Matthew Boeck
1/20/2012
SE4930
Dr. Schilling

Article Review #3 – Silver Bullet Podcast #64

This week I chose to listen to a podcast. The podcast was the silver bullet podcast, show 064 and was an interview with Markus Schumacher. The link for this podcast can be found at http://www.cigital.com/silver-bullet/show-064/. The podcast began by talking about the dynamic differences between a small startup company versus a large company. Markus talks about how different it is working for a startup company compared to his prior company, SAP. From here he goes onto details about how his new startup company, Virtual Forge, built a code scanning tool for SAP's ABAP code. ABAP code is basically a scripting language, and the tool that Virtual Forge wrote, is a code scanner for all of this code. It can find defects pretty easily, and is highly automated. This is comparable to Fortify and other tools developed by HP.

From here the podcast talks about false positives and how often they occur during code scanning. Markus talks about how his tool can prioritize found defects and exploits. The tool is written to help people find out what to do first, what to fix first. One interesting concept that I learned from this podcast is the concept of static analysis. Static analysis is where the effect of an immediate change to the system is calculated without respect to the longer term response on the system to that change. The complete opposite of this is dynamic analysis.

Towards the end of the podcast, Markus and Gary ask the question, "Do security engineers know about secure design patterns?" This was an interesting discussion. Gary and Markus talk about how security engineers are good at breaking things, but not at fixing things or preventing things from being broken. This is because they are not developers. They then mention that developers are good at coding, but not as good at the security side of things. This is an interesting paradigm. I would like to be a security engineer in the future, but having an intensive background in development, I think I would make a good security engineer.

From this podcast I learned about ABAP and the code scanner that Virtual Forge wrote. I also learned about static and dynamic analysis. I didn't learn too much from the end of the podcast that I didn't already know, but it was an interesting discussion. I enjoyed listening to each side of the "Do security engineers know about secure design patterns?" discussion.

If I would like to become a security engineer in the future, I believe that I can do this best by not losing the developer knowledge I currently have. I believe that I can be a highly effective security engineer if I know how code works. Testing and finding exploits works best by knowing what is going on behind the scenes. On the converse side of things, I believe that I can be a great developer by using the security knowledge I have gained so far. If I am always conscious of the attack vectors and exploits out there, as well as how to exploit them, I can develop more secure software to prevent this. I think I can be good in both positions because of the experience I already have.