Revery: from Proof-of-Concept to Exploitable

Dr Chao Zhang
Associate Professor
Tsinghua University
China

Date : 3 October 2018 (Wednesday)
Time : 11:00 a.m. – 12:00 noon
Venue : Room PQ703, 7/Floor, PQ Core, Mong Man Wai Building,
The Hong Kong Polytechnic University

Abstract

Software vulnerabilities are one of the root causes of many severe cyber security incidents. More and more vulnerabilities are found and reported, due to the increasing number of software and vulnerability discovery solutions. Vulnerability assessment, especially exploitability assessment, is important for both defenders and attackers. Automated exploit generation (AEG) is an important way to assess the exploitability of vulnerabilities. However, AEG is an open challenge. In some cases, the given proof-of-concept (PoC) input, which triggers the vulnerability, could exercise a crashing path but could not enter an exploitable program state. In this talk the speaker will introduce a solution Revery to this specific challenge. It finds a diverging path (different from the crashing path), which triggers an exploitable state, by fuzzing rather than symbolic execution. Then it stitches the diverging path and the crashing path together, and synthesizes a new program path that triggers both the vulnerability and the exploitable state. With symbolic execution, it thus could generate exploits in some cases. The prototype of Revery is evaluated on 19 CTF (Capture The Flag) challenges. The results showed that Revery is able to generate exploits for 9 of them, and generate PoCs to trigger vulnerabilities and enter exploitable states for another 5.

About the Speaker

Dr Chao Zhang is an Associate Professor at Tsinghua University. Prior to joining Tsinghua, he graduated from Peking University and did postdoc research in UC Berkeley with Dawn Song. His research interest lies in system and software security, especially in vulnerability detection, exploit and defense. His defense solution FPGate won the Special Recognition Award in Microsoft's BlueHat Prize Contest in 2012. He co-led a team CodeJitsu from UC Berkeley and built a system Glactica able to perform automated vulnerability detection, exploit and defense, which did excellently in the Cyber Grand Challenge launched by DARPA. He is a member of the CTF team Blue-Lotus.

All are welcome!

Enquiries:
Professor George Baciu
Email: csgeorge@comp.polyu.edu.hk
Tel : 2766 7295 / 2766 7272

We drive innovation through SMART COMPUTING