Zhang Qing

✉ zhangqingsdu@gmail.com

☎ +86 19800211550

📅 1989/06/10

EDUCATION

Shandong University, Master
2012/09 – 2015/06
Security and Privacy Protection

National University of Singapore, Invited visiting scholar
2013/10 – 2014/05
Model Checking on Security

Shandong University, Bachelor
2008/09 – 2016/06
Computer Science and Technology

AWARD

ID: Zhang Qing & cnwatcher

Acknowledged for 100+ CVE security vulnerabilities by Google and etc.

2022: 1st in Honor Annual Vulnerability Research; 2023: 2nd place; Overall top ranker.

2016: 1st in Huawei Cloud Service Vulnerability Research; 2022: 2nd place in Huawei Annual Research.

2016, 2021-2023: 1st in Meizu Annual Vulnerability Research; Overall top ranker.

2020: 1st in OnePlus Annual Vulnerability Research.

2018: 1st in OPPO Annual Vulnerability Research and Double Festival Event.

2017-2018: 1st in SmartOS Public Testing Vulnerability Research.

2017: Top in Samsung Security Vulnerability Acknowledgments.

2016: 2nd in Xiaomi Annual Vulnerability Research.

Renowned instructor in Android and Payment Security at Aichunqiu, with over 400K course enrollments.

PROFESSIONAL EXPERIENCE

Bytedance, Senior Privacy and Security Expert
2019/09
Received 2 individual breakthrough awards and 3 collaborative success awards. Achieved performance level 'E' twice.

Vulnerability Research:

- Problem Discovery: Conducted mobile security vulnerability research across all company products, uncovering hundreds of vulnerabilities, including RCE, LCE, and account takeovers in many core business areas.
- Tool Development: Led the development of the first and second generation mobile vulnerability scanning engines.

Privacy Red Team + Privacy Technology Group Head:

- Problem Discovery: Led the team in specialized inspections, discovering thousands of issues.
- Tool Development: Developed an APP privacy assessment audit platform for monitoring privacy data lifecycle during APP usage; Apollo Flare for illuminating APP behavior and network traffic; established a third-party SDK information collection database. Collaborated with legal and compliance teams to standardize the disclosure of third-party SDK data sharing, addressing incomplete coverage, unclear entry points, complex versioning, and process closure issues in third-party SDK privacy analysis.
- Rule Setting: Formulated detailed technical principles for privacy and security; developed a universal privacy and compliance technical testing framework, addressing the inefficiency of checklist-only privacy problem mining and providing a practical guide for privacy technology audits.

Tiktok Red Team:

- Specialized in Tiktok privacy and security vulnerability research; emergency response to external events; responsible for the security audit of the mobile code for the Tiktok Transparency Center (TC).

APP Signature Management System Development:

- Identified and addressed security issues in signature management, driving risk governance, cloud signature plugin development, signature rotation, external monitoring, and other signature management security concerns.

SDLC Lead for Multiple Business Sectors including Finance, Healthcare, and Social Media for a Period.

Xiaomi, Security Engineer
2017/01 – 2019/03

- IoT and Mobile Vulnerability Research; Account Risk Control.
- Presentation: Spoke at Hitb2018 and Syscan2018 about a new approach to vulnerability research transitioning from quantitative to qualitative change, with a patent.
- Presentation: Hitb2017, on the discovery of 200 Android vulnerabilities.
- Presentation: T00LS, on Android application security SDL processes and protection.

CERTIFICATES

- 2022: IAPP Certified Information Privacy Professional (FIP).
- 2022: IAPP Certified Information Privacy Professional/Europe (CIPP/E), specializing in EU GDPR.
- 2021: IAPP Certified Information Privacy Technologist (CIPT).
- 2011: IBM DB2 730 Certification; 2009 IBM UML Modeling Language Certification.
- 2010: General Management Capability Level Certificate.
- Lifetime member of OWASP.

PAPERS AND SPEECHES

Lead Author at a Tier-A Conference, NDSS 2023: "Post-GDPR Threat Hunting on Android Phones: Dissecting OS-level Safeguards of User-unresettable Identifiers."

Blackhat 2023: "Revisiting Stealthy Sensitive Information Collection from Android Apps."

Huawei 2023: "From Android to HarmonyOS - A Comprehensive View of Mobile Device Privacy and Security."

Hitb 2022: "Import Library, Import Liability: Analyzing Sensitive Information Collection of Third-party SDKs."

Lead Author at a Tier-A Conference, MobiCom 2022: "Assessing Certificate Validation User Interfaces of WPA Supplicants."

BlackHat 2021: "Hey, You, Get off My Private Data: Do Apps Respect Your Privacy as They Claim?"

Hitb 2021: "Stay Off My Private Data: A Framework to Examine Mobile App Privacy Claims."

ISC 2021: "A Journey to Find the 'Backdoors': The Inconsistent Android Permission Authentication Mechanism."

