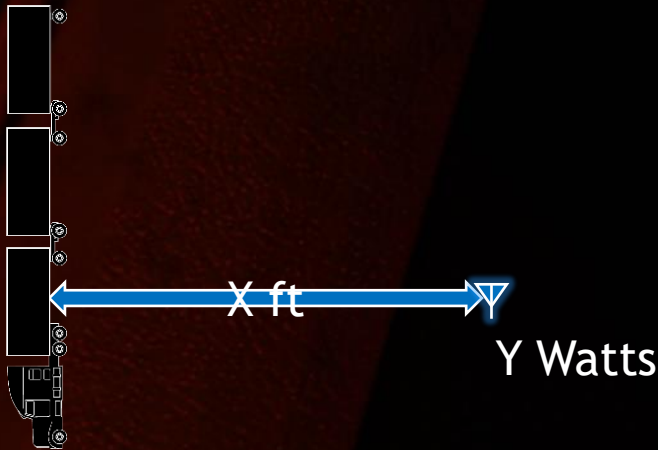
Dry-van, Metal Decking

Distance, Driver-side [ft]	Minimum Power [W]	Power Amp Cost [USD]
1.5	12.5	100
3	Unknown (but >50)	Unknown (but >200)



Tanker

3	1.5	10
5	2	50
8	10	100
11.5	12.5	100
22	Unknown (but >45)	Unknown (but >200)



Triple Dry-van, Wood Decking

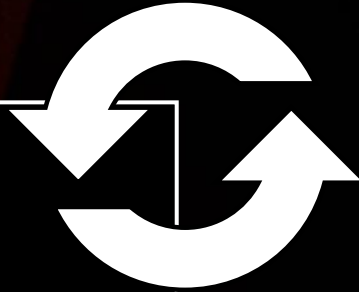
1.5	40	200
3	40	200
4.5	75	1,000
6	100	10,000
8	160	10,000
20	Unknown (but >160)	Unknown (but >10K)

Also: Can Replay All Trailer Diagnostics Commands

CVE-2022-25922

- All supplier J2497 diagnostics can be replayed

acfe89_____	acfef6_____
acfe89_____	acfef6_____
acfe89_____	acfef6_____
acfe89_____	acfef6_____
acfe89_____	acfef6_____
acfe8a_____	acfef7_____
acfe8a_____	acfef7_____
acfe8a_____	acfef7_____
acfe8a_____	acfef7_____
acfe8a_____	acfef7_____
acfe8b_____	
acfe8b_____	
acfe8b_____	
acfe8b_____	
acfe8b_____	



A dark, grayscale photograph of a truck's rear wheels and chassis. In the foreground, on the ground, there is a piece of electronic equipment, possibly a radio or a computer monitor, with various cables connected to it. The scene is dimly lit, suggesting an industrial or outdoor setting at night or in low light.

What is this RF-Foo?

