Xiangkun Jia

Addr: Building 5, 4# South Fourth Street, Zhong Guan Cun, Beijing, CHINA, 100190
Phone: (86)15652143223
Email: jiaxiangkun@tca.iscas.ac.cn ajiahit@gmail.com

Research Interests

Program analysis

Analyze software security, especially based on taint analysis and symbolic execution.

Vulnerability analysis

Find potential vulnerabilities in an active way, analyze root causes of program crashes and assess the exploitability of program bugs.

Malware detection

Detect malwares and APT attacks based on dynamic program behaviors.

Machine learning

Solve security problems with machine learning, understand the learning results.

Education

Institute of Software, Chinese Academy of Sciences *09/2012 - Now*
Ph.D., Computer Applications Technology,
Advisor: Purui Su, Dengguo Feng

Harbin Institute of Technology *09/2008 - 07/2012*
B.E., Information Security

Feng Chia University *09/2010 - 01/2011*
Exchange student, Computer Science and Information Engineering

Publications

Conferences

1. **Xiangkun Jia**, Chao Zhang, Purui Su, Yi Yang, Huafeng Huang, Dengguo Feng. *Towards Efficient Heap Overflow Discovery*. 26th USENIX Security Symposium (USENIX Security'17).
2. Liang He, Yan Cai, Hong Hu, Purui Su, Zhenkai Liang, Yi Yang, Huafeng Huang, Jia Yan, **Xiangkun Jia**, Dengguo Feng. *Automatically Assessing Crashes from Heap Overflows*. The 32nd IEEE/ACM International Conference on Automated Software Engineering (ASE'17).
3. **Xiangkun Jia**, Jia Yan, Purui Su. *Safety analysis and evaluation of security protocol implementation*. Bulletin of Chinese Association for Cryptologic Research. Issue 6, 2014. in Chinese.

Patents

1. **Xiangkun Jia**, Chao Zhang, Purui Su, …… *An automatic identification method for custom heap management functions based on dynamic features*. in Chinese. (Applying)
2. **Xiangkun Jia**, Chao Zhang, Purui Su, …… *An offline method for heap overflow*

discovery based active construction. in Chinese. (Applying)

3. **Xiangkun Jia**, Liang He, Purui Su, …… *A binary-oriented heap overflow detection method*. in Chinese. (Applying)
4. **Xiangkun Jia**, Jia Yan, Purui Su, …... *A network protocol reverse analysis method based on identifying message segment separators.* in Chinese. (Applying)

Book

Purui Su, Lingyun Ying, Yi Yang. Software security analysis and application. Chapter 2 basic knowledge and Chapter 5 symbolic execution. in Chinese.

Bug report

CVE-2016-6164 for ffmpeg, CVE-2016-9931 for Realplayer, CVE-2017-13823 for QuickTime.

Rewarded by Tencent Security Response Center, Alibaba Security Response Center

Project Experiences

1. **Heap overflow vulnerability discovery/detection/assess**
   Designed and implemented a system to discover/detect/assess heap overflow vulnerabilities based on dynamic taint analysis and symbolic execution.
2. **Application-oriented taint analysis system development**
   Implemented hook functions for taint sources and heap allocation operations.
3. **Malware detection and analysis platform development**
   Implemented interaction analysis tools for malware detection based MFC.

Other Experiences

Student PC for Oakland S&P 2018.

Writing sub-reviews for some conferences (CSET'17, RAID'17, VARA'17, CODASPY'16), and some journals (Chinese Journal of Computers, Journal of Software, Chinese Journal of Electronics)

Honor

1. 2017, Internet security scholarship of CHINA internet development foundation
2. 2017, National Scholarship
3. 2016~2017, Merit Student, and Excellent Leader in UCAS.
4. 2012~2013, Merit Student in UCAS.
5. 2012, Excellent graduate of Heilongjiang Province in HIT.
6. 2008~2012, Merit Student in HIT.