Traceability: Making the Case for Certification

Charles Wilson, Principal Engineer, Cybersecurity Development Lifecycle Practice

11/3/20 10:47:00 AM

Category: security-certification

Tags: security, cybersecurity, autonomous vehicles, certification, ISO 21434

In my post, **Certifiably Secure: Does It Matter?** [2], I addressed the question of why we get a product certified. In this one I'd like to address one of the main techniques used to make the case for certification.

What is Traceability?

I was going to drop in the IEEE definition, but it's so torturous that I'm just providing a link at the end of the post [1]. Instead, allow me to quote from the esteemed Inigo Montoya,

"Let me explain … no, there is too much. Let me sum up."

Traceability gives us the ability to assert that the choices made and actions taken can be linked back, in a continuous fashion, to one or more fundamental assertions (policies).

Certification

Traceability is integral to certification. It is understood that safety-critical cyber-physical systems will fail. Because of this, we need to be able to trace the failure both in terms of the system and the processes back to their root. Then, we need to take corrective action.

This may include both technical (hardware / software) and human (decisions) changes to the system and process. Without traceability, we will not be able to assert that decisions were made based on sound principles or that the system was constructed according to both the design and following best practices.

How Do You Trace?

Traceability is a large subject. For example, within the domain of software requirements management, requirements traceability is considered a sub-discipline.

In the case of autonomous vehicle development, we must establish traceability from inception through decommissioning. This means we must be able to trace things including (in no special order):

- Non-functional (security) requirements selection
- Linking of security requirements to functional (product) requirements
- Design review feedback
- Tool usage
- Accepted threat disposition
- Tool use tracking
- Tool settings choices
- Static and dynamic analysis issue disposition
- Penetration test issue disposition
- Phase gate transitions
- Incident tracking
- PII tracking
- Artifact manifest and archiving

If that (arguably abbreviated) list makes you uncomfortable given the topic, don't feel bad. The implications are pretty far-reaching. Consider the following:

> A failure occurs in a deployed system. Analysis shows that there was a security incursion, and that one result of the incursion was a failure in the system. A root cause determines that an open-source component was leveraged in the incursion. Additionally, it was discovered that there was a known issue with this component and that this issue surfaced during fuzz testing. However, the triage of the issue determined that the rank and risk was sufficiently low enough to disposition the issue as not needing to be addressed.

Take a moment to list all the processes and tracking that would have had to be in place in order to provide that traceability.

Where Do You Start

The short answer is anywhere.

Let's assume that you're coming to this whole certification thing for the first time. Maybe you've got a few products under your belt. Maybe those products have involved both hardware and software. Maybe those products have had hundreds of people in multiple locations involved. Maybe not.

Look at your processes. Look at their inputs and outputs. Now, wherever there is a decision that a person must make, you need to put a tracking system in place.

Wherever you use automation, document the choice of control plane and settings. Create and document the process for tool selection and qualification.

Document tool use. Automate the process of verifying that the tools used were those you qualified. When you do reviews, ensure that there is a way for the corrective actions to be fed back into the design documents.

All of these are individually manageable activities. All of them are necessary.

Are We There Yet?

Probably not. At least not on the first pass. The good news is that these steps are additive. The more you can do, the better the process becomes. One of the pervasive impacts of implementing traceability is that people become more aware of the decision-making process. Hopefully this leads to more thoughtful choices and better products.

References

1. **ISO/IEC/IEEE 24765:2010(E) - Systems and software engineering – Vocabulary**
   https://ieeexplore.ieee.org/document/5733835
2. **Certifiably Secure: Does It Matter?**
   https://github.com/nutonomy/AVCDL/blob/main/background_material/blog%20posts/certifiably%20secure%20-%20does%20it%20matter.pdf