NMFTA

*National Motor Freight
Traffic Association, Inc.*

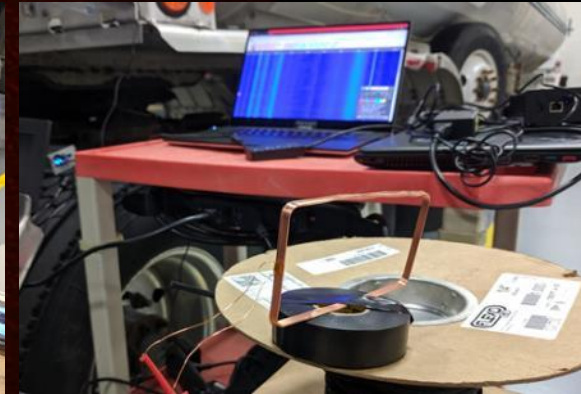


ais

ASSURED
INFORMATION
SECURITY

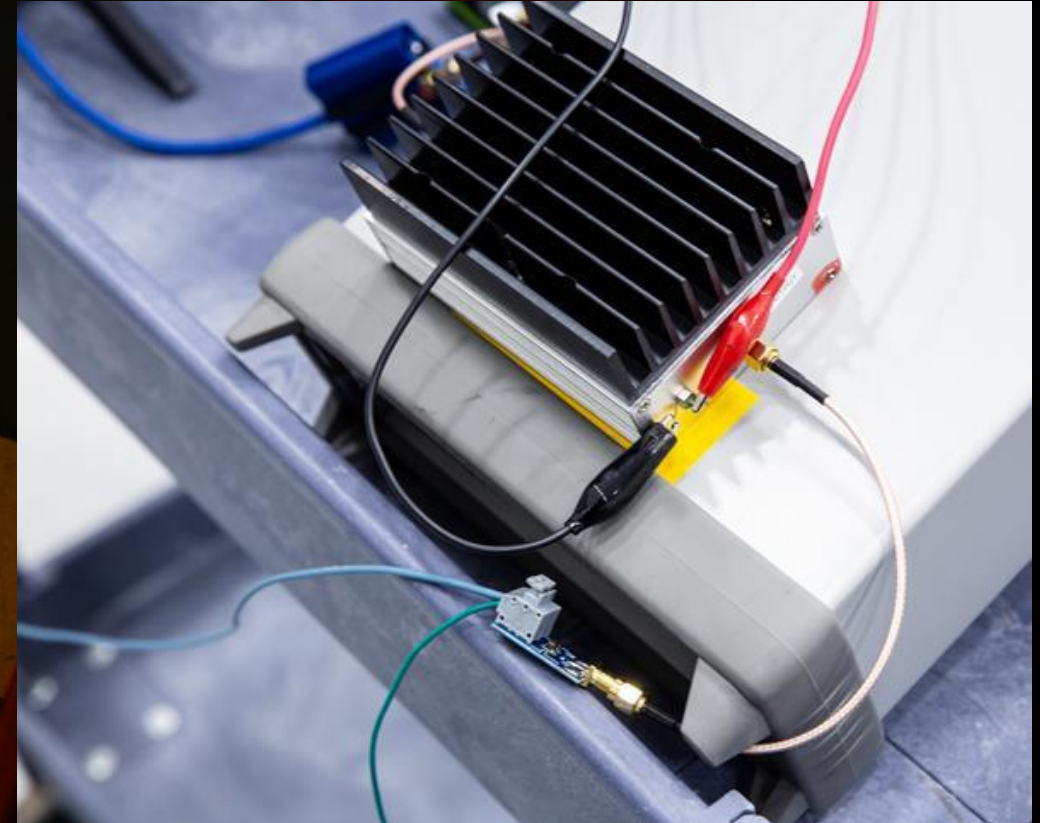
What is this Remote Foo (RF) foo you speak of?

- There are a lot of things that don't work
 - Loop antennas
 - Loading coils
 - Rolling out ground planes
 - Transmitting the bitbang signal from a modified Truck Duck
 - i.e. toggling GPIOs from real-time software
<https://github.com/TruckHacking/plc4trucksduck>
- Breaking the power amplifier



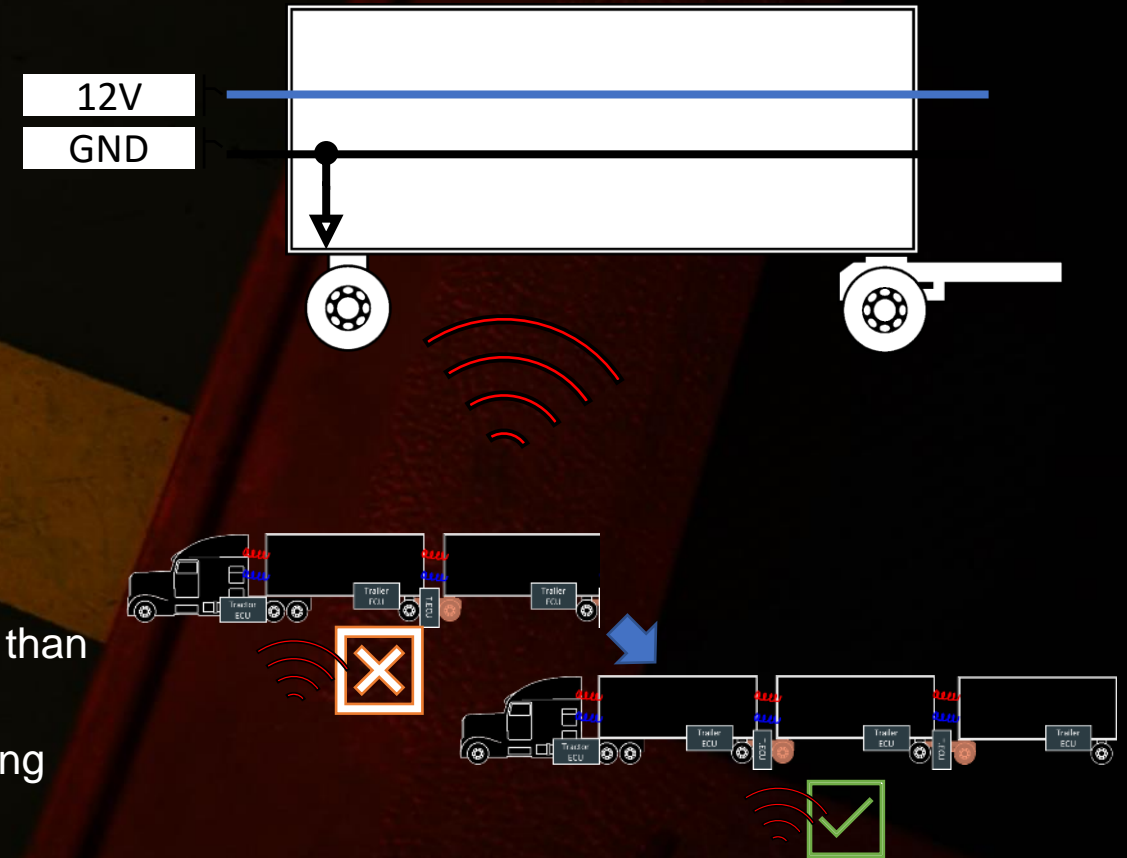
But what does work?

