1500 - 25 Years of Program Analysis

Sunday at 15:00 in 101 Track
45 minutes | Hacker History, Demo
Zardus (Yan Shoshitaishvili)*Assitant Professor, Arizona State University*

Last year, DARPA hosted the Cyber Grand Challenge, the culmination of humanity's research into autonomous detection, exploitation, and mitigation of software vulnerabilities. Imagine the CGC from the outside: huge racks of servers battling it out on stage, throwing exploit after exploit at each other while humans watch helplessly from the sidelines. But that vantage point misses the program analysis methods used, the subtle trade-offs made, and the actual capabilities of these systems. It also misses why, outside of the controlled CGC environment, most automated techniques don't quite scale to the analysis of real-world software!

This talk will provide a better perspective. On the 25th anniversary of DEFCON, we will go through these last 25 years of program analysis. We'll learn about the different disciplines of program analysis (and learn strange terms such as static, dynamic, symbolic, and abstract), understand the strength and drawbacks of each, and see if, and to what extent, they are used in the course of actual vulnerability analysis.

Did you know that every finalist system in the Cyber Grand Challenge used a combination of dynamic analysis and symbolic execution to find vulnerabilities, but used static analysis to patch them? Why is that? Did you know that, to make the contest feasible for modern program analysis techniques, the CGC enforced a drastically-simplified OS model? What does this mean for you, if you want to use program analysis while finding vulns and collecting bug bounties? Come to this talk, become an expert, and go on to contribute to the future of program analysis!
Zardus (Yan Shoshitaishvili)
Zardus is one of the hacking aces on Shellphish, the oldest-running CTF team in the world. He's been attending DEFCON since 2001, playing DEFCON CTF since 2009, and talking at DEFCON since 2015. Through this time, he also pursued a PhD in Computer Security, focusing on Program Analysis. The application of cutting-edge academic program analysis techniques to CTF (and, later, to his participation in the DARPA Cyber Grand Challenge, where he led Shellphish to a 3rd-place victory and a big prize payout) gave Zardus a unique understanding of the actual capabilities of the state of the art of program analysis, which in turn drove his research and culminated in the release of the angr binary analysis framework and the Mechanical Phish, one of the world's first autonomous Cyber Reasoning Systems.

#defcon25/by_track/101/Sunday #defcon25/By_Day/_Sunday