Unlocking the Potential of Seed-Key Exchange Guide

Co-Author
Joe Ohr
NMFTA

Co-Author
Ben Gardiner
NMFTA

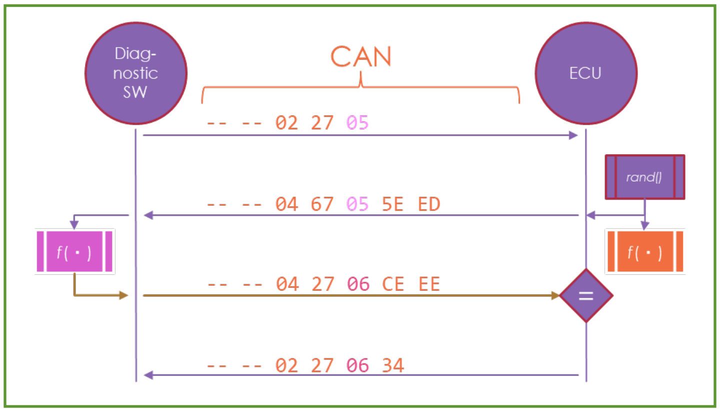
NMFTA™
National Motor Freight
Traffic Association, Inc.

CYBER

What Is It?

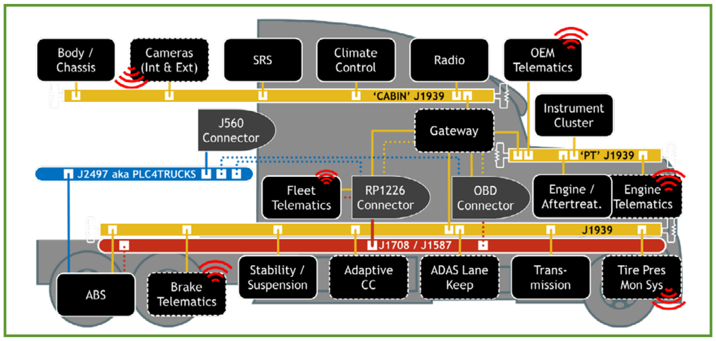
Seed-key exchange is an authentication and authorization protocol that protects diagnostic and engineering functions in trucks today and for the decades of vehicle networks before. The protocol is specified in the Unified Diagnostic Services (UDS) and KWP2000 standards for diagnostics and was present in non–standard implementations on J1587 networks before this. A successful seed-key exchange is required for most diagnostic functions on Electronic Control Units (ECUs) from unauthorized access.

The protocol is a challenge-response protocol where the ECU seeks to authenticate a source – which is usually diagnostics software but (as we will discuss further below) could be malicious software on the vehicle network. The ECU sends a "seed" challenge to the source, who must transform it correctly to gain access. The correct transformation routine is present in both the ECU and the authentic source.



This method was originally meant to prevent piracy, not cyberattacks, and is vulnerable to many attacks. And, once broken, the attackers can reuse and unlock everywhere that same ECU is used ("break once, use everywhere").

Truck networks are, of course, created to replace the pairs of wires which used to carry analog signals around the vehicle and, now with less weight, are carried by digital messages on the vehicle networks. These messages contain the signals that are the state of the vehicle control loops and for the most part when the control loops receive malicious state information they will react. But in addition to this, the trucks have diagnostic functions which are used frequently by the fleets and the same ECUs also host engineering functions which are used less frequently but not never. Seed-key exchange is the protocol protecting both the diagnostics and engineering functions on these ECUs.



Why Should Industry Leaders and Cyber Execs Care?

There has been a lot of recent attention about telematics and/or Electronic Logging Devices (ELDs) that could be compromised. A recent video released showed that a vehicle's acceleration could be blocked using a local Wi-Fi attack on a telematics device. This highlighted that compromised telematics devices can control vehicle network components via the Controller Area Network (CAN), which is designed for control loops where EDUs respond to messages they receive.

