Marc Anders
SE 4930
Dr. Schilling
Security Summary #2

I listened to “Show 062 – An Interview with Halvar Flake” from The Silver Bullet Security Podcast. This podcast was, as the title states, an interview with Halvar Flake. Halvar Flake founded his own company called Zynamics that focuses on reverse engineering and security analysis. After working within his company for a few years, Google bought it and now employs him.

Before Halvar started his company he spent time creating a program titled bin-dif. This was created in order to determine what was changing in the Microsoft updates. This was at a time when Microsoft was not explaining what was exactly changing, and so Halvar started analyzing the executables. Instead of focusing on the byte code of the exe’s he instead focused on the structure of them. By doing this he was able to find chunks of file that were similar and so could eliminate them. By focusing on the structure rather than what was exactly written down, he was able to eliminate the small differences resulting from different compilers. After this he was able to start using various unstated algorithms to find what exactly had changed.

When asked why developers do not seem to focus as much on security, he stated he thought it was because developers like to create programs, whereas security analysis focuses on the special cases when the program breaks. He also talked about the fact that he does not think that developers focusing on reverse engineering do not have a want to understand the code better, but are forced to because of the lack of good applications to help with reverse analysis.

One code analysis application that he feels needs to be developed is the ability to find architectural defects rather than just programming defects. In order to do this the developer needs to understand the actual architecture and he states that this is very difficult to transfer to an automated process. Also on the topic of code analysis and reverse engineering code, he

expressed his opinion on the two popular ways to analyze code: static and dynamic analysis. He stated that he uses both when they are applicable, and thinks it is ridiculous for an analyzer to only use one type.

When asked whether he thought the complexity of malware was increasing he said that he definitely thought so, and pointed to Stuxnet as an example. He believes that creating malware is much like creating any software application at this point, that large amounts of time are put into planning and designing the attack.

Yet another topic discussed within this podcast was the balancing act of high security and availability. He talked about he fact that companies are finding it more and more difficult to allow access to their employees while keeping sensitive information within the company. If security is put at an extremely high level then it impairs the employees from doing their job, but if the security is too low, almost anyone can access it; hurting the company.