AVCMDS: Autonomous Vehicle Cybersecurity Manufacturer Disclosure Statement

Charles Wilson
Principal Engineer, Cybersecurity Development Lifecycle Practice

2021-07-19

Category: security-supply-chain

Tags: security, cybersecurity, autonomous vehicles, supply chain, AVCMDS, manufacturer disclosure statement

In my previous post, **Turtles All the Way Down: Security at Every Level**, I made the case for ensuring that every participant in the supply chain addresses the cybersecurity of their contribution to the system. In this post, we'll look at the first step toward making that possible.

Perfect Information

Chess is a game of **perfect information** [1]. That is to say that there is no information hidden from either player. This differs from games of **complete information** [2], where players have only a behavioral knowledge of each other. For example, in the board game Battleship, the mechanism of play is fully known, but the initial placement of pieces is not. The inverse of **complete information** is **incomplete information**, where players possess private information. Poker is one such game.

From a functional standpoint, we can usually get by with complete information regarding our supply chain. It suffices to understand how our suppliers and their products will behave. This is not the case when dealing with cybersecurity.

The realm of cyber is one in which the adversary probes and ruthlessly exploits any weakness in a target's defense. Without knowledge of the possible points of exposure present in the supply chain, we put ourselves at unnecessary risk. Cybersecurity does not simply have an interest in perfect information, it requires it.

But how do we get from a complete information world to a perfect information world?

Reactive Cybersecurity

One could argue that cybersecurity came about as a reaction to people abusing computer-based systems. As such, the security tools available at the system level far outnumber those focused on the component level, both in number and maturity.

Although it's possible to apply an attack surface analysis (ASA) to any component, or at any level of integration, we tend to apply it only at the system level. The same holds true regarding penetration testing. Threat modeling is slightly different in that it requires that we have knowledge of the design and data flow, but these aren't always available.

We're Not Using the Right Tools

There's also a problem with these tools. They are applied after the fact. If we were looking at the supply chain from a purely mechanical standpoint, we would put out a request for quote (RFQ) with the specifications for the component we needed. We would request and compare data sheets to determine whether the baseline requirements were met. From there we would go into greater depth prior to committing to a supplier.

We don't do this with cybersecurity. We acquire the component, and then assess its security. Why? Because we don't have a standard data sheet for cybersecurity.

Safety Data Sheets

If you've worked for any major manufacturer (from any industry), your on-boarding probably included training on how to work around hazardous materials. This includes an understanding of at least some elements contained in the **Safety Data Sheets** [SDS] (formerly **Material Safety Data Sheets** [MSDS]) [3]. The following is from the OSHA brief on the SDS [4]:

> *The SDS includes information such as the properties of each chemical; the physical, health, and environmental health hazards; protective measures; and safety precautions for handling, storing, and transporting the chemical. … In addition, OSHA requires that SDS preparers provide specific minimum information as detailed in Appendix D of 29 CFR 1910.1200. The SDS preparers may also include additional information in various section(s).*

Although we can't trace manufacturer disclosure statements back to Middle-Earth [5], we can trace them back over 4,000 years to Egyptian tombs, where we find descriptions of materials, sources, storage, and application procedures for pharmaceuticals [6].

MDS2

A standard data sheet for cybersecurity is not a problem that no one has considered. In fact, a very good solution comes to us from the medical device industry. It's called the **Manufacturer Disclosure Statement for Medical Device Security** (MDS2).

The MDS2 covers numerous topics, including:

- Personally Identifiable Information (PII)
- Auditing
- Communications security
- Updating
- Remote access
- Active countermeasures
- Authentication

Each area is examined in detail. The result is a highly expressive view of the cybersecurity posture of the supplier.

AVCMDS

But isn't this highly medical-centric? Can it even be applied to autonomous vehicles?

Motional used the MDS2 as our starting point. Fortunately, the National Electrical Manufacturers Association (NEMA) makes the MDS2 spreadsheet available on their site and grants the right to copy and use it [7]. We removed the medical-specific bits and added autonomous vehicle-specific ones.

We are making this AV-specific spreadsheet available on the AVCDL GitHub site. As with the AVCDL itself, we hope that the community will engage with this material to establish a consistent means of exchange for this information. The AVCMDS spreadsheet can be downloaded here.

Function Follows Form

So how do we use the information in the AVCMDS? There are several ways the AVCMDS answers can be used. They can be used to establish the cybersecurity posture of the supplier today. Not what they promise, but what they do.

They can be used to compare multiple vendors bidding on the same component. They can serve as the basis of discussion into required features and how to best attain them. They can point to security deficiencies in the component. They may even point to enhanced functionality not previously considered for inclusion in the final product.

Almost Perfect

Although the AVCMDS alone doesn't get us to having perfect information, it is a major step forward. Hopefully though, this post has motivated the use of the AVCMDS as a first step toward better supply chain security, and by extension, the safest possible AVs.

In the next post in this series, we'll examine why knowing a supplier's cybersecurity maturity is important.

References

1. **Perfect information**
   https://en.wikipedia.org/wiki/Perfect_information
2. **Complete Information**
   https://en.wikipedia.org/wiki/Complete_information
3. **Safety data sheet**
   https://en.wikipedia.org/wiki/Safety_data_sheet
4. **Hazard Communication Standard: Safety Data Sheets**
   https://www.osha.gov/sites/default/files/publications/OSHA3514.pdf
5. **Middle-earth**
   https://en.wikipedia.org/wiki/Middle-earth
6. **Development of Material Safety Data Sheets**
   https://jrm.phys.ksu.edu/Safety/kaplan.html
7. **Manufacturer Disclosure Statement for Medical Device Security**
   https://www.nema.org/standards/view/manufacturer-disclosure-statement-for-medical-device-security