- Surprisingly, the FL2K dongle
 - An unaltered USB 3.0 to VGA adapter
 - Provides more output power than most SDRs
 - Much cheaper than other SDRs
- Lengthy wire runs parallel to the trailer
- An updated gr-J2497 GNU Radio module with signal transmission
 - <https://github.com/ainfosec/gr-j2497>
 - Use with any SDR compatible with GNU Radio
 - Reverse the Ham It Up to be a 125 MHz to 100-400 kHz downconverter



What is happening and how is RF Received?

- The RF signal (100-400 kHz) can be injected onto the 12V power line because of...
 - A lack of differential mode signaling on the cable
 - The resonance effect in road trains
 - The high sensitivity of the Intellon chips
 - (more) Wild Speculation™
- Despite all the roadblocks
 - Low frequency (LF/MF bands), wide relative bandwidth
 - It's all 'near-field' at our scales
 - Makes for bad transmit and receive antennas
 - Reflections and impedance mismatches at terminations
 - Some chirp frequencies are transmitted/received better than others
 - Certain trailers have more exposed cabling, less shielding
 - Amplifier harmonics and signal conditioning challenges

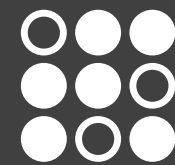




How did we Discover This?

NMFTA

*National Motor Freight
Traffic Association, Inc.*



ais

ASSURED
INFORMATION
SECURITY

Timeline 1/2

2019-05	“Hey, it would be cool to transmit J2497 onto a trailer with SDRs”
2019-07	A call for collaborators sent out to NMFTA CTSRP (then HVCS).
2019-10	Testing at a member fleet confirms that remote read tools work. Testing at a research partner facility with a signal generator and 5W amplifier indicates that tanker trailers are susceptible to RF induction, but the method used at this time was invalid due to galvanic coupling between the amplifier and tanker.
2019-11	All 3x trailer brake suppliers are notified of the transmit tests above at the same time as disclosure of replay attacks on diagnostics and of remote read (the galvanic coupling issue was unknown at this time). NMFTA CTSRP (then HVCS) update on progress.
2019-12	Testing on member fleet’s dry-van trailer at AIS location results in the first indications that inducing messages on a dry van requires more transmit power than with a tanker.
2020-02	Galvanic coupling issue recognized. Testing at member fleet location with no new results: dry-vans require more transmit power.
2020-06	All 3x trailer brake suppliers are updated on progress so far.

Timeline 2/2

2020-08	Remote read CISA advisory ICSA-20-219-01 is released. Talk at DEF CON 28 Safe Mode CHV.
2021-09	Testing at a research partner facility with new equipment and techniques to avoid the galvanic coupling problem confirms remote write is possible and practical on tanker trailers. We propose exclusion of diagnostics on J2497 for the RP1217 trailer interface requirements by ATA TMC S.12.
2021-10	Testing at a research partner facility confirms remote write on all 3x trailer brake supplier's equipment and also shows it is possible on some dry-van trailers (e.g., with metal decking).
2021-11	Testing at a member fleet confirms remote write is practical on 3x road trains.
2021-12	Disclosure process is halted due to legal problems. We focus on developing our mitigation technology ideas against these attacks.
2022-01	Thanks to tireless efforts by Urban Jonson, the new results are disclosed to all 3x trailer brake suppliers in a coordinated disclosure with CISA VDP. We share with Auto ISAC a couple weeks later and with the ONG ISAC as well.
2022-03	The remote write CISA advisory ICSA-22-063-01 is released. We share the disclosure with our member fleets, trailer OEMs, ATA TMC, and later, the National Tank Truck Carriers.
2022-04	We present arguments to the ATA TMC Task Force on NGTTI asking them to exclude J2497 diagnostics from the next generation tractor trailer interface and to include attack mitigations on new tractors.

