Joe Edmisson

I listened to the 9th episode of the Silver Bullet Security Podcast from December 14th, 2006. In this episode the host Gary McGraw, interviewed Bruce Schneier, the founder and CTO of Counterpane, as well as a bestselling author. Over the course of this interview they talked about the transition from physical security to technological security, digital rights management, and Microsoft’s software security strides.

Near the beginning of the interview they have a discussion about the future of security. The security that they are speaking of is a broad view of security, not simply computer security. Gary brought up that in one of his previous interviews, the interviewee had stated that security was moving away from physical security, guns, dogs, and concrete, as he put it, and moving towards technological security. Bruce agreed that we are in a time where technological security is becoming more and more important. However, he disagreed that the need for the physical security would remain as long as there were physical threats. So rather than replacing physical security, technological security is becoming integrated into physical security. I found this interesting because I had never really thought about the idea that technological security was making physical security less important. After listening to this I began to think over the needs of security, and I feel like he made some good points. Simply because there are my threats in the computer realm doesn’t mean that there are any less in the physical realm.

They also have a discussion about digital rights management, or DRM. Bruce’s opinion on DRM seems to be that the technology behind it isn’t going to be enough to keep it alive. As he puts it, “trying to make digital file not copy-able is like trying to make water not wet”. He believes that the main force behind functional DRM is actually the media companies pushing for laws to back them up and prosecuting people. He goes on to say that people are going to have to look into different avenues for getting digital products to people. This podcast was from over five years ago, and in that time, people have started to do that. Many smaller software developers don’t bother to try to copy protect their work, and rather simply hope that if someone uses it and likes it, they will pay for it. However some companies have also gone in a different direction, and are trying very hard to keep their files from being copied, and generally failing at that.

They finish with a discussion about Microsoft and how they are approaching their own security problems. This conversation basically boils down to Microsoft getting a bad rap due in part to them having such a large market share of operating systems. However, it is also due to the sheer amount of legacy code that they have to support. The amount of people using their software, and the amount of software being used makes it very difficult to stay on top of everything all the time. So it also takes them a large period of time for security practices to get in all versions of code. They also appear to be improving their patching issues.

All around I found the discussion to be rather interesting. Given that the interview was from late 2006, it was also interesting to listen to discussion about things which are still being struggled over today by many companies such as DRM. This is interesting because this conversation was happening before I was thinking about things such as computer security (or choosing a career).