Chen Peng 陈鹏

Phone: +86 185 1655 7902
Email: spinpx@gmail.com
Homepage: http://spinpx.com/

Education

M.S., Computer Science, ShanghaiTech University (中国科学院学位) Sep 2015 -- Jul 2018

Exchange student, Computer Science, National Chiao Tung University Feb 2013 -- Jun 2013

B.S., Computer Science, Harbin Institute of Technology (哈尔滨工业大学) Sep 2011 -- Jul 2015

Experience

Intern at Compound Search Department, Baidu. Jun 2014 – Sep 2014

TA for Data Structure (Outstanding TA award) 2015

Publications

[1] Peng Chen and Hao Chen. "Angora: efficient fuzzing by principled search". In: *IEEE Symposium on Security and Privacy (S&P)*. San Francisco, CA, May 21–23, 2018.

[2] Peng Chen and Hao Chen. "Security analysis of personal unmanned aerial vehicles". In: *International Conference on Security and Privacy in Communication Networks (SECURECOMM)*. Guangzhou, China, Oct. 10–12, 2016.

Projects

Angora: efficient fuzzing by principled search Oct 2016 – Present

We propose Angora, a new mutation-based fuzzer that outperforms the state-of-the-art fuzzers by a wide margin. The main goal of Angora is to increase branch coverage by solving path constraints without symbolic execution. To solve path constraints efficiently, we introduce several key techniques: scalable byte-level taint tracking, context-sensitive branch count, search based on gradient descent, and input length exploration.

Skills: C/C++, Rust, LLVM, IPC, taint tracking, machine learning

Security analysis of unmanned aerial vehicles Mar 2015 – Sep 2015

We studied the risks of UAVs and conducted an empirical analysis of three popular DJI UAVs. We discovered a series of vulnerabilities, including insecure communication channels, misuse of cryptography, and insecure UAV activation and developer authorization. By exploiting these vulnerabilities, we designed a series of attacks for UAV.

Skills: Python, TCP/UDP, Android security

Source code author deanonymization Nov 2015 – Jan 2016

In this work, we explored neural network based approaches (Recurrent neural network) towards the source code author deanonymization problem. With a dataset extracted from Google Code Jam, our char-level model performs competitively on normal size dataset comparing to previous state-of-art work.

Skills: Lua, Torch, deep learning