But this most recent demonstration by Colorado State University researchers was not the first sign that this would be a problem. In Nov 2023 we posted a reply to a question from a trucking company: "Is an ELD hackable?" The response here summarizes research released by two independent teams in 2022 and 2023: Sam Curry et. al. and Ramiro Pareja et al, that found multiple issues with telematics devices. Most of the issues are in passenger car telematics (but not all) and the latter work also found an instance of being able to control vehicle network data via telematics backend compromise.

While the Curry and Pareja research did not find issues with ELDs or telematics devices that are clearly used in North America, the technological similarity to the relevant telematics equipment is clear and the potential for ELD compromise has been publicly disclosed since as early as 2016 – see the Corey Thuen video linked in the response.

Today, fleets face a clear and present danger from ransomware operators; there have been many such cases over the past 3 years and whether these attacks are actively targeting logistics companies or not, it is undeniable that these malicious actors can obtain control of enterprise networks in our industry. Beyond the connectivity brought to the rolling assets by telematics devices in general (and regulation-required ELDs in particular), is the near-constant connection of the trucks to maintenance software on maintenance laptops. Considering that malicious software presence on fleet IT systems is an undeniable possibility and the regular and frequent maintenance software connections to the trucks; fleet maintenance laptop security is of paramount importance. As Dale Peterson, ICS Security expert, has pointed out: what the recent Volt Typhoon incidents teach us about threat actors is that they will acquire control and leave it dormant for a very long time until using it suits them https://www.linkedin.com/pulse/volt-typhoon-new-status-quo-ics-dale-peterson-yd8hc/ .

Both malicious software on telematics devices and malicious software on a maintenance laptop would have vehicle network access and, with it, the malicious software could attempt to inject messages. Many of these possible injections will, in fact, yield an engine de-rate (more details in the next section). These are all attacks of the *mission time* of the vehicle and whereas these attack paths are being designed-out of modern vehicle networks (e.g. via message authentication) the diagnostics systems are also a key feature of trucks and abuses of this feature cannot be designed-out. The diagnostics systems, once unlocked, allow access to parameter reconfiguration (reflash) and some cyber-physical commands (e.g. solenoid aka chuff test). But, beyond that, it is seed-key exchange (albeit usually a different routine) that also protects the even higher-privileged engineering functions which are also possible on the ECUs.

Overall, anything with vehicle network control can inject messages; what is reachable by the injection varies a lot and the attacker utility of injection is becoming less and less over time. But even in the near future, when all signal injection is blocked by perfect message authentication and network segmentation (if it ever actually exists), diagnostics will still be a necessary feature, and diagnostics services will almost certainly be reachable from the connectivity points of the truck. The diagnostics services are protected by seed-key exchange, and they also host the engineering functions which are protected by the same. As we will discuss, seed-key exchange is an inadequate protection and something better is needed now and for the future.

What Does an Attack Look Like?

While not a limitation of attacks in general, there are specific constraints for a 'simple compromise' or 'attacks with CAN spoofing alone'. Attackers cannot control all truck functions through telematics. As newer truck network technologies and topologies are deployed, some actions, especially those with physical impacts like certain diagnostics, require more than just a command. For example, testing the brake controller's service valve solenoid, which releases a lot of air, is a diagnostic function.

Attacks could finish with injection into control loops. As was demonstrated by NMFTA-funded researchers CanBusHack in 2020 even a very naïve fuzzing will result in a de-rate of the vehicle; furthermore, a NMFTA survey of all the public vehicle hacks in 2021 concluded that the vast majority result also in de-rates. In most cases, though, this requires that the attacker can inject onto the vehicle's powertrain segment.

The same CanBusHack research showed however, that the de-rates are also possible by re-configuration of engine limits (e.g. oil pressure). Changing parameters on ECUs usually requires only diagnostics access, but for some it requires engineering access. Either way the attacks could finish with seed-key unlock to re-configure the parameters of the ECU. Or, after unlock, execute cyberphysical test functions (e.g. cylinder disable or solenoid test). Or, finally after unlock, they could add malicious code (requiring the most privilege but also having the highest impact).