Gotta Chuff 'em All

- There is no authz nor authn.
- So we created a signal that chuffs:
 - Every trailer ABS supplier's ECU
 - At every possible dynamic address
 - Plus 1 of 2 supplier's tractor ABS (2nd is WIP)
 - On a loop 🖱
 - The DLEs don't interfere with each other on different supplier's equipment (lucky).
 - 'unichuff' works
- This can be done for any of the other J2497 commands without authz/n (i.e. all of them)

acfe89_____	acfe8b_____
acfe89_____	acfe8b_____
acfe89_____	acfef6_____
acfe89_____	acfef6_____
acfe89_____	acfef6_____
acfe8a_____	acfef6_____
acfe8a_____	acfef6_____
acfe8a_____	acfef7_____
acfe8a_____	acfef7_____
acfe8a_____	acfef7_____
acfe8b_____	acfef7_____
acfe8b_____	acfef7_____
acfe8b_____	acc3038800b0



How can YOU do This?

NMFTA

*National Motor Freight
Traffic Association, Inc.*



ais

ASSURED
INFORMATION
SECURITY

How can you do this?

- TL;DR Don't
 - Don't transmit onto equipment you do not own
 - Bench Setups
- Hardware Hacking diagnostics adapters
- Using FL2K adapter designs from Yapo on OSH Park
 - [OSH Park ~ Shared Projects by ted.yapo](#)
 - [PCBs assembled; LPF tested; boards shared | Details | Hackaday.io](#)
- Optional / Bonus Bench Features
- SDRs, downconverters, and amplifiers







A Largely Unexplored Network

NMFTA

*National Motor Freight
Traffic Association, Inc.*



ais

ASSURED
INFORMATION
SECURITY

The J2497 Network

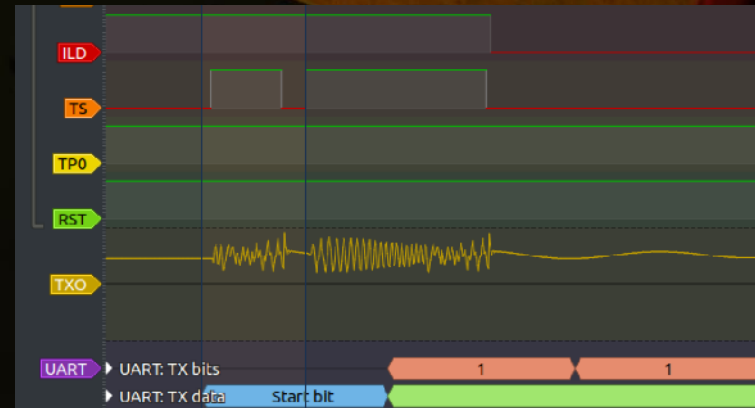


When inducing J2497:

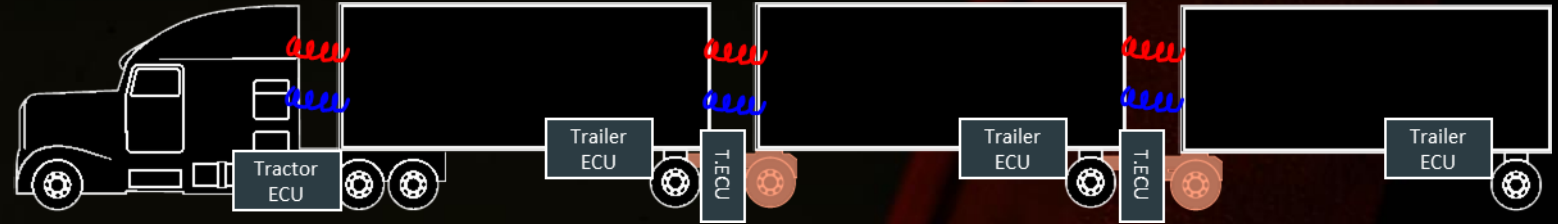
- At a minimum there will be a tractor and one trailer unit (e.g. tankers)
- More trailers brings more trailer units: many need converter dollies. A triple road train could have 5 trailer units
- When rolling the only required function is LAMP messages: sent-from trailer units, received-by tractor units
 - Everything else is vendor value add

