All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

How deep is the problem?

I saw a really good presentation by Ralph Langner on Youtube about nuclear safety systems and their manipulation by cyber attack on the non-safety systems. He made it seem simple, although there remains exponential complexity in the number of paths feasible at some level of granularity. At a conceptual level, however, it was just right; start at the bad consequences, find the paths to them by examining design constraints, violate the design constraints, win.

However, the analysis of the paths to violating the design constraints made various inherent assumptions about the level of sophistication. The problem is not solved once you identify all of the normal operational methods for causing the mechanisms to violate design constraints, which is what Ralph essentially did, and this goes to the simplicity issue.

Abnormal (to most) methods

In the mid-1990s I decided to make a list of the attack methods against systems. I published it, it's available online at all.net in the security database, and thee is even automated analysis to support understanding these elements to a limited extent. That list had (has?) about 94 methods. To date, the cybersecurity community has explored perhaps 30 of them in enough depth to be seriously considered.

Let's take a few examples (I stopped at the first “e” and ignored some good candidates; the list goes through “w”):

- **below-threshold attacks:** Use multiple attacks that are below the perceived threshold of import.
- **cascade failures:** Cause failures that cause other failures that cause ...
- **collaborative misuse:** Use several collaborators to affect the desired result.
- **electronic interference:** Use waveforms to attain a result.

It doesn't matter how much analysis you do of the obvious paths to a failure. Just taking one example, electromagnetic interference may be limited by the power usage of each component of each system as it varies over time. Suppose we coordinate computations in thousands of components so that they produce, as a side effect, waveforms that combine at nodes in specific places at specific times in the surrounding region of space, to generate higher electromagnetic fields. Suppose we use these to induce currents in connections that in turn, because of the physicality of the systems they reside in and time time function induced by our computations, produce increasing voltages over time through positive feedback. At some point, the system they reside in will break because the voltages or currents will exceed design constraints. We then do this in particular sequences to multiple components to induce multiple component failures designed to induce undesired system behaviors.

I will assume for now that at the level of the specifics, nobody knows how to analyze all of the potential sequences of computational combinations and all of the signals they may induce in all of the components that compose any sophisticated overall composite.

Copyright(c) Management Analytics, 2016 - All Rights Reserved

The simplicity principal

The basic problem with using information technology for safety or protection against high consequence outcomes from malicious acts by knowledgeable will-funded threat actors is that the quantity of event sequences and the potential complex interactions between components forming the composite is beyond the capacity to analyze. The simplest commonly used modern computers have many millions of components and many more instructions encoded in them, producing unfathomably large potential sets of failure modes. The fact that these can often be invoked after arbitrary delays and under conditions dictated by the threat actor, that mixed mode attacks involving multiple insiders acting on concert with outsiders, the supply chain issues associated with the entire lifecycle of all the components and the composite they come together to form, and the lack of an approach to deal with the complexity effectively makes any attempt at perfection doomed to failure in practice. And to be clear, at the end of the day, the best we will likely ever be able to do is turn the attack and defense “game” into a force against force exercise with force associated with analytical capability under deception.

Come the simplicity principal. There is a reason that the best safety systems are based on the physics of the overall system. For example, a gravity-fed system that fails into a safe mode by no longer stopping water from falling from a high place to a low place under reasonably well defined conditions that are directly sensed and acted on by the mechanisms holding the water back and redundant in that they are separate and different, makes for a very hard-to-defeat system. An electromagnet holding up a control rod that, if the temperature rises above some threshold, melts the wire sending power to the electro part of the magnet, will almost certainly result in the control rods falling into the reactor and slowing or stopping the reaction.

This can of course be defeated by altering the mechanics of the system, which is why redundant systems and separation of duties will prevent conspiracies of less than a specified size from defeating the mechanics of enough of the components to cause the composite to fail to shut down. And it can of course be defeated by altering the way gravity works in the vicinity, but if gravity stops working, the nuclear power plant is not going to be our biggest problem. And a large enough explosive properly placed will likely cause a failure, but then the designs of such facilities are often such that the necessary explosion will be of even higher consequence. And mission impossible style attacks with enough resources properly directed may eventually cause it to fail in any case. But cyber attack will be very difficult to exploit in causing this mechanism to fail because, unless the attack alters the surrounding environment or is done at the design phase, the operation is essentially unalterable.

Conclusions

I am not intending to critique Ralph's talk. I come to praise Langner, not to bury him. But I want to make sure that, as a community, we never get too full of ourselves or believe that we have the solution to security in the face of malicious, intelligence, concerted, well resourced threat actors with specific objectives.

There is no, and likely can never be any, perfect defense. There will always be some set of people sufficiently skilled and motivated to defeat any system, and even if, for some period of time, that is not true, it will be true at some later time. Our saving grace is, in some sense, that everything takes time and leaves tracks. Some old sayings come to mind. Protection is something we do, not something we buy. Ain't a horse that can't be rode, ain't a man that can't be throwed. Evil flourishes when good men do nothing. Eternal vigilance is the price of peace.

Copyright(c) Management Analytics, 2016 - All Rights Reserved