OFFENSIVE SECURITY CONFERENCE

Ramtin Aryan

16-17 February
Berlin, Germany

In February, COINS supported me to attend The OFFENSIVE SECURITY CONFERENCE 2018.The conference was held in Berlin from the 16th to the 17th of February.

OffensiveCon Berlin was a highly technical international security conference focused on offensive security. The aim of the conference was to bring the community of research groups, independent researchers and hackers together for high quality and deep technical talks, engaging and renowned technical trainings. The talks at OffensiveCon were focused on offensive IT security topics such as vulnerability discovery, advanced exploitation techniques and reverse engineering. The conference was constructed as a single track of talks for two full days as well as technical trainings held in the days before the conference.

It was a great opportunity to meet researchers from the different fields in software security. Full program of the conference is available in the webpage of the conference [1].

The first day started with a very interesting keynote by Rodrigo Branco. The lecture title was "INSIDE THE MACHINE: HOW OFFENSIVE SECURITY IS DEFINING THE WAY WE COMPUTE DATA." As it explained in the title, he tried to talk about how offensiveSecurity can help us to develop the security and reliability of the computer systems. In part of the lecture, he talked about how the academia can help and in which parts it has weakness and can't release a solution for the practical problems in the sufficient time. As a conclusion, he believed that the new vulnerabilities going to be more complex. For mitigating we should have not only updated but also practical knowledge, and if we want to be a good defender, we should be an excellent attacker!

Niko Schmidit presents a novel solution for detecting the zero-days vulnerabilities in source codes. In first step, he tried to review the previous works

[1] https://www.offensivecon.org/agenda/

and compare the weaknesses and strengths. Then he started to explain the proposed method. The method tries to analyze the code and generate a semantic model. This step can be applied on different languages and syntaxes. The semantic model will be analyzed to detect the basic vulnerabilities that can be uses by exploits. They try to present a new language similar to a firewall configuration, which allows to specify exactly what an attacker can do, which input, she/he controls, and where data may leak to her/him. They show how this information, combined with language-neutral formulations of typical vulnerability patterns allow for cross-language identification of many classes of vulnerabilities, including object deserialization vulnerabilities, command injections and cross site scripting. The keen dream of the presenters is to build a machine that eats code on a large-scale and prepares accurate information about all the ways in which this program exposes itself to the attacker, fails to be cautious about the input it receives, and leak information. "This is not something you create in a year and not in five, and while you do it, you continuously remember that what you are trying to do is impossible in general. This does not mean though, that it will not work remarkably well in practice," he mentioned. At the end, he presents a nice demo of the first version of the engine.

There were so many interesting presentations and demos, such as "Discovering and Exploiting a Vulnerability in Cisco ASA" or "L'art de l'évasion: Modern VMWare Exploitation Techniques " or "From Assembly to Javascript and back: Turning Memory Corruption Errors into Code Execution with Client-Side Compilers" that it is impossible to describe them in this short report.

There is no doubt that the highest motivation for attending events like this, is the opportunity to be in touch with cutting-edge research and researchers, as well as to get to know new results and techniques in software security. I am grateful to COINS for having allowed my presence there through financial support.