There are many ways to 'break' seed-key exchange. Where breaking seed-key exchange is an attacker gaining the privilege on the ECU which was guarded by seed-key exchange. This topic has been taught as part of the training at the cybertruck challenge, where NMFTA has always been a key sponsor – for years: https://www.cybertruckchallenge.org/wp-content/uploads/2023/06/How-Crypto-Gets-Broken-by-YOU-Ben-Gardiner.pdf

The details of how seed-key exchange gets broken are very technical, but in summary:

- The seed-key routine can be reverse-engineered from either the diagnostics software executables or the firmware on the ECU
- The correct key can be replayed to the ECU's chosen seed due to bad random number generation in the ECU
- The correct key can be replayed due to time-based random number generation in the ECU
- An attacker can simply interact with an ECU once diagnostic software unlocks it, reusing the correctly authenticated session.
- (and some others not covered here).

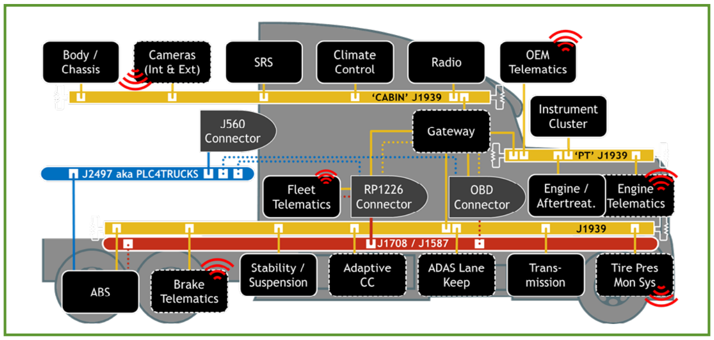
Once the attackers have a seed-key unlock they can use it in the overall attack strategy. One example attack scenario to consider is a telematics compromise followed by a seed-key unlock with enough privilege to add malicious code to an ECU. This is a scenario that the industry perhaps doesn't even want to say out loud lest they invoke it; however, based on the current landscape it is not unlikely enough to ignore it.

Another attack scenario may start with a maintenance laptop compromised by malicious software followed by the malicious software waiting until the authentic diagnostic software authenticates and then reuses that unlocked session to perform an ECU firmware dump which is exfiltrated to the attackers for further analysis.

