The Future of Cybersecurity: Where do we go from here?

Workshop / Direction Finding

DIGITAL SOLUTIONS CONFERENCE
CYBERSECURITY

POWERED BY NMFTA
National Motor Freight Traffic Association, Inc.

Agenda

20/20/20

- Threats as we see them
- Current projects: active & backlog
- Your Input on Our Directions

Please ask questions at any time

Threat ‘Landscape’

Our POV

Enterprise Services Threats

- N-Day vulnerabilities exploited due to missed patching.
- Lack of user awareness & Training
- Default Accessible Services / Misconfigurations
- Lack of Segmentation
- PHISHING PHISHING PHISHING

Back Office / Haul

- Compliance department through Dispatch departments' (see diagram above) availability impact due to TSP compromise.
- Fleet Location Data Confidentiality impact due to TSP compromise.
- Fleet Location Data confidentiality impact due to cellular location based aggregation services.
- Fleet telematics data (including location) confidentiality loss due to satellite downlink spread.
- Fleet telematics data (including location) confidentiality loss due to proximity Cellular downgrade attacks.
- Fleet location confidentiality loss due to internet availability of telematics devices. Theoretical / Anecdotally possible from public info based on e.g. Black Hat 2018 Sierra Wireless device findings.
- Multiple risks, as above, unknown, foisted on fleets due to re-sold / white-labeled telematics devices.
- Telematics integrity loss due to TCP sequence hijack and/or PEP abuse due to satellite internet misconfiguration.
- Telematics integrity loss due to cellular spoofing.
- Vehicle network message injection (telematics-connected segment) due to compromise of TSP or telematics device transport layer.

Maintenance

Tractor Availability Impacts via:

- ❖ diagnostic, reflash, engineering or undocumented ECU features via maintenance laptop DLL shim attacks.
- ❖ diagnostic, reflash, engineering or undocumented ECU features via unintended BlueTooth / Wi-Fi interfaces on VDAs.
- ❖ diagnostic, reflash, engineering or undocumented ECU features via semi-permanent remote VDA installation, internet accessible.
- ❖ diagnostic, reflash, engineering or undocumented ECU features via remote reflash without authorization.

Vehicle Access

- Tractor availability impacts via several possible cyber-physical de-rate resulting attacks via transmit on vehicle network segment.
- Tractor availability via immobilization via tractor brake controller abuse after J1708 message injection capability obtained.
- Tractor availability via J2497 command injection via 8-20ft proximity radio transmission (equipment configuration varies distance).
- Tractor impacts (various possible) via wireless injection onto tractor-trailer camera system.
- Tractor impacts (various possible) via transmitting J1939 messages via head unit (radio).
- Tractor impacts (various possible) via aftermarket device ‘install apps.’

Vehicle: More

- Increased likelihood of tractor impacts (various possible) due to lack of vehicle segmentation via various vectors e.g. Telematics or Diagnostics compromise. Applicable to older trucks.
- Increased likelihood of tractor impacts (various possible) due to lack of segmentation via various vectors. Applicable to any trucks with telematics connections to J1708, including newest trucks at the time of writing.
- Vehicle segmentation mitigations are non-existent for powertrain segment-installed telematics devices such as OEM telematics devices; de-rate and more vehicle impacts are possible via a telematics compromise.

Docks

- ❖ Legacy mainframe application impacts (various possible) via compromise of integrated dock systems e.g. weigh scales, dimensioners, dock PCs.
- ❖ Dock IoT impacts (various possible) via malicious palette.

Current Project List

Active & Backlog

Projects: Active

- Ultimate Truck Hacking Platform
- Heavy Vehicle Cybersecurity Training
- Telematics Firewalls
- Securing Legacy Maintenance Software
- Fleet Enterprise Penetration Testing
- Distribution Center Vulnerability Assessment

Projects: Backlog

A. Vehicle Cybersecurity Requirements Working Group (VCRWG)
B. Connected Forklift Security Assessment
C. Demonstration of Remote Telematics Device Compromise (via Internet or Enterprise networks)
D. Install App Security Requirements
E. CAN in Automation (CiA): WG on CAN Security Gateways
F. EV Charger and Vehicle Security Assessment
G. Overall Fleet Cybersecurity Risk Analysis
H. Streaming API
I. Research into FW upgrades on ECMs
J. RF Spectrum Survey of DC (from fence & from pallet)
K. j1587_map

YOUR IDEAS HERE