John Pires

SE 4930

February 4, 2012

Article Review 4 (Free Review):

Silver Bullet Show 070 – An Interview With Ross Anderson

Summary

On the 70th episode of The Silver Bullet Podcast Gary McGraw interviewed Ross Anderson, professor of Security Engineering at Cambridge. In addition to teaching Ross does independent security consulting and has authored several books. This interview covered a wide range of topics and it was difficult to really discern a specific theme; although there was heavy emphasis on how both economics and basic human nature are factored into security design. Gary and Ross begin by discussing the trusted computing controversy. They then move on to discussing some broader aspects of the economic theory behind computer security, specifically using The Prisoner's Dilemma as an example. The economic discussion then slowly shifted over to discussing how human nature can affect security design as well as what the correct role a government should play in regulating markets and computer security. Finally, the interview closed with a discussion on Wikileaks, medical information security, social networking security, timing-based financial fraud, and cyber warfare. As the list of topics suggests, this interview had a very broad range of topics, and much of the information was actually fairly difficult to follow. Overall the interview was very interesting but would have benefitted from restricting the conversation to a few key elements and having a more in-depth discussion of those elements.

Trusted Computing consists of loading hardware with unique encryption keys (inaccessible to the rest of the system) and then using those keys to enforce certain software behavior. The claimed purpose behind this technology is that it will make computers less susceptible to viruses and more secure in general. Ross Anderson however is very adamantly opposed to it for several reasons. In the interview he stated that the main purpose is not in fact security but instead it is digital rights management. He outlines several malicious uses that he believes are the true driving force behind Trusted Computing. First, it could be used to eliminate competition by not allowing competing software and operating systems to run on certain hardware. This is actually true as apparently any computer which ships with Windows 8 will never be able to run any other operating system. Secondly he claims it could be used as a means to perform remote censorship. For instance if someone used a windows tool to create

something then Windows could render it unusable simply by invalidating the key to the software which interprets it. Lastly he says that it simply takes too much power away from the user and owners and puts it in the hands of manufacturers.

The discussion of the economic/human aspect of computer security actually involved high level concepts and terminology and this section was the most difficult to follow. The basic economic idea discussed was that one of the main difficulties in the field of computer security is the fact that it is difficult to have world-wide policies without a global governing or regulatory body. The prisoner's dilemma was used effectively to illustrate this concept. Anderson used it to make the point that every country in the world would benefit from more cooperation rather than merely trying to act in solitary self-interest.

This led into a discussion of the proper role the government should play in regulating and controlling markets. Ross Anderson proposed that governments should play a limited role but still actively promote open platforms rather than allowing them to be restricted through the use of technologies such as Trusted Computing. Additionally Anderson suggested that current policies involving cyber warfare are incomplete and fail to adequately account for the disproportionate usage of civilian based infrastructure as opposed to traditional warfare. Furthermore, he stated that the United State's entire approach to cyber warfare and defense is skewed. Instead of devoting resources to reducing the overall potential for malware the U.S. is merely exacerbating things by concentrating on creating more malware of its own.

What Was Learned

The various discussions between Anderson and McGraw were actually not very informative in and of themselves and centered around personal opinions rather than facts. This is not to say it wasn't interesting, Anderson himself is clearly extremely intelligent and it was fascinating hearing him discuss the economic and human sides of security. Quite a bit was still learned however as I was often forced to pause the podcast and look up material related to the discussion. For instance, I had no idea what the Trusted Computing controversy is, nor had I heard of UEFI (which I probably should have). I was able to read all about the technical aspects of both technologies and after listening to opinions on them from someone like Anderson I believe I have a firm grasp of both the technologies and potential real-world ramifications.

I think I gleaned less from the discussions about economics and human nature as I believe I would require a bit more knowledge in these areas to adequately understand the points they were making; however, I was able to understand the general ideas, which were quite interesting. Finally, I was

introduced to a new security abuse called timing-based attacks. Anderson briefly spoke about how those people who have access to financial software can take advantage of delays in transferring information and perform certain actions either just before or just after some critical piece of information is changed. For instance, if a stock price is about to raise or fall then being able to act a picosecond before that information becomes active could provide an extremely lucrative abuse of the system.

In conclusion this was a very interesting interview although I feel that much of it was a bit higher level than I would have preferred, or at least a bit too much outside my areas of expertise. That being said, I was still able to follow the discussion and never really got lost. Anderson himself is the founder of the entire research domain of the economics of security and it was absolutely fascinating listening to him discuss it.

I think this interview will help in future software development in several ways. First, it provided a new perspective on the economic and human aspects to security. These are factors I had not previously devoted much consideration to but they clearly have a significant impact on computer security. Second, I now have a much better idea of how timing based attacks can be used against systems, especially those that rely too heavily on external clocks or timestamps.

Several questions occurred to me while listening to this podcast. I would like to know more about Trusted Computing. Specifically, I would like to know how much truth there is to the allegations Anderson made about Microsoft using it as a tool to choke out rival operating systems and programs. I would also like to know if there are any documented cases of timing based attacks being used for fraud in the financial industry. I think it would be extremely interesting to learn more about this attack vector as Anderson and McGraw only touched on it.

Works Cited

Anderson, Ross. "SHOW 070 – AN INTERVIEW WITH ROSS ANDERSON." Interview by Gary McGraw. Audio blog post. *Silver Bullet*. Cigital, 31 Jan. 2012. Web. 4 Feb. 2012. <http://www.cigital.com/silver-bullet/show-070/>.

"Trusted Computing." *Wikipedia, the Free Encyclopedia*. Web. 04 Feb. 2012. <http://en.wikipedia.org/wiki/Trusted_computing>.

"Unified Extensible Firmware Interface." *Wikipedia, the Free Encyclopedia*. Web. 05 Feb. 2012. <http://en.wikipedia.org/wiki/UEFI>.

"Ross J. Anderson." *Wikipedia, the Free Encyclopedia*. Web. 05 Feb. 2012. <http://en.wikipedia.org/wiki/Ross_J._Anderson>.