Cory Bryan

SE 4930

January 24, 2012

Silver Bullet Podcast – Show 60 – An Interview with Neil Daswani

http://www.cigital.com/silver-bullet/show-060/

In this podcast, Gary McGraw interviews Neil Daswani, CTO of Dasient and a former product manager at Google. This podcast was split into distinct sections, each covering a different series of questions.

Neil's Background in Software Security

The interview started with Gary asking Neil about his background in software security. Neil used to work at Google, and now works at Dasient, which he cofounded. They then talked a little about the differences between traditional software and web software security. Neil described some of the steps his company takes in producing secure software, starting at the requirements phase where they analyze security risks, create a threat model, and determine mitigation strategies. Neil mentioned that it is impossible to prevent all attacks, but defense in depth helps.

Security in a startup

Gary then asked Neil about how a startup handles developing secure software. Neil said they need to think about the tradeoffs, since they don't have the resources of large companies. Startups should try to have a little bit better than good enough defenses, and performing security reviews with their customers is a good thing to do.

Time at Google

During this section Gary asked Neil about his time spent at Google. Neil described Google as a "federation of startups". This is because while Google has very mature products, such as search and advertising, many of the Google labs projects are run in a startup-like manner. The difference between Google labs and real startups though is infrastructure. All Google projects have access to the Google infrastructure, but a real startup needs to build or buy infrastructure on their own.

Bad Ads

The discussion then turned to what Neil called malvertising, and Gary called "bad ads". The problem is that because ads are served through ad networks, a compromised ad network can be used to spread malware all over the web. These bad ads can run javascript in the browser, and automatically infect machines by using known vulnerabilities for the specific browser and OS the user is running.

Neil's Company

Neil's company works with ad networks to detect and block the spread of these bad ads. Server side scanning is used to detect these ads, and when a bad ad is detected an automated alert is sent out and the ad is blocked. One example of a significant occurrence Neil provided was that at one point the London stock exchange got flagged by the Google Safe Search API for hosting malware, which were distributed on its pages through compromised advertising.

Why not attack problem through better software security?

Gary asked Neil if this was really needed, and why we just can't patch vulnerable software. Neil said that there is so much software out there, it's impossible to secure it all. He was in favor of the idea, but said that defense in depth is the best plan.

Stanford Software security certification

The discussion then turned to the Stanford Advanced Security Certification Program, which Neil is co-director of. The idea of the program is that we don't have enough security professionals right now, so a program was needed to provide people a clear path to learning about security. They also have a program which covers emerging threats. The program doesn't necessarily target programmers, but also management. Neil finished this section by saying that security is a process, not just a product, so all levels need to be involved in it.

Neil's Time at Google (Part 2)

Finally, the discussion returned again to Neil's time at Google. There was a botnet designed specifically to click on ads which Google had to combat called Clickbot.A. This botnet ran on over 100,000 machines, and could be used to generate significant revenue for its operators. Google's approach to resolve this problem was to make the attacks unprofitable by identifying the invalid clicks and not charging advertisers for them. Gary then asked Neil how important testing was for Google. Neil said that Google is very focused on testing because the attack surface can increase with even a single line of code. Google uses both automated and manual tests for their software, and if the automated tests find anything, it usually means there are significant problem still hidden.