J1939-based networks vulnerability to Address Claim Hunter cyberattack

This article explores a particular weakness in CAN networks based on SAE J1939, which use the self-configurable address mechanism. Mitigation strategies are given to eliminate the vulnerability from an Address Claim Hunter cyberattack.

Cybersecurity in control systems is now receiving a lot of attention. A lot of the network technologies that are successfully used in many control systems have been found to be susceptible to attacks from malicious parties. This article explores a particular weakness in such J1939-based CAN networks as:

- SAE J1939 for trucks, buses, heavy-duty vehicles
- NMEA 2000 for marine applications
- ISO 11783 (Isobus) for agriculture vehicles
- RV-C for recreational vehicles

There is also a number of other J1939-based higher-layer protocols that have been implemented in practice. Using J1939 mechanisms as a basis, these may also have the described vulnerability.

J1939-based networks using the self-configurable address mechanism for claiming a source address enjoy the ability to automatically set themselves up with no user intervention by a defined plug-and-play method. There are 252 or more unique source addresses available, and each device will attempt to claim a unique one of these dynamically. If a device is not able to claim a unique source address, it signifies this by a "Cannot Claim Address" message and then does not participate in any further network communication activity. Whilst this feature provides a lot of flexibility, it also means that devices that support the self-configurable address feature are susceptible to an attack by an Address Claim Hunter algorithm, resulting in a "denial of service" (DoS). Such attacks can leave many devices disabled or at worst case disable the entire network. Depending on how safety-critical the devices on the network are, the outcome could at a minimum be an annoyance or endanger life.

The particular weakness

The first studies known to report a vulnerability in the SAE J1939 Address Claim functionality was in 2018 [1, 2]. They found that the dynamic address claim mechanism could be used to upset the network. However, testing carried out by the author on a random selection of devices shows that this situation is in fact more serious, and most were susceptible to invalid Address Claim messages (i.e. those with invalid fields, that should not be allowed on the network).

This particular weakness in J1939-based networks involves the following steps:

- Gain access to the CAN network so that a malicious algorithm can be deployed;
- Disable a device (e.g. a water speed sensor in NMEA 2000 network) using an Address Claim Hunter algorithm;
- Claim the device's old source address on the network and spoof the network by sending incorrect measured values (e.g. vessel water speed over the NMEA 2000 network).

To be able to attack one of these networks, the attacker just needs to be able to access the CAN network. Examples of these include:

- Physically add small device whose aim is to disrupt network (e.g. see Figure 1);
- Putting a USB key into a PC on the vessel. If the PC itself can reflash or reconfigure an ECU (electronic control unit);
- Via IoT-connected or Internet-connected type device.

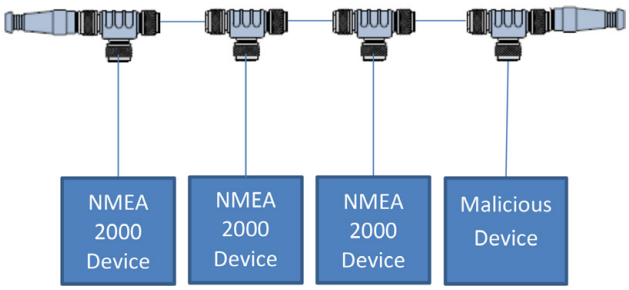

Figure 1: Typical installation for NMEA 2000 (Source: Warwick Control Technologies)

Figure 1 shows the typical configuration of an NMEA 2000 network in which off-the-shelf cables and connectors are simply screwed together via M12 connectors of the appropriate genders. It is easy just to add a T-connector and add the malicious device. NMEA 2000's easy wiring is an advantage for installation but also an advantage for hiding a malicious device behind a panel. Other networks such as J1939 on trucks could also easily have a malicious device added in secret.

There is no standard mechanism for detecting this and therefore the likelihood of this succeeding is quite high. An example of this could be that a malicious device could be installed on a vessel and wait for a trigger to occur before executing the attack. This could be a vessel location, speed, etc. When the trigger conditions are met, then the attack is initiated.

SAE J1939-based networks and address claim

The J1939-based networks support dynamic address claiming so that each ECU claims a unique source address. This feature is very flexible so that devices can be easily added to ▷

a network. However, this functionality is also vulnerable to a cyber-attack that can stop some or all nodes from working.

