ZHENYUAN LI

Ph.D. Student at Zhejiang University
lizhenyuan@zju.edu.cn, +86 18392593905

EDUCATION

Zhejiang University, Hangzhou, China *September 2017 - Present*
Ph.D. in Cyber Space Security - Advisor: Yan Chen
College of Computer Science and Technology

National University of Singapore, Singapore *May 2021 - Present*
Visiting Student sponsored by CSC - Advisor: Zhenkai Liang

Xidian University, Xi'an, China *September 2013 - June 2017*
Bachelor of Engineering in Information Security. Overall Ranking: 1/154

AWARDS AND HONORS

2021-02 Zhejiang Lab's International Talent Fund for Young Professionals (Funding 30,000 CNY)
2020-12 Zhejiang University's Academic Rising Star (Funding 20,000 CNY)
2020-11 Merit Student, Zhejiang University
2020-09 Academic Awards for Outstanding Doctoral Candidates, Zhejiang University
2020-08 Chinese Government Scholarship, China Scholarship Council
2019-12 Excellent Doctoral Scholarship, Zhejiang University
2017-05 Outstanding Graduate (20/ 5000), Xidian University
2015-11 National Scholarship, The Ministry of Education of the PeopleâĂŹs Republic China

PUBLICATION

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**)

PROJECTS

System-level Provenance Graph-based Threat Detection [2, 3] *August 2019 - present*

With the development of information technology, the border of the cyberspace gets much broader, exposing more and more vulnerabilities to attackers. Traditional mitigation-based defence strategies are challenging to cope with the current complicated situation. Security practitioners urgently need better tools to describe and modelling attacks for defence. The provenance graph seems like an ideal method for threat modelling with powerful semantic expression ability and attacks historic correlation ability. In this project, we aim to design a light-weight still effective detector based on the provenance graph.

Generic Deobfuscation Framework for PowerShell [1, 5] *July 2018 - November 2019*

In recent years, PowerShell is increasingly reported to appear in a variety of cyber attacks ranging from advanced persistent threat, ransomware, phishing emails, cryptojacking, financial threats, to fileless attacks. However, since the PowerShell language is dynamic by design and can construct script pieces at different levels, state-of-the-art static analysis based PowerShell attack detection approaches are inherently vulnerable to obfuscations. To overcome this challenge, we aim to design the first effective and light-weight deobfuscation approach for PowerShell scripts.

Endpoint Detection and Response for APT Attacks [4] *July 2016 - October 2020*

Advanced Persistent Threats (APTs) could cause significant damage to the targeted entities such as governments and corporations, and are attracting much attention from both scientific community and the commercial world. Previous malware detection methods are not fine-grained or robust enough for the problem of APT detection. In this project, we thwart against APT attacks by targeting remote access trojans (RATs), the core component in an APT campaign. We proposed *APTShield*, a real-time, fine-grained and situation-aware system to detect RATs by identifying the suspicious activities being exhibited and further determining the maliciousness based on the context information associated with the activities.

ACADEMIC SERVICES AND EVENTS

Reviewer : IEEE Access (2020)
Subreviewer/External reviewer : AsiaCCS'21, CCS'19, ICDCS'19, ESORICS'19, CCS'18

Presentation at **ACM CCS 2019**, London, UK
Inivited Talk at **InForSec** Cyber Security Academic Papers Sharing (Co-located with **Beijing Cyber Security Conference**), Virtual