J2497 Network Strangeness

- The J2497 preamble is discarded on receive
- J2497 Arbitration doesn't work – probably never worked
 - WABCO TCS II – unchanged from introduction in 2001 – sends random J2497 preamble (arbitration ID) bytes
 - 1 of 3 trailer supplier ECUs implements arbitration according to the specification
- In fact, the preamble isn't needed for receive
 - Any sync symbol will trigger reception
- Intellon SSC P485 sends chirp fragments due to some bug with its TS output controlling powerline amplifier



Solenoid Tests



- Also known as ‘chuff’ tests. Or ‘roll call’ on tractors (because each modulator clicks-off in sequence).
- Tractor ABS controllers have both a **modulator test** and a **service valve test**. The latter dumps **supply** air for the service brakes.
- Trailer Solenoid tests dump **reservoir air** when **control** air is applied
 - Recall for spring brakes **control** air signals to apply the brakes and **supply** air releases the springs and fills reservoirs
- ∴ Solenoid tests can drain reservoirs when the brake pedal is depressed and not in motion. But not when the trailer parking brake is applied.
- Except on **dollies** where solenoid tests dump reservoir air in both cases
 - Because **dollies** don’t use spring brakes
- Good news: Trailer ABS while in motion don’t accept solenoid test (on 1 of 3)
 - But it will if in fault and in motion (on 1 of 3)
- Solenoid tests are very useful for testing if a signal was received by an ABS controller. As a stand-in for a more damaging payload.
- We have not identified ‘service valve’ commands for Trailer ABS, nor such commands for Tractor ABS that work on J2497
 - We aren’t sure they exist
- RCE would almost certainly do the trick. We have not spent time researching vulns in any of the ABS controllers.

What Else? (On Tractors)

- Tractor units (both suppliers) respond to other J2497 messages, not just LAMP
- Some will reset in response to J1587 standard messages – the result is a 'roll call'
- Some bridge J2497 to J1708 (irrelevant on new trucks)
- Some support diagnostics from J1939 to J2497 (do they support the reverse?)
- None found so far support diagnostics on J2497

What Else? (On Trailers)

All diagnostics to trailer units are over J2497. Just looking at software and vendor literature yields: (other than chuff test):

- Tone ring / tire size configuration
- Axle number and function configuration
- Diagnostic Trouble Codes Read/Clear
- Notebook read/write
- Lift axle status and control

The trailer ECUs also have engineering tools (not intended to be in customer hands):

- Scripting language uploads
- Firmware updates



Why Disclose This?