There are a few different address claim mechanisms defined in SAE J1939-81 for network management. The final of these is concerned with dynamic addressing and referred to as "self-configurable address ECUs", which enables a plug-and-play functionality. If two ECUs have the same source address, the clash is dealt with and the process re-assigns each source address automatically.

Whilst address claiming is taking place, a device or ECU cannot send its normal PGNs (parameter group numbers) onto the CAN network, therefore the system is disrupted at this time. Arbitration when two nodes claim the same source address is dealt with using the NAME field (or Address Claim field in RV-C), which is the 8-byte data field of the address claimed message. The lower numerical value of this 64-bit value wins the address claim and, in theory, a data field with all zeroes has therefore the highest priority and will always win the claim for a source address. The data field with all zeros (e.g. 0000 0000 0000 0000) is however an invalid setting. The following explains why. The NAME or Address Claim field across the four networks is compared in Table 1 to Table 4.

Table 1: SAE J1939 – NAME convention (Source: Warwick Control Technologies)

Arbitrary Address Capable	Industry Group	Vehicle System Instance	Vehicle System	Reserved	Function	Function Instance	ECU Instance	Manufacturer Code	Identity Number
1 bit	3 bit	4 bit	7 bit	1 bit	8 bit	5 bit	3 bit	11 bit	21 bit

Table 2: ISO 11783 – NAME convention (Source: Warwick Control Technologies)

Self Configurable Address	Industry Group	Device Class Instance	Device Class	Reserved	Function	Function Instance	ECU Instance	Manufacturer Code	Unique Number
1 bit	3 bit	4 bit	7 bit	1 bit	8 bit	5 bit	3 bit	11 bit	21 bit

Table 3: NMEA 2000 – NAME convention (Source: Warwick Control Technologies)

Reserved (set to 1)	Industry Group	System Instance	Device Class	Reserved	Device Function	Device Instance (Upper)	Device Instance (Lower)	Manufacturer Code	Unique Number
1 bit	3 bit	4 bit	7 bit	1 bit	8 bit	5 bit	3 bit	11 bit	21 bit

Table 4: RV-C – Address claim field (Source: Warwick Control Technologies)

Arbitrary Address Capable	Compatibility Field			Reserved	Compatibility Field	Function Instance	Node Instance	Manufacturer Code	Serial Number
1 bit	3 bit	4 bit	7 bit	1 bit	8 bit	5 bit	3 bit	11 bit	21 bit

The first part to examine why all zeroes in the Address Claim field is invalid is to look at the left-most bit, which is called "Arbitrary Address Capable" in SAE J1939 and RV-C. This should be set to 1 if to correctly indicate that the ECU supports self-configurable addressing. In NMEA 2000 it is called "Reserved" and should always be set to 1. For NMEA 2000, the "Industry Group" will always be set to 4 (which means a marine network). In SAE J1939, the "Manufacturer Code" of 0 is not allowed and is a reserved value. This means that a NAME field set to all zeros should not occur on these networks in practice. However, many devices in the market will lose the address claim process to a NAME field including all zeroes. According to NMEA 2000, Appendix D (D 4.3), NMEA 2000 does not support an unknown or not available state or value for any of the NAME fields. However, from testing carried out it is clear that this is not the case.

Address Claim Hunter algorithm and impact on a self-configurable device

The Address Claim Hunter algorithm is a simple method to force one or many devices from their source address so that they eventually run out of source addresses to claim. This results in the affected devices to not be able to claim an address, issue the "Cannot Claim Address" message and then no longer participate in (NMEA 2000) network communications. It is possible to use this method to attack all devices (all source addresses) or a specific manufacturer code. Example algorithms 1 and 2 illustrate the simplicity of this approach.

Example algorithm 1 running in malicious device

If (Address Claim Msg Received)
THEN Send Address Claim Msg with
NAME 00 00 00 00 00 00 00 00

The execution of the example algorithm 1 would trigger a sequence of events as shown in Figure 2. The process starts with an attempt by a device (device under attack) to claim source address (SA) as 0. This device is then attacked by a malicious device, which claims SA=0. Then the device under attack attempts to claim addresses 1 through to 251, but each time the malicious device claims the source address using a higher-priority NAME field. The process ends with the device under attack having tried to claim every possible source address, issues a "Cannot Claim Address" message with source address = 254. It then takes part in no further network activity. Once this has happened, it is usual that some kind of external intervention is needed to reset the device such as an ignition/power cycle.