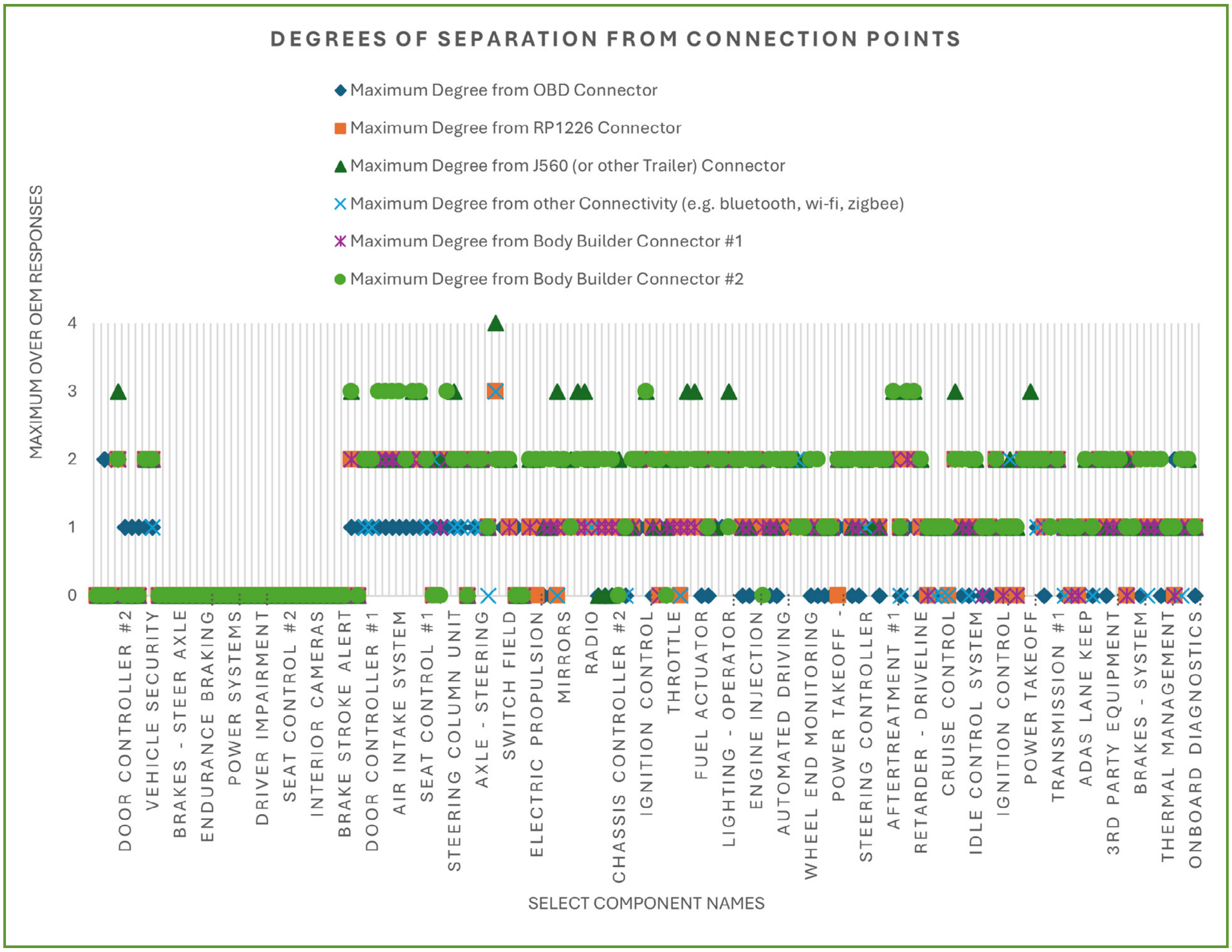
Of course, there are many more varied attack scenarios that could be listed and the activity of listing these can be entertaining or sobering – depending on your skillset and focus in cybersecurity. Let's consider one last attack scenario: attackers install radio transmitter equipment at choke points (e.g. bridges, tunnels) and broadcast valid J2497 messages which are picked up by tractor and trailer (due to https://nvd.nist.gov/vuln/detail/CVE-2022-25922). The J2497 sequence and timing is carefully crafted to reset trailer ECUs and perform a seed-key exchange at the right time to be able to predict the seed and send a successful key. The unlock allows the attackers to follow-up with any diagnostic command but in this case, they use chuff tests to bleed air supply from the tractors. This is a scenario which, thankfully, is not entirely possible on a grand scale and we will talk more about this attack, what it means for the industry as a whole and what we are doing about it during our October cybersecurity conference in Cleveland OH. Register now.

What about Truck Topologies and Access?

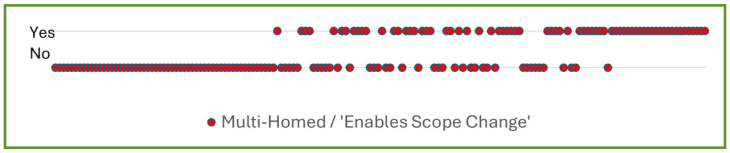
Different trucks have varied designs. Not all telematics devices can reach the powertrain segment directly. But even some modern trucks with security features still allow brake diagnostics from the RP1226 telematics port but this should be changing.



