Joe Edmisson

I listened to the 52nd episode of the Silver Bullet Security Podcast from July 21st, 2010. In this episode the host Gary McGraw, interviewed Paul Kocher, the President and Chief Scientist of Cryptography Research. Over the course of this interview they covered a multitude of topics, including whether or not engineer of software systems need to think like the people who are attempting to break into their systems and the decision to put Blu-Ray content protection on the discs instead of the player.

The section of this interview which I found to be most interesting and informative was when they were talking about whether or not defenders need to be able to think like attackers. This idea is one that I had heard before listening to the podcast. The general idea behind it is that for someone to be able to properly defend a system, then they need to be able to understand the mindset of the people who will be attempting to break into the system and deduce the most likely points where entry will be attempted. Paul had an interesting idea about this. What he said was that a major difference between attackers and defenders is the view on their success rates. An attacker with a 1% attack rate is considered successful, while if 1% of attacks get through, then the defender is considered a failure. However he did agree that it is important to understand the basic methodologies which tend to be utilized by attackers. I found it interesting that he feels the defender needs a much broader view of the system than the attacker does. I believe that this will help me to become more proficient at creating secure software because I will be able it will help direct my focus when working viewing my software and architecture from a security standpoint.

Another topic that they spent some time covering was when Paul was working on developing the content protection for Blu-Ray movies. They decided to put it onto the disc instead of the player for a number of reasons, including simplifying the job for player makers, giving studios the ability to adapt to the way attacks change, and keeping the job of protecting the content in the hands of those who want it protected the most. The player maker's jobs were simplified by no longer being solely responsible for protecting the content. The studios became able to adapt to changing attacks by having the ability to change the security on each batch of discs. And since the studios care considerably more about whether the content stayed protected than the player makers, the person with the largest stake became the person in charge of protecting the data. I wouldn't have thought of the last reason, which makes sense because people who have a vested interest in something tend to work harder for it.

All said I found this podcast to be rather enlightening. It was interesting to hear the opinion of someone who has made a sizeable fortune from the software business, and his take on how things have progressed since he started out.