K.J. Grewal
02/07/2012
SE-4930 – Article 4

Silver Bullet Talks with David Rice

IEEE Security & Privacy – Silver Bullet Podcast, Mar. – Apr. 2011

Summary

In this podcast David Rice, the executive director of a strategic consulting firm called *The Monterey Group*, discusses the amount of liability software manufacturers need to begin taking for producing insecure software. He discusses how he first became interested in software security and how he noticed that some configuration settings could be changed to mitigate *some* security vulnerabilities which I thought was interesting. David goes on to state that the software security problem is very similar to the problem that GM dealt with not too long ago with measuring the safety of their vehicles. Additionally, there is no single solution to the software security problem, but this may be resolved by looking at economic incentives in the marketplace since technological solutions will not be enough.

David mentions that most of cybersecurity spending is for cost avoidance. A few companies attempt to use this as an incentive for the creation and use of their tools, but there are thousands of companies that merely don't see it as such. Companies like Google and Microsoft have created their own security tools, but they choose to keep these internalized due to lack of commercial viability and a weak spending market. The lack of demand for consumers of the tools combined with the hold out of tools being released to the public puts us in a loop of having mediocre security analysis tools.

The result is a slow increase in the effectiveness of the current tools out in the marketplace which David believes is not sufficient to address the large systematic failures. This is also due to the fact that it truly inexpensive to create insecure software, but it expensive to produce secure software. David

states, “Anyone can sit down, write a Web app, connect it to a database, and now you’ve got a perfect SQL injection vector (McGraw 9).” To combat this, he proposes that we *invert the market* which will cause the insecure software to be more expensive to produce. As an example David suggests, “Software manufacturers pay the cost of the patch—that’s the private cost—but they don’t pay the cost of patching, which is the social cost. We want to try to reverse that model such that the private cost of producing software, just as the private cost for producing steel, is increased by taking into account the social cost (McGraw 10).” This model will allow software manufacturers to recognize the true cost of production and improve the quality of security in their products. As a result, consumers will benefit.

What I learned

By listening to the podcast and reading through the printed version, I understood the rationale behind why insecure software is so prevalent. Prior to listening to this podcast, I did not realize how software security is so behind in quality when compared to other industries. I believe that this podcast helped me understand the direction in which software security needs to go and what changes can improve security. One question that I still have is what measures can be taken to speed up the widespread process of improving software security throughout the industry?

Bibliography

McGraw, Gary; , "Silver Bullet Talks with David Rice," Security & Privacy, IEEE , vol.9, no.2, pp.8-11, March-April 2011, doi: 10.1109/MSP.2011.38