李振源

(+86) 183-9259-3905 · lizhenyuan@zju.edu.cn · 浙江大学-网络空间安全-博士在读 · GitHub @li-zhenyuan

个人总结

博士期间主要研究方向包括终端安全、威胁检测分析、恶意程序动静态分析等。近 4 年来，主持与参与国家、校级网络与信息安全领域项目 5 项，包括：面向 APT 网络攻击链的智能检测与溯源方法及关键技术研究（国家自然基金联合重点基金项目）、面向大规模网络的安全威胁智能分析发现技术（全军共用信息系统项目）、基于系统溯源图的入侵检测（之江青年人才基金）等。目前在 2019 ACM Conference on Computer and Communications Security (CCF-A)、Computer & Security (Q1) 和 IEEE Transactions on Dependable and Secure Computing (TOP SCI, Q1) 等网络与信息安全相关领域重要期刊和会议发表 SCI/EI 检索论文多篇。

教育背景

浙江大学 - 计算机科学与技术学院，网络空间安全，在读博士研究生　　2017.9 - 2022 (预期)

导师：陈焰 (Yan Chen) - IEEE Fellow，浙江大学-美国西北大学互联网安全联合实验室主任

之江实验室国际青年人才基金 2020 （￥30K），**浙江大学博士生学术新星项目 2020 （￥20K）**，三好研究生，优秀博士生岗位助学金（￥10K）

National University of Singapore - School of Computing，CSC 联培博士　2021.5 - 2022.5 (预期)

导师：梁振凯 (Liang Zhenkai) - Steering Group Member of NDSS'21

西安电子科技大学 - 通信工程学院，信息安全，工学学士　　2013.9 - 2017.6

排名 1/154 (**前** 1%)，**国家奖学金**，**西安电子科技大学优秀毕业生标兵** (20/5000)，大学生数模竞赛 (2 次)，优秀学生标兵/优秀学生 (3 次)

主要荣誉

- 国家公派留学基金联培博士项目，国家留学基金委 2020
- 之江实验室国际青年人才基金（￥30K），之江实验室 2020
- 浙江大学博士生学术新星项目（￥36K），浙江大学 2020
- 三好研究生，浙江大学 2020
- 优秀博士生岗位助学金，浙江大学 2019
- 西安电子科技大学优秀毕业生标兵 (20/5000)，西安电子科技大学 2017
- 国家奖学金，中华人民共和国教育部 2015

学术论文

1. **Zhenyuan Li**, Qi Alfred Chen, Chunlin Xiong, Yan Chen, Tiantian Zhu,and Hai Yang. **"Effective and Light-Weight Deobfuscation and Semantic-Aware Attack Detection for PowerShell Scripts"**, In ACM Conference on Computer and Communications Security 2019 (**ACM CCS'19, CCF-A**).

   [Paper] [Code] [Slides] [Vedio]

2. **Zhenyuan Li**, Qi Alfred Chen, Yang Runqing, Yan Chen. **"Threat Detection and Investigation with System-level Provenance Graphs: A Survey"**, **Computer & Security 2021, (CCF-B)**

   [Paper]

3. **Zhenyuan Li**, Yang Runqing, Qi Alfred Chen, Yan Chen. **"A First Look at Evasion against Provenance Graph-based Threat Detection"**, Annual Computer Security Applications Conference. (**ACSAC' 20 Poster session, CCF-B**)

   [Paper] [Poster]

4. Runqing Yang, Xutong Chen, Haitao Xu, Yueqiang Chen, Chunlin Xiong, Linqi Ruan, Mohammad Kavousl, **Zhenyuan Li**, Liheng Xu, Yan Chen. **"RATScope: Recording and Reconstructing Missing RAT Semantic Behaviors for Forensic Analysis on Windows"**, IEEE Transactions on Dependable and Secure Computing 2021 (**IEEE TDSC' 21, CCF-A**)

   [Paper]

5. Chunlin Xiong, **Zhenyuan Li**, Qi Alfred Chen, Yan Chen, Tiantian Zhu, Hai Yang, and Wei Ruan. **"Generic, Efficient, and Effective Deobfuscation and Semantic-Aware Attack Detection for PowerShell Scripts"**, Frontiers of Information Technology & Electronic Engineering. (**FITEE, SCI**)

专利列表

- 201910994645.4 解混淆方法、装置、计算机设备和存储介质 (第一作者)
- 201810131880.4 基于动态行为的细粒度 RAT 程序检测方法、系统及相应的 APT 攻击检测方法 (第三作者)

