James Durand
1/8/2012
SE 4930
Podcast Review

Silver Bullet – An Interview with Markus Schumacher (Episode 64)

This interview had two main security related focuses. The first focus was on code analysis tools. These tools are for finding vulnerabilities in software that are introduced by poor coding practices or lack of knowledge. Markus talked about his company's code analysis tool and how it compares to the industry leader's similar tools. One of the big distinctions to be made is that his tool works for one language and uses expert knowledge of the language to give the best and most in depth coverage of code written in that language.

Many code analysis tools are very generic to work on as many languages as possible. Markus says that this can be a weakness. These tools scratch the surface in terms of finding defects and potential security holes. If this is what is desired then these tools are fine. However using a tool that is tailored to specific language can provide significantly better results and will result in a better designed application. This is fairly intuitive and yet many groups still do not try for language specific tools because it makes the company more flexible.

Markus also gave some of his findings in relation to security holes that they found. Markus reported that there were not really many false positives that his tools tended to find. In general the tool would report a potential security flaw but the developers would say that there is no risk. They gave the analogy of the parent with the perfect child. Parent's always think they have perfect children but in reality the child may be ugly. The same applies to code. The developer will always think their code is perfect and is the best there is but in reality it could be riddled with holes and could be poorly designed. In Markus' opinion these tend to be the worst kind of flaws because the developer may reject them or may not understand why the flaw was there.

The second focus of the podcast was on security patterns. They did not go into details on what a security pattern was in the interview so I did some background research on the topic. What I have found so far tells me that security patterns are specific form of architectural and design patterns specifically designed for handling security problems. One example that they gave in the podcast was the Checkpoint pattern. The idea there is to check the state of things at specific points to make sure that all the security parameters are correct. The real life example they gave was the security checkpoints when entering a country. You need to have your passport and various other papers to enter the country legally; if the credentials do not match then you cannot enter.

This is an interesting concept even though in a way it's not that earth shattering. I think the part I like most is that it's not something that I immediately thought of when learning about design patterns the first time. It makes sense that there are patterns for security. I also find it interesting that these patterns extend to architecture as much as the design phase of a project. I will have to look at more security patterns for my own projects especially as I work on more that are network based.