HITB 2020, Alibaba 2020: "The Secret Codes Tell the Secrets."

SKILLS

Skilled in Android reverse engineering and vulnerability research, proficient with tools like JEB, IDA, and familiar with binary analysis.

Knowledgeable in common web security attacks and defense strategies, as well as basic web vulnerability exploitation.

LANGUAGES

CET-6, proficient in listening, speaking, reading, and writing.

Qihoo 360, Security Engineer(Sepcail Offer)
2015/08 – 2016/12

- Establishment and maintenance of internal Android SDL (Software Development Lifecycle) and conducting Android security training within the company.
- Regular security audits of corporate Android products, establishment of a vulnerability database, and maintenance of internal APP security.
- Research on 3G/4G network vulnerabilities; Speaker at Black Hat 2017 on this topic, covering areas such as EXP writing, scanning, data analysis, and maintaining internal network security.
- Research on Chrome security. Assisted in the security audit of 360 OS. Worked on IoT security for smart hardware.
- Led a team to first place in the 40-day Feiyang training, involving 14 teams (as team leader).
- Handled Android vulnerability response for 360Src.
- Participated in external security emergency response for several corporate products.

Suzhou Huolian Intelligent Communication Co., Ltd., CEO
2014/06 – 2015/08

Founder of the company, our product is a voice-centric stranger social APP called "Nuanyu." Secured Series A funding, over ten million in financing.

Nuanyu is a telephone social APP, a thrilling social tool for young people. It primarily facilitates instant calls to chat about topics of interest. Users can share life's beautiful moments through captivating photos and texts, send gifts to each other, displayed through lovely animations. Features like "Arrow to the Heart" and chat rooms allow group chats, games, and private conversations for interested parties. Nuanyu enables users to make direct phone calls to new friends from all corners of the world who share common interests. Users can also earn "Nuanyu coins" through voice interactions, which can be exchanged for cash or used to purchase items in the online store, making it a fun, useful, and exciting social APP.

Nation University of Singapore, Invited visiting scholar
2013/10 – 2014/05

- Conducted research on PC and mobile payment security using the Model Checking method, identifying over a dozen types of attack methods. Presented a keynote speech on payment security vulnerability exploration and protection at the International Advanced Information Security Conference (Syscan360) in November 2016.

Beijing iQIYI Company, Business Intelligence Department (Internship)
2013/05 – 2013/07

- Participated in iQIYI's 'One Search, Hundred Displays' precise advertising project, mainly responsible for data management and data mining. The project involved obtaining user data from Baidu, mining for user information to determine gender, age, interests, and search orientation in the last 30 days, and implementing targeted ad placements during video playback.
- Responsible for building the data display platform for the Business Intelligence Department, using technologies like Hadoop, Python, and Shell.

张清

zhangqingsdu@gmail.com

+86 19800211550

06/10/1989

教育经历

山东大学, 硕士

09/2012 – 06/2015

系统安全与隐私保护

新加坡国立大学, 受邀访问学者

10/2013 – 05/2014

Model Checking on Security

山东大学, 学士

09/2008 – 06/2012

计算机科学与技术软件工程专业

获奖

- 漏洞挖掘ID：cnwatcher，Zhang Qing。
- 谷歌等国际知名公司CVE安全漏洞致谢100+。
- 2022荣耀全年漏洞挖掘第一名；2023荣耀全年漏洞挖掘二等奖；总榜第一名。
- 2016华为云服务奖励计划漏洞挖掘第一名；2022年华为全年漏洞挖掘二等奖。
- 2016，2021-2023魅族全年漏洞挖掘第一名；总排行第一名。
- 2020一加全年漏洞挖掘第一名。
- 2018 OPPO全年漏洞挖掘第一名；双节漏洞活动第一名。
- 2017-2018，SmartOS众测漏洞挖掘第一名。
- 2017年三星安全漏洞致谢总数第一名。
- 2016小米全年漏洞挖掘第二名。
- 爱春秋知名Android和支付安全讲师，课程被学习次数40w+。

语言

- CET-6, 听说读写能力良好。

工作经历

字节跳动, 资深隐私和安全专家

09/2019

2次个人攻坚突破奖，3次协作共赢奖。2次绩效E。

漏洞挖掘

- 问题发现：面向公司所有产品的移动端安全漏洞挖掘发现数百漏洞，包括众多核心业务的RCE、LCE、账户接管等漏洞。
- 工具建设：负责移动端一二代漏洞扫描引擎建设。

隐私蓝军负责人+隐私技术小组负责人

- 问题发现：带领团队开展相关检查专项，发现数千问题。
- 工具建设：建设APP隐私评估审计平台，检测APP使用过程中隐私数据生命周期流转使用情况； 阿波罗照明弹，APP行为和网络流量照明；三方sdk信息收集数据库，与法务和合规同学共同推进制定了三方SDK数据共享披露常态化方案，解决三方SDK隐私分析覆盖不全、入口不明、版本关系复杂，流程无法闭环的问题。
- 规则制定：负责制定隐私安全技术原则细则；通用性隐私和合规技术测试框架，解决了隐私问题挖掘只有checklist造成的大而不全的问题，从而隐私技术审计有了一个可以执行的指导思想。

