Song Li
http://songli.io

Email : songli@jhu.edu
Mobile : +1-484-935-1501

Education

- **Johns Hopkins University** — Maryland, USA
  Expected Ph.D. in Computer Science and Engineering; GPA: 3.9/4.0 — *Aug. 2018–May. 2022*
- **Lehigh University** — Pennsylvania, USA
  Master in Computer Science and Engineering; GPA: 3.9/4.0 — *Aug. 2015–May. 2017*
- **Beijing Institute of Technology** — Beijing, China
  Bachelor of Software Engineering; GPA: 3.4/4.0 — *Aug. 2011–May. 2015*

Publications

1) Mining Node.js Vulnerabilities via Object Dependence Graph and Query,
Song Li, Mingqing Kang, Jianwei Hou, Yinzhi Cao,
in the Proceeding of the 31th USENIX Security Symposium, 2022

2) Detecting Node.js Prototype Pollution Vulnerabilities via Object Lookup Analysis,
Song Li, Mingqing Kang, Jianwei Hou and Yinzhi Cao,
in the Proceeding of the ACM Joint European Software Engineering Conference
and Symposium on the Foundations of Software Engineering (ESEC/FSE), 2021

3) Who Touched My Fingerprint? A Large-scale Measurement Study and Classification of Fingerprint Dynamics,
Song Li, Yinzhi Cao,
in the Proceeding of the ACM Internet Measurement Conference (IMC), 2020

4) Rendered Private: Making GLSL Execution Uniform to Prevent WebGL-based Browser Fingerprinting,
Shujiang Wu, **Song Li** and Yinzhi Cao, Ningfei Wang,
in the Proceeding of the 28th USENIX Security Symposium, 2019

5) Deterministic Browser,
Yinzhi Cao, Zhanhao Chen, **Song Li**, Shujiang Wu,
in the Proceeding of ACM Conference on Computer and Communications Security (CCS), 2017

6) (Cross-)Browser Fingerprinting via OS and Hardware Level Features,
Yinzhi Cao, **Song Li*** and Erik Wijmans,
in the Proceeding of the Annual Network & Distributed System Security Symposium (NDSS), 2017
(* first student author)

Professional Experience

- **Research Assistant** — Johns Hopkins University, USA
  Code Property Graph Based Vulnerability Detection — *Feb. 2018–Present*
  - **Funded by**: National Science Foundation (NSF) and Defense Advanced Research Projects Agency (DARPA)
  - **Mining Node.js Vulnerabilities via Object Dependence Graph and Query**: Designed and implemented a new type of Code Property Graph, which is cross-function, cross-file, and object-based, to detect varies vulnerabilities in JavaScript (Node.JS) programs including code injection, XSS, authentication error and other CVEs. This graph can also be easily applied to other languages. The research results in 70 CVEs and the related paper is published to USENIX Security '22
  - **Detecting Node.js Prototype Pollution Vulnerabilities via Object Lookup Analysis**: Proposed a flow-, context-, and branch-sensitive static taint analysis tool, called ObjLupAnsys, to detect prototype pollution vulnerabilities. The key of ObjLupAnsys is a so-called object lookup analysis, which gradually expands the source and sink objects into big clusters with a complex inner structure by performing targeted object lookups in both clusters so that a system built-in function can be redefined. The research results in 11 CVEs, and the related paper is published to ESEC/FSE '21
- **Research Assistant** — Johns Hopkins University, USA
  Browser Fingerprinting — *Feb. 2018–Jan. 2019*

- **Rendered Private**: Proposed and implemented UNIGL, a novel system that rewrites GLSL programs and redefines all the floating-point operations in the aforementioned three stages of WebGL rendering, which can make the rendering results of programs deterministic across browsers and devices. This work is used to defend against WebGL based (cross-)browser fingerprinting. The paper has been accepted by USENIX Security '19.
- **A Large-scale Measurement Study of Browser Fingerprint**: Made a large-scale measurement of browser fingerprint, including popular features introduced by multiple research papers. Collected more than 15,500,788 visiting records from 226 countries, 960,853 pieces of dynamics information belonging to 661,827 browser instances. We analyzed the robustness, uniqueness of each feature and also extracted the dynamics of browser fingerprints and the reason for fingerprints changing. The related paper has been accepted by IMC '20.

- **Data Scientist Research Intern** — Microsoft, USA
  Deep Learning — *May. 2019–Aug. 2019 & May. 2020–Aug. 2020*
  - **Power Virtual Agents Model Analyzing System**: Designed and implemented a system to analyze the Power Virtual Agents model developed by Microsoft. This system can interpret the NLP model, analyze the details of each layer including the attention heat map, the embedding of sentences, the 2D visualization of sentences, etc. This project is used by the PVA team and considered to be applied to the PVA production.
  - **AI Builder Dataset Modification Recommendation System**: Designed and implemented a system to recommend modifications on the dataset at the user level to make the prediction of the machine learning model more accurate. More specifically, the users of the machine learning platform may not know how to make a predictive dataset. By my work, the system can suggest what modifications on the dataset may help to get a better result. This work is based on designing an algorithm to define the distance between dataset, and do the recommendation based on the similar dataset in the dataset pool built on top of the history.