NMFTA

*National Motor Freight
Traffic Association, Inc.*



ais

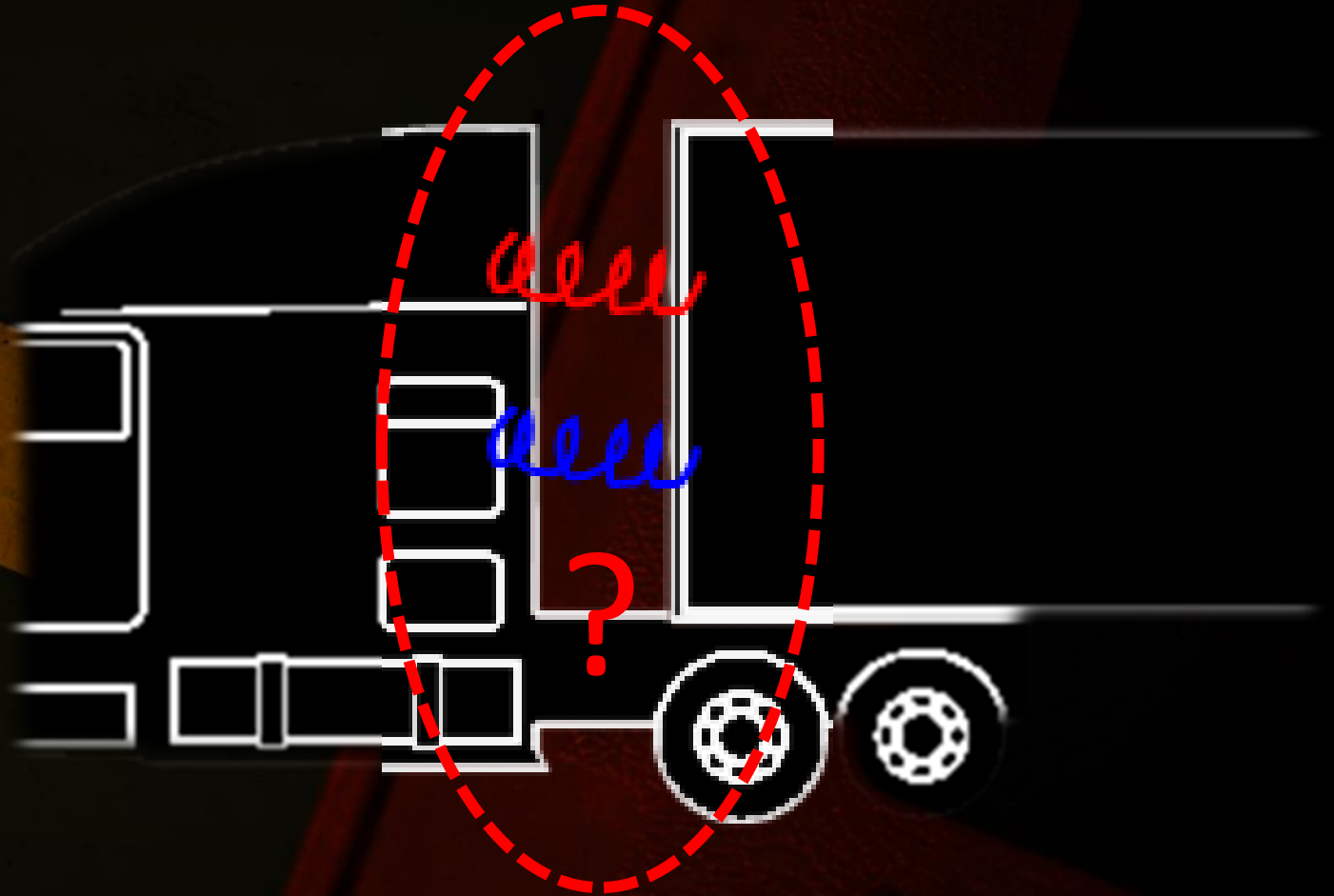
ASSURED
INFORMATION
SECURITY

Why Disclose?

Dilemma (not unique):

- Any discussion puts unwanted attention on 1000s of vulnerable and critical devices.
- Fleets need backwards-compatibility. This could result in importing all the same problems

The industry is specifying the next generation tractor-trailer interface now ; the issue must be widely understood to be fixed.



A dark, grayscale background image showing the lower portion of a truck, including its large tires and chassis. In the foreground, on the ground, there is a piece of electronic equipment, possibly a laptop or a specialized device, with various cables connected to it.

Demo Video

NMFTA

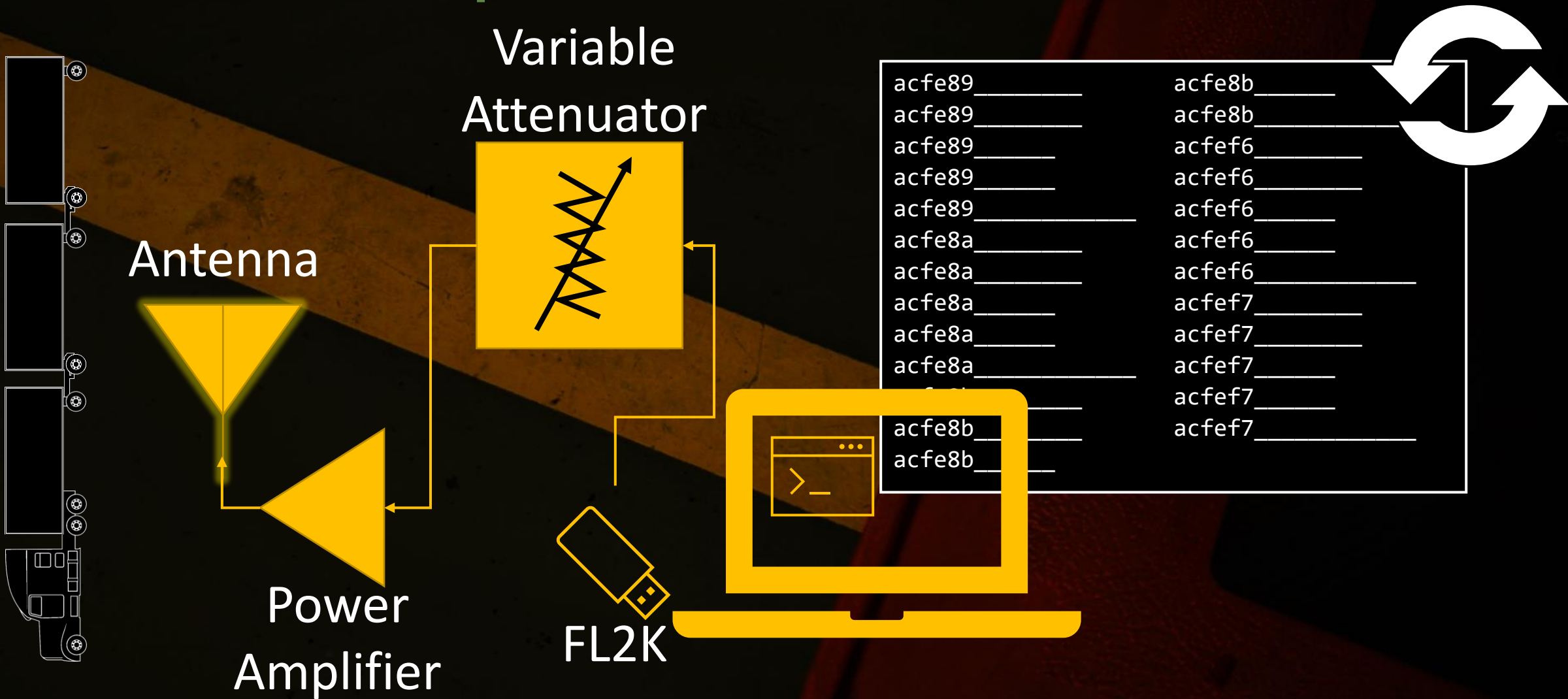
*National Motor Freight
Traffic Association, Inc.*



