Purpose-driven Security

By Charles Wilson, Principal Engineer, Cybersecurity Development Lifecycle Practice

11/3/20 9:06:00 AM

Category: security-general

Tags: security, cybersecurity, autonomous vehicles

A Bad Example

In 2014, St John Ambulance [1] posted a short [1m12s], amusing video encouraging people to take a reasonable approach to keeping one's children safe. Ridiculous to be sure, but this is how we tend to approach security — all or nothing.

Cheese Sandwich in a Bank Vault

In the security realm, we see this approach all the time. I attribute the use of military-grade security measures for every issue to two things. First, as a discipline, security hasn't been around for all that long relative to how long we've had computers. Second, we didn't take security seriously for a really, really long time.

As a result, most people don't have an appreciation for either the security domain, or the tools and techniques available to address issues. So, when a problem is perceived, people reach for the biggest hammer in the toolbox and swing it as hard as they can to ensure that it's dealt with once and for all.

There's a price to pay for this approach, namely time and power. Any countermeasures we apply will consume both.

It takes time to verify that the data is the size the message says it is, that we haven't seen the message before, and the like. If we add cryptographic protection into the mix, we have far greater costs. When you use the big hammer approach, you end up paying a high price for a level of security that could have been attained with a lesser set of controls (law of diminishing returns [2]).

As a result, your system must be more computationally capable. This leads to the need for more power to operate it. The big hammer approach can also adversely impact the data rate since it takes time to perform the cryptographic operations protecting the data. This is time which would have been available to other processes within the system.

Balance

Ideally, you only want to pay for what you need. This is where purpose-driven security comes in.

In the case of autonomous vehicles, the most important thing is the safety of those in and around the vehicle. When we establish security controls, it should be to achieve that goal. With this as a guide, we can provide guidance as to what does and doesn't need to be done. From there, we look at specific situations and recommend the type and strength of controls needed.

This is not to say that no consideration is given to non-safety-related areas of the system. Such controls are simply not as important as those directly impacting safety. For example, someone losing their radio presets is basically at the bottom of the scale of things we need to worry about.

Action

In practice, we use purpose-driven security to guide our efforts. Cybersecurity groups will always be far smaller than the design and development teams. Applying the lens of security in support of safety enables us to focus on the things that matter the most. In this way, our emphasis is on providing feedback to the issues with critical impact. We do so by applying methodologies that help us intentionally sort through the many possible issues.

In upcoming posts, we'll address what those methodologies are and how they support us.

References

1. **St John Ambulance**
   https://sja.org.uk
2. **Diminishing returns**
   https://en.wikipedia.org/wiki/Diminishing_returns