Steve Roehl

SE4930-001

1/25/2012

I read “Stuxnet: Dissceting a Cyberwarfare Weapon” by Ralph Langner. This article explained what Stuxnet is and how it worked. Stuxnet was one of the first cyberwarfare weapons used. It didn’t do what a normal attack would it. Instead of trying to steal information and hi-jack a computer, it was made to destroy industrial equipment. It did this by targeting the controllers that control this equipment. It also was unlike a normal attack because it didn’t try to be as wide spread as possible. Instead, it limited itself to a very specific target, the Natanz uranium enrichment plant in Iran. Most attacks try hard to spread themselves as large as they possibly can, but this attack used went through a bunch of checks to make sure that it was only targeting the control systems that it wanted to destroy.

From this article I learned that we cannot think that any system is secure. We must think about anything that we build as having the possibility of being attacked. This attack was able to succeed because of a variety of failures. First, there was a failure by Microsoft which is what allowed the attack to spread and get to its target. Then there was a failure by Siemens who manufactured the controllers. They used an insecure method of communicating to the control in the form of a DLL. They also did not build more checks into the controller itself. The article points out, however, that because the controller must be a real time system it has a little resources to be spent worrying about

attacks. This means that the attack needs to be prevented or at least found before it makes its way to the controller. If this were the case then a technician would be able to shut down the system before there was any damage. Before reading this article it never really occurred to me an industrial system like this must be monitor for attacks. The article points that this type of attack even goes against the common confidentially, integrity, and availability thought. This attack did really nothing to affect these as we see them. It could have effected integrity in the fact that it loaded malicious code, but it did not really change any data.

This article brought a lot of questions to my mind. The biggest question is what are these controller manufactures doing to prevent more attacks like this. We know this was a rather targeted attack, but what if some rogue organization were to attack a lot of American manufactures with this type of attack. They could destroy billions, maybe trillions, of dollars worth of industrial equipment. That would be a huge blow to the American economy and one that I think we need to think about. I understand that these are real time systems, so what if we were to add more systems to the real time system. Perhaps any data that entered the controller could be checked by a different system before being relayed to the controller. This could add some security that a normal real-time system cannot.