ais

ASSURED
INFORMATION
SECURITY

Demo Video Setup





Conclusions

NMFTA

*National Motor Freight
Traffic Association, Inc.*



ais

ASSURED
INFORMATION
SECURITY

Conclusions

- It is possible to read and write PLC4TRUCKS remotely on some tractor-trailer configurations with varying distance and budget
 - In the worst case, remote write can be achieved with very cheap transmitter (FL2K)
- Writes reach both the trailer and tractor brake controllers
- Trailer brake controllers serve diagnostics over PLC4TRUCKS, and more
- Tractor brake controllers respond to more than LAMP on PLC4TRUCKS, including some (limited) bridging

Acknowledgements

- The attack research and tools were developed in collaboration with Assured Information Security (AIS) researchers Chris Poore, Dan Salloum, and Eric Thayer. Many thanks to them and AIS for their commitment to this project.
- We gratefully acknowledge the insights of Andrew Wallner and the thorough and timely edits of Urban Jonson. We also wish to thank all of the following for their support: CyberTruck™ Challenge, Trailer Equipment Manufacturers, ATA TMC Working Groups, Dr. Jeremy Daily, Sean Bumgarner, Thomas M. Forest, John Sheehy, Chris York, sixvolts, haystack, and atlas.
- This work was made possible by the continued support of the LTL motor freight carrier membership of the National Motor Freight Traffic Association Inc (NMFTA)

Questions?