- **Research Assistant** — Lehigh University, USA
  Browser Fingerprinting — *Dec. 2015–Feb. 2018*
  - **Deterministic Browser**: Built the first execution time deterministic browser, DeterFox (deterfox.com), based on Firefox open-source project to defend against timing channel attacks. The related paper has been accepted by The ACM Conference on Computer and Communications Security (CCS) '17.
  - **Cross-browser Fingerprinting**: Implemented the first cross-browser fingerprinting framework that relies on novel hardware and OS level features, such as graphics cards and installed writing scripts. The related paper has been accepted by Network & Distributed System Security Symposium (NDSS) '17.

Selected Artifacts

1) Cross Browser Fingerprinting,
Paper: (Cross-)Browser Fingerprinting via OS and Hardware Level Features,
GitHub Repo: https://github.com/Song-Li/cross_browser
Stars: 1.1k Forks: 244 LoC: 21k
Selected Media Outlets: BeepingComputer, Top Tech News, Sci-Tech Today, The Hackers News, Digital Journal and IEEE Spectrum

2) ODGen,
Paper: Mining Node.js Vulnerabilities via Object Dependence Graph and Query,
GitHub Repo: https://github.com/Song-Li/ODGen
Results in 70 new CVEs, e.g., CVE-2019-10777 in aws-lambda and CVE-2020-7625 in op-browser

3) ObjLupAnsys,
Paper: Detecting Node.js Prototype Pollution Vulnerabilities via Object Lookup Analysis,
GitHub Repo: https://github.com/Song-Li/ObjLupAnsys
Results in 11 new CVEs, e.g., CVE-2019-10795 in undefsafe (>5M weekly downloads)

Patent

Improved Solving Method for Quasi-identifier in K-anonymization,
Fusheng Jin, XIaowei Hu, Zhen Yan, Song Li, Xiangyu Han,
CN104318167A, SIPO (The State Intellectul Property Office of The People's Republic of China), 2015

Presentations & Talks

- **Detecting Node.js Prototype Pollution Vulnerabilities via Object Lookup Analysis**
  ESEC/FSE '21 *Aug. 2020*
- **A Large-scale Measurement Study and Classification of Fingerprint Dynamics**
  ACM IMC '20 *Oct. 2020*
- **(Cross-)Browser Fingerprinting via OS and Hardware Level Features**
  NDSS '17 *Feb. 2017*

Professional Activities

Program Committee

- **USENIX Security AE**: 31st USENIX Security Symposium (USENIX Security '22 artifact evaluation)

External Reviewer for

- **WWW**: International World Wide Web Conference, Security and Privacy Track, 2018

Teaching

- **Teaching Assistant**: Web Security, Johns Hopkins University, Fall/2019

Research Mentoring

Master Students:

- **Yichao Xu**: Johns Hopkins University, 07/2021-Present
- **Siqi Cao**: Johns Hopkins University, 12/2020-03/2021
- **Huangyin Chen**: Johns Hopkins University, 12/2020-03/2021
- **Qingshan Zhang**: Johns Hopkins University, 12/2020-03/2021
- **Mingqing Kang**: Johns Hopkins University, now a PhD student at the Johns Hopkins University, 12/2020-03/2021
- **Queenie Gao**: Johns Hopkins University, 12/2019-03/2020
- **Minjie Fu**: Johns Hopkins University, First Job: Facebook, 12/2019-03/2020
- **Jingyi Li**: Johns Hopkins University, 12/2019-03/2020
- **Guanlong Wu**: Johns Hopkins University, now a PhD student at the University of Virginia, 04/2018-03/2019
- **Ningfei Wang**: Lehigh University, now a PhD student at the University of California, Irvine, 10/2017-05/2018

BS Students:

- **Rohan Jasani**: Indian Institutes of Technology, 06/2020-09/2020
- **Tianchen Zhang**: Beihang University, 06/2020-09/2020
- **Gongqi Huang**: Johns Hopkins University, 08/2019-02/2020
- **Xueqi Ren**: Lehigh University, then a Master student at the Columbia University, 10/2017-05/2018
- **Olivia Orrell-Jones**: Brown University, 05/2017-08/2017
- **Erik Wijmans**: Washington University in St. Louis, now a PhD student at the Georgia Institute of Technology, 05/2016-08/2016

High School Students:

- **Kylie Gong**: 07/2021-09/2021
- **Kevin Y.**: 07/2021-09/2021