In 2022, the NMFTA collaborated with several heavy-duty vehicle OEMs in the Vehicle Cybersecurity requirements Working Group (VCRWG). One of the things accomplished was a survey of the typical degrees of separation of ECUs in vehicles to the points of connectivity in the vehicles. The results of this survey on the vehicles contemporary with that year are below – and there is a lot detail to try and capture here. Perhaps the most important thing to note that the large number of points on the 0 and 1 degree of separation line; i.e. many of the ECUs in trucks – even newer 2022-year trucks – are connected-to a diagnostics port, a RP1226 port or a wireless connectivity.



And the plot below shows that many of the ECUs are connected to multiple busses which can give attackers the means to 'pivot' into the ECUs which have higher degrees of separation. But of course, attackers don't need to cook up fancy exploits to pivot; because as noted above, many vehicles of this year and newer simply permit diagnostic traffic to be forwarded across the multi-homed gateways in the vehicle network.



What Are the Current Protections?

Seed-Key Exchange:

Engineering functions are usually protected by a different seed-key routine. So, they aren't unlockable by the same "break once, use anywhere" routine for diagnostics. But it is still usually another "break once, use anywhere" situation.

Seed-key routines are migrating to higher complexity which is making it harder to break from traffic captures. Some diagnostics software is integrating anti-reverse engineering techniques to thwart "break once, use anywhere" wins. But without $29 enhancements an attacker can wait for a maintenance laptop to unlock the ECU and then take advantage.

Passwords:

Some ECUs also use passwords for programming, which adds another layer of security. Fleets should use unique or at least batched passwords (to prevent 'break once, use everywhere').

What is the Long-Term Solution That NMFTA Recommends?

Newer trucks might use certificate-based authentication (service $29) instead of the older seed-key method (service $27).

Certificate-based methods are more secure but could affect fleet control over trucks, so fleets should ensure that their supplier's $29 service supports offline authentication and ideally fleet-controlled authorization of devices without the need for OEM special requests.

Fleets typically use trucks for up to 15 years, so new security features won't be immediately available fleetwide.

What is the NMFTA Doing to Help?

The example we mentioned above, where time-based random number generation could be predicted sufficiently well to unlock seed-key exchange blind, wirelessly, was discovered and disclosed to the supplier using their coordinated disclosure process. The NMFTA worked with that supplier to demonstrate the vulnerability and complete the disclosure process before presenting on the topic at esCar USA 2024 to an audience containing other suppliers and OEMs in the industry and called on the SAE to add mitigations to the next generation tract trailer interface standards against these attacks.

The NMFTA has been a key sponsor of the Cybertruck Challenge since its inception and, in addition to the monetary commitment, we send Ben Gardiner, our senior cybersecurity research engineer, to teach classes and mentor students during assessments. Each year, Gardiner has taught the students (and the industry people auditing the class) about seed-key exchange protocol and common weaknesses.

The NMFTA is actively seeking collaboration with universities to publish research and/or reference designs on service $29 which can avoid the 'break once, use anywhere' failure of seed-key exchange and enable fleets to take control of authorization for cyberphysical functions on their ECU and trucks.

Stream Ciphers
One-Time Pad (OTP) – the only proven secure encryption scheme
Uses random key-stream, of length equal to or greater than the message
Then combine key-stream with message (assume XOR)
Stream Ciphers – approximate the OTP
Expand short key into pseudo-random keystream
Then XOR (⊕) (^)
e.g. RC4, Salsa20, FISH
note: IV – initialization vector. It shouldn't need to be secret
IV + key
seed
RC4
keystream
Plain text
Cipher text
11
native encoding, right? So we're going to talk about modern crypto.
Stream ciphers all operate on this concept of
Automated and Connected Mobility
USDOT 644415

Summary

Telematics devices can control vehicle components, but there are limitations and protections in place, like the seed-key exchange, to prevent unauthorized actions. Some newer trucks are starting to use more secure methods, though widespread adoption will take time.

NMFTA™
National Motor Freight
Traffic Association, Inc.

CYBER

1001 N. Fairfax Street Suite, 600
Alexandria, VA 22314-1798
(866) 411-6632
www.nmfta.org