SHITONG ZHU

900 University Ave, Riverside, CA 92521
shitong.zhu@email.ucr.edu ⋄ **shitong.me**

EDUCATION

University of California, Riverside — Sep 2016 - Jun 2021 (expected)
Ph.D. in **Computer Science** - CGPA: 3.67/4.00 — *Riverside, CA*
Advisor: Zhiyun Qian

Chongqing University of Posts and Telecommunications — Sep 2012 - Jun 2016
BEng. in Telecoms Engineering (**with Honors**) - CGPA: 3.73/4.00 - Top 6% — *Chongqing, China*

PUBLICATIONS

[**C7**] **Connecting the Dots: Detecting Adversarial Perturbations Using Context Inconsistency**
Shasha Li, **Shitong Zhu**, Sudipta Paul, Amit Roy-chowdhury, Chengyu Song, Srikanth Krishnamurthy, Ananthram Swami, Kevin S Chan
European Conference on Computer Vision (**ECCV '20**)

[**C6**] **AdGraph: A Graph-Based Approach to Ad and Tracker Blocking**
Umar Iqbal, Peter Snyder, **Shitong Zhu**, Benjamin Livshits, Zhiyun Qian and Zubair Shafiq
IEEE Symposium on Security & Privacy (**S&P '20**)

[**C5**] **SymTCP: Eluding Stateful Deep Packet Inspection with Automated Discrepancy Discovery**
Zhongjie Wang, **Shitong Zhu**, Yue Cao, Zhiyun Qian, Chengyu Song, Srikanth Krishnamurthy, Tracy D. Braun and Kevin S. Chan
Network & Distributed System Security Symposium (**NDSS '20**)

[**C4**] **ShadowBlock: A Lightweight and Stealthy Adblocking Browser**
Shitong Zhu, Umar Iqbal, Zhongjie Wang, Zhiyun Qian, Zubair Shafiq, and Weiteng Chen
The Web Conference (**WWW '19**)

[**C3**] **Measuring and Disrupting Anti-Adblockers Using Differential Execution Analysis**
Shitong Zhu, Xunchao Hu, Zhiyun Qian, Zubair Shafiq, and Heng Yin
Network & Distributed System Security Symposium (**NDSS '18**)

[**C2**] **Source-location Privacy Protection Strategy via Pseudo Normal Distribution-based Phantom Routing in WSNs**
Jun Huang, Meisong Sun, **Shitong Zhu**, Yi Sun, Cong-cong Xing, and Qiang Duan
Annual ACM Symposium on Applied Computing (**SAC '15**)

[**C1**] **On Selecting Composite Network-Cloud Services: A Quality-of-Service Based Approach**
Minkailu Mohamed Jalloh, **Shitong Zhu**, Fang Fang, and Jun Huang
Conference on Research in Adaptive and Convergent Systems (**RACS '15**)

[**J2**] **A Defense Model of Reactive Worms Based on Dynamic Time**
Haokun Tang, **Shitong Zhu**, Jun Huang, and Hong Liu
Journal of Software, 2778-2788, Sep 2014

[**J1**] **Propagation of Active Worms in P2P Networks: Modeling and Analysis**
Haokun Tang, Yukui Lu, **Shitong Zhu**, Jun Huang
Journal of Computers, 2514-2524, Sep 2014

PROJECTS

Detecting Adversarial Perturbations Using Context Consistency **[C7]**

· Defined, extracted and formulated context information from clean images to detect adversarially perturbed samples

ML-based Intrusion Detection System for Stealthy Attacks **[WIP]**

· Improving the detection accuracy/efficiency by constructing ML-based representations

Adversarial Examples Under Restricted Conditions **[WIP]**

· Improved the performance of adversarial machine learning under special requirements/circumstances

ML-based Automatic and Effective Adblocking **[C6]**

· Leveraged multiple layers of the web stack (HTML/HTTP/JavaScript) to train a classifier for blocking ads/trackers
· Replicated state-of-the-art filter lists with high accuracy (97.7%)
· Enhanced filter lists by automatically correcting their errors

Evading Deep Packet Inspection Systems Using Symbolic Execution **[C5]**

· Used symbolic execution to guide the generation of insertion and evasion packets at the TCP level for automated testing against DPI middleboxes
· Discovered over 20 strategies to elude DPI middleboxses that target Zeek (formerly Bro), Snort and GFW within an hour

Stealthy Adblcoking **[C4]**

· Built invisible adblocker that evades current generation of anti-adblockers with 100% of success rate in manual evaluation
· Replicated 98.2% of ad coverage achieved by popular adblocking extensions, while causing minor visual breakage on less than 0.6% of Alexa top 1K websites. In the meantime, page loads are sped up by over 5% on average

Anti-Adblocker Measurement and Disruption via Dynamic Program Analysis **[C3]**

· Modified V8 engine to apply differential execution trace analysis in Chromium
· Launched large-scale (Alexa top 10K) measurement, revealed 5-52 times more anti-adblockers than reported in prior literature
· Experimented with countermeasures against anti-adblockers, achieved promising effectiveness

WORK EXPERIENCE

PhD ML Software Engineer Intern @ Facebook Jul 2020 - Present
Business Integrity Team (Host: Abdel Baligh) *Remote*

· Fighting bad actors

Research Intern @ Samsung Research America Jan 2020 - Mar 2020
KNOX Security Team (Host: Xun Chen) *Remote*

· ML-based cyber-security infrastructure

Research Intern @ Samsung Research America Jun 2019 - Sep 2019
KNOX Security Team (Host: Xun Chen) *Mountain View, CA*

· Adversarial machine learning

Graduate Student Researcher @ UCR CSE Sep 2016 - Present
UCR SecLab *Riverside, CA*

· Pursued research on computer security and fulfilled the entire cycle of projects

· Published/co-authored papers accepted by or submitted to top-tier venues

Consulting Intern @ Deloitte TTL Jan 2016 - Mar 2016
ERS - Technology Risk *Shenzhen, China*

· Advised tech organizations to avoid being victim of a security breach through big data analytics
· Assisted team of a major bank in designing reliable identity and access management framework

SKILLS

Languages	Python, C/C++, JavaScript, MATLAB
Others	PyTorch, Chromium, Selenium/Puppeteer, NodeJS, Hadoop/Spark, Git

HONORS & AWARDS

Dissertation Year Program (DYP) Award UC Riverside CSE, 2020-2021
Dean's Distinguished Fellowship (full scholarship) UC Riverside CSE, 2016-2017
2nd Class University Scholarship CUPT, 2015-2016
National 2nd Prize @ National Olympiad in Informatics China Computer Federation, 2009