Steve Roehl
2/06/2012
SE4930-001

I listened to the Silver Bullet Episode 70: An Interview with Ross Anderson. He is a professor of security at Cambridge. There were many security related topics talked about in this podcast. They started out by talking about trusted computing. This is where a motherboard would have a chip on it that would only allow it to run signed operating systems. This is very similar to how a game console works with its software. This idea of using signed code for an operating system was brought up before in 2003. Anderson states that he does not think this would be very useful because each government would want to have the ability to sign software. This is so that they can partially control what software is out there and so that they themselves would be able to put out software if they so wanted. He argues that if you grant each country the ability to sign code then malicious code will eventually get signed as well. This seems to be pretty straight forward sense. If enough entities have the ability to sign code pretty soon it will fall into the wrong hands.

He then goes on to talk about the prisoner's dilemma and what happens if this experiment is ran iteratively. They found that people build a tit-for-tat mentality that makes it so if they get attacked then they want to get revenge against the person. Anderson says this is similar to how security actually works and proves that there is no way to completely prevent security.

Anderson talks about the state of the medical records in Europe. He tells a story

about how in Scotland they released all the records of everyone to anyone involved with health care. Apparently, after not too long a doctor downloaded the records of many well known people and was able to release them to the public. He says that this is why releasing medical records to the entire health system is very dangerous. He makes the claim that this type of information must be compartmentalized so that it is not easy for anyone person to gain all of the information. He claims that eventually records that are de identified will be released to something like Wikileaks and then people will figure how to match the records up to real people's names and then the public will have all of the medical records anyways.

They then go on to talk about how dangerous time in systems can be. If the time or date can be changed in systems and then the system malfunctions and allows an attacker easily in then this can be a very dangerous attacks. They also talk about how financial institutions make transactions in pica seconds and in this small of time an attacker could modify the time very slightly but be able to make a lot of money.

I think the most interesting about this interview was how much it talked largely about people and not technology. I think it is very important to realize that in computer security one of the biggest weaknesses is people. A computer could be designed to never give out a password, but if the user is willing to give up a password then the security of the system is very weak. I think that to be a security expert you must think about how people affect the security.