项目经历 - 终端威胁检测

一、基于细粒度行为分析和溯源图的高级持续性威胁的检测 [2, 4] 2016.7 - 2020.10

- **背景**：随着信息技术的发展，网络空间的边界不断延展, 向攻击者暴露了越来越多的漏洞。传统的补漏式的防御策略越来越难以为继。安全从业人员和研究者亟需新的工具来描述攻击并进行检测。
- **我们的工作**：（1）本项目主要研究了被广泛用于 APT 攻击的远控木马（RAT）的多种攻击行为。研发了基于系统调用和上层 API 结合的实时，细粒度的检测系统 APTShield。（2）然后利用系统级的溯源图能够将系统中的行为根据因果关系联系起来, 结合上下文信息对初步检测结果进行过滤，最终给出更加准确的检测结果。
- **关键词**：APT, RAT, Provenance Graph, Causality Analysis, Potential Harmful Behavior
- **基金**：国家自然基金联合基金项目 - 面向 APT 网络攻击链的智能检测与溯源方法及关键技术研究，浙江大学学术新星项目
- **产出成果**：CCF-A Paper × 1, CCF-B Survey × 1, 专利 × 1, 原型系统发展成为奇盾公司[1]EDR 产品。

二、针对基于溯源图的入侵检测系统的 Live-off-the-Land 攻击研究 [3] 2020.7 - 2020.11

- **背景**：现有的基于溯源图的入侵检测系统都存在粗粒度因果分析导致的依赖爆炸问题。为了缓解这一问题，已有系统对溯源的深度或广度做出了一定的限制。这些限制引入了潜在的风险。
- **我们的工作**：针对上述的风险，我们开发了一套工具来系统性的生成攻击样本。这些攻击样本可以帮助我们设计与测试检测系统。
- **关键词**：Provenance Graph, Causality Analysis, Evasion, Live-off-the-Land Attack.
- **产出成果**：CCF-B Poster × 1,

三、基于攻击技术模板的攻击报告解析和结构化威胁情报提取 2020.11 - present

- **背景**：基于日志的威胁检测是很有效的解决复杂的网络攻击的手段。但是现有的方案仍然需要大量的人工操作来构建恶意行为的特征描述。为了提高自动化程度，加快应急响应速度。我们迫切的需要一个自动化的攻击描述提取方案。
- **我们的工作**：为了解决这一问题，我们认为可以采用大量已有的含有丰富攻击描述的“攻击报告”作为数据源。利用 NLP 技术提取粗粒度的攻击描述图，然后利用自动生成的攻击描述模板来提取其中的攻击技术实现细节和结构化的 IoC 信息。
- **关键词**：Cyber Threat Intelligence Reports, MITRE TTPs, Attack Technique Template, NLP
- **基金**：全军共用信息系统（预研）项目 - 面向大规模网络的安全威胁智能分析发现技术，之江青年人才基金

项目经历 - 恶意程序分析

四、高效且轻量的脚本类语言通用解混淆框架 [1, 5] 2018.7 - 2019.11

- **背景**：近年来, PowerShell 被广泛的用于多种网络攻击, 包括钓鱼邮件攻击，勒索病毒，无文件攻击等。但是由于 PowerShell 的动态特性，可很方便的混淆和实施无文件攻击。因此现有的检测方法无法准确的检测基于 PowerShell 的攻击。
- **我们的工作**：我们针对关键的混淆问题，设计了一套细粒度（抽象语法子树）的，准确且轻量的解混淆系统。实验证明可以有效处理多种、多层的混淆，且解混淆可以有效提高检测的准确度。
- **关键词**：PowerShell (Scripting Language), 静态分析, Fileless Attack, De-Obfuscation, AST.
- **基金**：浙江省重点研发项目 (2018C01088).
- **产出成果**：CCF-A Paper × 1，SCI Paper × 1，专利 × 1，原型系统被部署在奇盾公司的生产环境中。

[1] 奇盾-MagicSheild 是我导师陈焰于 17 年创立的终端安全公司，已经获得多轮共计千万级风险投资。

五、服务器侧恶意程序检测绕过技术研究 2020.7 - present

- **背景**：服务器侧恶意程序（以 WebShell 为例）一直是最大的系统安全威胁之一。相较于用户侧的恶意程序，服务器侧恶意程序的影响面往往更广，造成的破坏更大。同时，服务器侧的恶意程序往往使用更为复杂的绕过技术（包括混淆、变体等），给检测工作带来更大的困扰。
- **我们的工作**：我们分析了大量的恶意程序样本中使用的绕过技术，以及多个商用和研究的检测系统对绕过的抵抗能力。总结了服务器侧恶意程序检测与绕过的对抗经验。
- **关键词**：Server-side Malware, PHP, Evasion, Obfuscation, Metamorphism

实习经历

阿里云- 基础安全部, *研究型实习生* 2021.3 - 2021.4

- 分析关键账号数据库日志（app_name, account_name, db_instance, sql_text, etc.），研究攻击模型，设计基于异常访问的检测方案。
- 利用阿里云 ODPS 计算平台实现检测方案，并通过和部门内部蓝军对抗测试检测能力和性能。

学术活动

- 于 “ACM CCS 2019” 做报告展示关于 PowerShell 解混淆的最新工作，英国伦敦
- 受邀于 “InforSec 网络空间安全国际顶会论文分享会” 做报告 (北京网络空间安全大会分会场)，在线
- Reviewer: IEEE ACCESS (2020)
- SubReviewer: AsiaCCS’22, CCS’19, ICDCS’19, ESORICS’19, CCS’18