Example algorithm 2 running in malicious device

Another Address Claim Hunter algorithm for an example attack on a fictional Warwick device is shown in Figure 3. This has a simple approach to attack a particular device manufacturer, e.g. send ISO request for address claimed to all devices:

If ((Address Claim Msg Received) AND (Manufacturer Code is Warwick))
THEN Send Address Claim Msg with
NAME 00 00 00 00 00 00 00 00

The result of this attack is that a device under attack:

- Will try to claim new source addresses thus upsetting the network;
- Whilst claiming a new source address, all control PGNs will normally be suspended, because the device does not know which source address it should be using and receiving devices do not know which source address to expect to receive the PGNs from;

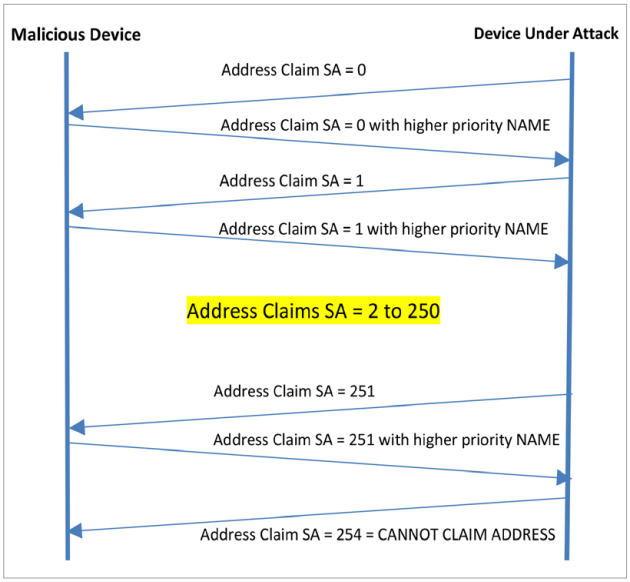

Figure 2: Address Claim Hunter algorithm 1 sequence (Source: Warwick Control Technologies)

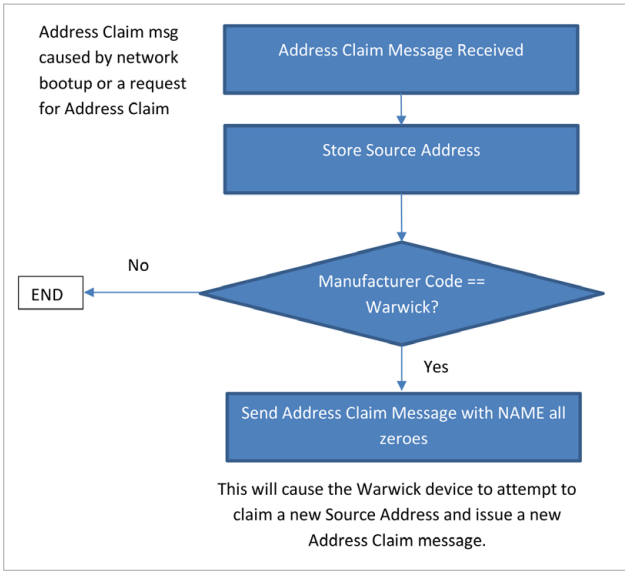

Figure 3: An Address Claim Hunter algorithm 2 (Source: Warwick Control Technologies)

- Once all possible source addresses have been tried by the device, it will issue a "Cannot Claim Address" message (on the null address FE_h) and cease all communications. Usually, the only way to make this device to go online again is some kind of operator intervention.

Potentially the severity of this is dependent upon the type of device that is attacked. For example, does your system remain safe if it uses GPS location or water speed? What if a system providing Thruster feedback information is taken down, what will the system do?

Address Claim Hunter followed by a spoof attack

It is possible to use the Address Claim Hunter algorithm to spoof the network. The process for this is to take the device down using one of the previously described Address Claim Hunter algorithms. Once the device has been taken down, spoof PGNs can be sent, potentially using incorrect values with the intent of sending malicious damage. For example, actual vessel speed could be 3 m/s when it is actually 0 m/s.