Please send feedback to our CTO John.Talieri@nmfta.org

Ben Gardiner
ben.gardiner@nmfta.org



References

- Haystack & Sixvolts, Cheap Tools For Hacking Heavy Trucks, DEF CON 24 CHV <https://media.defcon.org/DEF%20CON%2024/DEF%20CON%2024%20presentations/DEF%20CON%2024%20-%20SixVolts-and-Haystack-Cheap-Tools-For-Hacking-Heavy-Trucks.pdf>
- Haystack & Sixvolts, TruckDuck (tool), <https://truckhacking.github.io/>
- Haystack, Python Heavy Vehicle Interface <https://truckhacking.github.io/>
- SAE J2497 https://www.sae.org/standards/content/j2497_201207/
- SAE J1708 https://www.sae.org/standards/content/j1708_200408/
- SAE J1587 https://www.sae.org/standards/content/j1587_201301/
- ATA TMC (S.1) Next Generation Tractor/Trailer Electrical Interface -- <https://tmconnect.trucking.org/communities/community-home/digestviewer/viewthread?GroupId=2173&MessageKey=1dd4568e-400f-4d11-b481-b68961657165&CommunityKey=782c741b-674d-4af4-b962-9019b3e7d056&tab=digestviewer&ReturnUrl=%2fcommunities%2fcommunity-home%2fdigestviewer%3ftab%3ddigestviewer%26CommunityKey%3d782c741b-674d-4af4-b962-9019b3e7d056%26ssopc%3d1&ssopc=1>
- ATA TMC (S.1) Next Generation Tractor/Trailer Electrical Interface New TMC Webinar Series Alert: Next Generation Trailer Electrical/Electronic Architecture -- <https://tmconnect.trucking.org/communities/community-home/digestviewer/viewthread?GroupId=2173&MessageKey=384c5d4e-4f7e-4e4d-b2b0-d47047fa8f78&CommunityKey=782c741b-674d-4af4-b962-9019b3e7d056&tab=digestviewer&ReturnUrl=%2fcommunities%2fcommunity-home%2fdigestviewer%3fcommunitykey%3d782c741b-674d-4af4-b962-9019b3e7d056%26tab%3ddigestviewer>
- ICS Advisory (ICSA-20-219-01) Trailer Power Line Communications <https://www.cisa.gov/uscert/ics/advisories/icsa-20-219-01> <https://nvd.nist.gov/vuln/detail/CVE-2020-14514>
- ICS Advisory (ICSA-22-063-01) Trailer Power Line Communications (PLC) J2497 <https://www.cisa.gov/uscert/ics/advisories/icsa-22-063-01> <https://nvd.nist.gov/vuln/detail/CVE-2022-25922> <https://nvd.nist.gov/vuln/detail/CVE-2022-26131>
- 49 CFR § 571.121 - Standard No. 121; Air brake systems.
- 49 CFR § 393.55 - Antilock brake systems.
- Wheel Monitor Inc. "About Us" <https://www.wheelmonitor.ca/about-us.html>
- Tom Berg, Tests shedding light on ABS warning systems Trucknews.com <https://www.trucknews.com/features/tests-shedding-light-on-abs-warning-systems/>
- Bruce Sauer, New Power for Trailers <https://www.bulktransporter.com/archive/article/21649717/new-power-for-trailers>
- Jim Mele, PLC4TRUCKS Hits a Snag <https://www.fleetowner.com/news/article/21664669/plc4trucks-hits-a-snag>
- DOT Task Order 7 of the Commercial Motor Vehicle Technology Diagnostics and Performance Enhancement Program https://rosap.nhtl.bts.gov/view/dot/155/dot_155_DS1.pdf
- Opendous Inc. Hamitup <https://web.archive.org/web/20190514113133/https://code.google.com/archive/p/opendous/wikis/Upconverter.wiki>
- Nooelec Hamitup nano https://www.nooelec.com/store/downloads/dl/file/id/100/product/323/ham_it_up_nano_datasheet_revision_1.pdf
- Airspy Spyverter <https://www.itead.cc/spyverter-r2.html>
- Hozumi et. al. Low cost development of HF receiver prototype for HF-START field campaign <http://www.ursi.org/proceedings/procAT18/papers/PID5209275.pdf>
- Balun One Nine <https://www.nooelec.com/store/balun-one-nine.html>
- Yapo, Ted. FL2K AM LPF May 2018 https://oshpark.com/shared_projects/OOkzY6K6 Accessed 20220407
- Texas Instruments Beaglebone and PRU SDKs http://downloads.ti.com/codegen/esd/cgt_public_sw/PRU/2.1.1/ti_cgt_pru_2.1.1_armlinuxa8hf_busybox_installer.sh http://downloads.ti.com/sitara_linux/esd/AM335xSDK/exports/ti-sdk-am335x-evm-07.00.00.00-Linux-x86-Install.bin http://software-dl.ti.com/sitara_linux/esd/PRU-SWPKG/01_00_00_00/exports/pru-addon-v1.0-Linux-x86-Install.bin <https://git.ti.com/cgi/pru-software-support-package/pru-software-support-package/>
- Poore, Chris, and Gardiner, Ben. "Power Line Truck Hacking: 2TOOLS4PLC4TRUCKS." DEF CON 30 Car Hacking Village 2019. http://www.nmfta.org/documents/ctsrp/Power_Line_Truck_Hacking_2TOOLS4PLC4TRUCKS.pdf?v=1
- Eduard Kovacs, Tractor-Trailer Brake Controllers Vulnerable to Remote Hacker Attacks, SecurityWeek <https://www.securityweek.com/tractor-trailer-brake-controllers-vulnerable-remote-hacker-attacks> 2022
- Baker, R. and Martinovic, I., 2019. Losing the Car Keys: Wireless PHY-Layer Insecurity in EV Charging. In 28th USENIX Security Symposium (USENIX Security 19) (pp. 407-424). <https://www.usenix.org/system/files/sec19-baker.pdf>
- Michael Ossman's H2HC 2017 keynote <https://github.com/h2hconference/2017/blob/41318f8412ff60339fcf7ba37f037f0f91b7265a/H2HC%20-%20Mike%20Ossmann%20-%20Keynote%20Notes.txt#L1>
- Sebastian Köhler and Richard Baker and Martin Strohmeier and Ivan Martinovic, "Brokenwire : Wireless Disruption of CCS Electric Vehicle Charging" 2022 <https://arxiv.org/pdf/2202.02104.pdf> Accessed 20220428

