Chen Peng 陈鹏

上海科技大学 (中科院学位)
信息科学与技术学院

电话: 185 1655 7902
邮箱: spinpx@gmail.com
个人主页: http://spinpx.com/

教育经历

硕士, 计算机科学与技术, 上海科技大学 (中科院学位) 2015.9 – 2018.7

本科, 计算机科学与技术, 哈尔滨工业大学 2011.9 – 2015.7

个人经历

百度复合搜索部实习 2014.6 – 2014.9

年度最佳助教 (数据结构课程) 2015

发表论文

[1] Peng Chen and Hao Chen. "Angora: Efficient fuzzing by principled search". In: *IEEE Symposium on Security and Privacy (IEEE 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.

项目

无人机飞行器的安全分析 2015.3 – 2015.9
针对市面上主流的几款无人机, 我们研究和分析它们存在的安全隐患和风险。在这个过程中, 我们发现了无人机系统上的一系列安全缺陷, 包括不安全的通信方式, 加密方法的错误使用, 以及对无人机和开发者不安全的认证激活方式等。通过对这些漏洞的利用, 我们设计了一系列的攻击手段。最后, 我们分类出三种对无人机的攻击方式, 并提出防御机制, 以及探讨无人机安全的特别挑战。
相关技术: *TCP/UDP*, 逆向工程，安卓安全，密码学

源代码作者的去匿名化 2015.12 – 2016.1
在这个工作中, 我们尝试使用深度学习的方法 (LSTM) 来解决源代码作者去匿名化的问题。在 Google Code Jam 数据集上, 我们的字符粒度模型取得较高的精确度, 并与目前最好的工作具有可比性。
相关技术: 爬虫, *Lua* 语言, *Torch* 框架, 深度学习

Angora: 高效, 覆盖率导向的现代模糊测试工具 2016.10 – 2017.12
我们设计了一种新的模糊测试工具，Angora。它的主要思想是利用非符号执行的方法来解决路径约束，从而增加代码执行的覆盖率找到漏洞。我们把每个约束看成一个黑盒函数，通过优化方法求解这个函数的解。为了实现这个思想，我们提出了以下关键技术：稳健高效的字符粒度的污点分析，上下文敏感的分支统计，基于梯度下降的搜索优化方法，和输入长度的智能增长。
相关技术: *C/C++*, *Rust*, *LLVM*, *IPC*, 污点分析