John Pires

SE 4930

January 10, 2012

### Article Review 3 (Podcast Review):Silver Bullet Show 065 – An Interview With Giovanni Vigna

**Summary**

On the 65th episode of The Silver Bullet Podcast Gary McGraw interviewed UC Santa Barbara professor of Computer Science Giovanni Vigna. Professor Vigna specializes in computer security, specifically intrusion detection, and is the organizer of iCTF (UCSB International Capture The Flag). Gary and Giovanni discuss a number of topics, including Giovanni’s CTF competition, DEF CON CTF, teaching security at UC Santa Barbara, Basic problems with developing secure systems, intrusion detection, black box testing, and interestingly the Trinity of Trouble discussed during lecture.

The interview started with a lengthy discussion of the capture the flag events Professor Vigna participates in, namely DEF CON and his own iCTF. A computer-security capture the flag competition is similar to the real thing except the flag is usually some sort of file on an opposing team’s network and the playing field is the entire competition computer network. In general each team is given the same Virtual Machine server. Each team must then discover and patch the vulnerabilities on the server. Then, in the attack portion of the competition the teams use their knowledge of whatever vulnerabilities they found to attempt to hack into opposing team’s networks. Giovanni’s team actually won the DEF CON competition is 2005, although he was quite modest about it in the interview, assuring Gary that it was due to a lack of competition that particular year. He did seem very adamant about a particular point he made that in security situations tools are important but infinitely more important is working with the right people: “having the right people is everything”.

McGraw and Vigna then went on to discuss some of the basic security problems with modern software development. Giovanni briefly mentioned that one of the biggest problems is that every time a current platform or system is made more secure, for instance windows XP to windows 7, a new one is released that offers a host of new exploits, such as the Android. This led to a brief discussion on the Trinity of trouble, where they discussed the basic concept. It was interesting hearing them directly discuss something covered in class, but the only new content they offered was on how it relates to social engineering exploits such as fake anti malware.

The final topic discussed in the interview was black box testing and specifically the role it should play in security. Professor Vigna stated that the only legitimate use it has is to demonstrate to stakeholders that security is a real issue. If a bug is found it does not tell the testers anything about the overall security and sophistication of system, it only shows that a bug was found. Furthermore it is impossible to get code coverage metrics from a black box test and apparently most black box testing hovers around 12% coverage. He was not completely against black box testing however and said that it is always better than doing nothing. The discussion ended with Giovanni stating that running a few BB testing tools against a system and finding nothing is much better than simply doing nothing and assuming the system is secure.

**What was learned**

This was a very interesting and entertaining podcast. Giovanni Vigna is a very funny person and kept the discourse lively and fresh. I learned a few general security lessons, for instance, the tools being used are far less important than the people using them. Professor Vigna is from Italy he and McGraw had a very interesting discussion on the different culture and mind frames of Americans and Europeans and how it relates to security. I also learned quite a bit about computer security capture the flag and black box testing.

Several Questions occurred to me while listening to the podcast. Firstly I would like to know a bit more about these capture the flag competitions because they seem very interesting. Secondly I really want to know more about the new security problems unique to mobile development as the interview only touched on that topic but did not go into detail. Thirdly, I’m curious as to what sort of automated black box testing tools exist and how effective they are. In conclusion I think I learned a fair amount from this article and it definitely got me thinking about software vulnerabilities in general and testing, which will most likely help my future software development.

Works Cited

McGraw, Gary. "An Interview With Giovanni Vigna." Interview. Audio blog post. *Silver Bullet*. Cigital, 29 Aug. 2011. Web. 21 Jan. 2012. <http://www.cigital.com/silver-bullet/show-065/>.