Tiktok蓝军

- Tiktok隐私和安全漏洞挖掘；外部事件应急；负责TC透明中心移动端代码的安全审计。

APP签名管理系统建设

- 发现签名管理中的安全问题并推负责推动风险治理和云端签名插件建设、签名轮转、外部监控等一系列签名管理安全问题。

财经、医疗、社交等多个业务的一段时间的SDLC负责人

小米, 安全工程师

01/2017 – 03/2019

- IOT、手机漏洞挖掘；账号风控。
- **演讲**：Hitb2018、Syscan2018演讲，从量变到质变一种新的漏洞挖掘方式，有专利。
- **演讲**：Hitb2017 200个Android漏洞挖掘。
- **演讲**：T00LS android应用安全SDL流程与防护。

证书

- 2022，IAPP 信息隐私资深专家（FIP）
- 2022，IAPP 国际注册信息隐私专家（CIPP/E，欧盟GDPR方向）
- 2021，IAPP 国际注册信息隐私技术专家（CIPT）
- 2011, IBM DB2 730认证；2009 IBM UML建模语言认证
- 2010，通用管理能力水平等级证书
- OWASP终身会员

论文和部分演讲

- A类顶会一作 NDSS 2023：Post-GDPR Threat Hunting on Android Phones: Dissecting OS-level Safeguards of User-unresettable Identifiers
- Blackhat 2023：Revisiting Stealthy Sensitive Information Collection from Android Apps
- 华为 2023：从Android看鸿蒙-移动设备隐私安全面面观
- Hitb 2022：Import library, import liability: Analyzing Sensitive Information Collection of Third-party SDKs
- A类顶会一作 MobiCom 2022：Assessing Certificate Validation User Interfaces of WPA Supplicants
- BlackHat 2021：Hey, You, Get off My Private Data: Do Apps Respect Your Privacy as They Claim?
- Hitb 2021：Stay Off My Private Data: A Framework to Examine Mobile App Privacy Claims
- ISC 2021：“后门”寻找之旅：表里不一的Android权限认证机制
- HITB 2020，阿里 2020：The Secret Codes Tell the Secrets

职业技能

- 擅长Android逆向、漏洞挖掘等，熟练使用JEB、IDA等工具，熟悉二进制等。
- 了解web常见安全攻击和防护方案，以及基本的web安全漏洞的挖掘。

奇虎360, 安全工程师（SP+北京户口）

08/2015 – 12/2016

- 企业内部的Android SDL的建立、维护以及企业内部的Android安全培训。
- 企业Android产品的日常安全审计，建立漏洞库，维护企业内部APP安全。
- 3G/4G虫洞漏洞安全研究；**演讲**：Black Hat 2017此议题演讲者，（EXP编写、扫描、数据分析、维护内网安全等）。
- Chrome安全研究。辅助360 OS安全审计。智能硬件IOT安全。
- 40天飞扬培训14支队伍第一名（队长）。
- 360Src Android漏洞响应处理。
- 多次参与企业部分产品的外部安全应急响应。

苏州火联智能通信有限责任公司, CEO

06/2014 – 08/2015

公司创始人，产品是一款以语音为主的陌生人社交APP：暖语。A轮，千万+融资。

暖语是一款电话社交APP，是一个刺激年轻人心跳的社交工具。主要通过即时通话，随时畅聊你感兴趣的话题，并且可以通过精彩的图片和文字分享生活中的美好点滴，可以互相赠送礼物，并可以通过漂亮的动画的形式展示出来；一箭倾心和聊天室功能可以群组聊天玩游戏，并且感兴趣的双方可以一起牵手私聊。通过暖语可以以最直接的打电话的形式结识来自天涯海角却与你有共同话题的新朋友，亦可以通过语音的形式去赚取暖币，暖币可以直接兑换现金，亦可以购买在线商城物品，是一款好玩、有用、刺激的社交APP。

新加坡国立大学, 受邀访问学者

09/2013 – 05/2014

- 使用Model Checking方法研究PC和移动支付安全，发现十几种类型的攻击方式，并于2016年11月在国际前瞻信息安全会议（Syscan360）上发表基于支付安全漏洞挖掘和防护的主题演讲。

北京爱奇艺公司, 商务智能部（实习）

05/2013 – 07/2013

- 参与爱奇艺公司一搜百映精准广告投放项目，主要职责：数据管理、数据挖掘。项目主要是从百度取得用户数据，对用户信息进行挖掘，得到用户的性别、年龄、兴趣以及30天内的搜索取向，在视频播放时进行贴片式定向广告投放。
- 负责商务智能部数据展示平台搭建工作，主要技术：Hadoop+python+Shell。