Possible protection mechanisms

Protecting proposals outlined in this clause are by no means exhaustive but merely some initial suggestions for designer to consider.

NAME and Address Claim field plausibility checks

Here are some recommendations of plausibility checks that can be made on the NAME field:

- The fields "Reserved" (NMEA 2000), "Arbitrary Address Capable" (J1939, RV-C), and "Self-Configurable Address" (ISO 11783) should equal 1. This is the easiest of checks to carry out. In NMEA 2000, two of the fields in the NAME field are nominated as "Reserved" and should be set to 1.
- Creation of an Allow/Deny list of manufacturer codes, function code, and class: The more sophisticated protection can be achieved by a simple plausibility check of the fields "Manufacturer Code", "Function Code", and "Class" within the NAME field. A vessel manufacturer will know which combinations are valid for a specific model and from the NMEA organization a list of certified products and their attributes is available so that these can be cross-checked for plausibility using a combination of Allow/Deny lists. Upon receipt of an address claim message, it would be possible to check which combinations are valid from the published NMEA list of certified products. This approach reduces the openness, interoperability and plug-and-play capabilities of the NMEA 2000 protocol. Devices would need a firmware update to be able to accept a newly fitted device. However, this could be an important feature for safety-critical systems.

Fixed address for safety-critical devices

In SAE J1939 a number of devices have recommended fixed source addresses, e.g. source address 0 for the engine. Such devices do not take part in any dynamic source address assignment activity. There is usually a range of source addresses that are reserved for devices that take part in the dynamic source address assignment. As the networks grow with the addition of new PGNs considerable for safety-critical systems (e.g. electric propulsion, steering controls, etc.) then a limited area of recommended fixed addresses would protect such devices from attacks such as the Address Claim Hunter.

Wait then recover

A way for a device that "Cannot Claim Address" could be to wait for an application-specific time and then attempt to recycle again. The trigger could be a prompt on a mobile field device or tablet to allow user intervention or some automatic application software triggering to lead to an attempt to claim an address again (e.g. searching for a gap using ISO request).

Address claim NAME tracking

Apply an additional rule to the address claim process, e.g. has the same device (NAME) made another address claim, when no other device has requested that address? For example, Device A has address 10, it receives an ISO address claim from a device with NAME 00000000_h, which ▷

Device A relinquishes and gets an address 11. It then receives another ISO address claim from a device with the same NAME 00000000_h for address 11, but no other device requested the address 10, so it rejects the address claim and transmits a new alert PGN for “Suspicious Network Activity Detected”. Therefore, a device would simply need to remember its last valid CAN address, the NAME of the device that requested it and if any other device has requested its last valid CAN address. This is a bit of an overhead but should be easy to implement.

Conclusion and recommendations

This article has highlighted a particular vulnerability that the J1939-based networks have to a cybersecurity attack that exploits part of the protocol that deals with dynamic address claiming for self-configurable ECUs and devices. The dynamic address claim feature is one of the benefits of these protocols that allows a plug-and-play type functionality for adding new devices to the network. However, it has been shown that this can be exploited and result in a complete network shutdown for susceptible devices. The impact of this can range from being an annoyance through to being a serious safety concern as these networks being used increasingly for more important control applications. Not all J1939-based implementations will be susceptible. The susceptibility will depend upon how the dynamic address claim functionality is implemented. The good news is that the implementation of some additional checks and balances can reduce the risk. Designers of J1939-based systems should consider implementing various address claim plausibility checks to ensure that this weakness cannot be exploited.

Author

Dr. Chris Quigley
Warwick Control Technologies
enquiries@warwickcontrol.com
www.warwickcontrol.com

References

[1] Murvay P.S. and Groza B. (2018); "Security Shortcomings and Countermeasures for the SAE J1939 Commercial Vehicle Bus Protocol," in IEEE Transactions on Vehicular Technology, vol. 67, no. 5, pp. 4325-4339, May 2018

[2] Daily J. (2018); “Introduction to SAE J1939” Cybertruck Presentation, page 124

- SAE J1939-81, J1939 network management
- ISO 11783-5, Tractors and machinery for agriculture and forestry — Serial control and communications data network — Part 5: Network management
- NMEA 2000, Specification package v. 3.0
- RV-C, Recreation vehicle communications, clause 3.3.