# 杨荣海

深圳
深信服科技
(+86) 13662258083
ronghai1130@gmail.com

## 学历

2013 – 2017 博士, 香港中文大学信息工程专业.
2009 – 2013 学士, 中国科学技术大学信息安全专业.

## 研究方向

网络安全 AI 安全
AI for Security

## 工作经历

2017–2020 深信服科技, 创新研究院, 安全技术专家.
2020–2021 深信服科技, 网络安全能力部, 架构师.
2021-2022 深信服科技, 网络安全能力部, 部门主管, 负责公司网络安全与数据安全核心能力建设，网络安全能力公司/市场认可达到业界一流水平.
2023-至今 深信服科技, 天问 *AI* 部, 部门主管, 负责公司安全 GPT 业务。国内首个发布并广泛商用的安全领域大模型，首个通过网信办双重备案.

## 科研论文

Oct 2024 **Ronghai Yang**, Xianbo Wang, Kaixuan Luo, Xin Lei, Ke Li, Jiayuan Xin and Wing Cheong Lau, "SWIDE: A Semantic-aware Detection Engine for Successful Web Injection Attacks". in ACM CCS (CCF-A), 2024.

Oct 2023 **Ronghai Yang**, Xin Lei, and Jiayuan Xin, "Beyond Generation: Detecting Zero-Day Web Attacks via Security-GPT". GeekCon 2023 （This work received the Frontier Breakthrough Award).

Sep 2021 Shangcheng Shi, Xianbo Wang, Kyle Zeng, **Ronghai Yang**, Wing Cheong Lau, "An Empirical Study on Mobile Payment Credential Leaks and Their Exploits". SecureComm, 2021.

Aug 2021 **Ronghai Yang**, Xianbo Wang, Cheng Chi, Dawei Wang, Jiawei He, Shiming Pang, and Wing Cheong Lau, "Scalable Detection of Promotional Website Defacements in Black Hat SEO Campaigns," in USENIX Security Symposium (CCF-A), Aug 2021.

Dec 2020 Xianbo Wang, Wing Cheong Lau, Yikang Chen, Shangcheng Shi, **Ronghai Yang**, "Fingerprint-jacking: Practical Fingerprint Authorization Hijacking in Android Apps," BlackHat Europe Briefings, Dec 2020.

Mar 2019 Xianbo Wang, Wing Cheong Lau, Shangcheng Shi, **Ronghai Yang**, "Make Redirection Evil Again URL Parser Issues in OAuth," in Black Hat Asia, Mar 2019.

Aug 2018 **Ronghai Yang**, Wing Cheong Lau, Jiongyi Chen, Kehuan Zhang, *"Vetting Single-Sign-On SDK Implementations via Symbolic Reasoning,"* in the 27th USENIX Security Symposium (CCF-A), 2018. (This work received the 2nd Runner-up Internet Defense Prize 2018 from USENIX and Facebook).

Feb 2018 Jiongyi Chen, Wenrui Diao, Qingchuan Zhao, Chaoshun Zuo, Zhiqiang Lin, XiaoFeng Wang, Wing Cheong Lau, Menghan Sun, **Ronghai Yang** and Kehuan Zhang, *IoTFuzzer: Discovering Vulnerabilities in IoT Devices With a Mobile App Based Fuzzing Framework*. to appear in the Network and Distributed System Security Symposium (NDSS).

Jul 2017 **Ronghai Yang**, Wing Cheong Lau and Shangcheng Shi, *Breaking and Fixing Mobile App Authentication with OAuth2.0,* in 第 15 届应用密码和网络安全会议 ( ACNS 2017 ) .

Nov 2016 **Ronghai Yang**, Wing Cheong Lau and Tianyu Liu, *Signing into One Billion Mobile App Accounts Effortlessly with OAuth2.0,* 黑帽子大会 ( Black Hat Europe 2016 ) .

May 2016 **Ronghai Yang**, Guanchen Li, Wing Cheong Lau, Kehuan Zhang and Pili Hu, *Model-based Security Testing: an Empirical Study on OAuth 2.0 Implementations*, 第 11 届亚洲计算机与通信安全会议 ( AsiaCCS 2016 ) .

Nov 2015 **Ronghai Yang***, Huanle Xu*, Zhibo Yang and Wing Cheong Lau, *Solving Large Graph Problems in MapReduce-Like Frameworks via Optimized Parameter Configuration*, 第十五届国际并行算法和结构会议 (ICA3PP 2015).

Oct 2014 **Ronghai Yang***, Pili Hu*, Yue Li and Wing Cheong Lau, *Application Impersonation: Problems of OAuth and API Design in Online Social Networks*, 第二届在线社交网络会议 (ACM COSN 2014).

Oct 2014 **Ronghai Yang**, Pili Hu and Wing Cheong Lau, *Model-based Testing for Security Flaw Detection in OAuth2.0 (Poster)*, 第二届在线社交网络会议 (ACM COSN 2014).

* These authors contributed equally to this work.

## 科研项目

2024 项目负责人，主持深圳市重点科技创新项目: 重 202403011 面向大数据平台的数据要素化安全防护技术研发及应用 ( 2000 万元 ) .

2025 课题负责人，参与 2025 年广东省重点领域研发计划项目：新一代人工智能专项 ▪ 核心算法与数据安全 -多模态大模型安全体系研究及应用 ( 1000 万元 ) .

## 科研项目获奖情况

2025 中央网信办举办的《人工智能技术赋能网络安全应用测试》比赛「大模型生成内容安全风险检测」第一名

2024 中国通信学会年度十大网络和数据安全重大科技进展：《AI 赋能攻防实战场景下的网络安全运营关键技术及应用实践》项目的主要完成人

2024 安全 GPT 入选 2024 年数博会优秀科技成果

2024 中央网信办举办的《人工智能技术赋能网络安全应用测试》比赛「钓鱼邮件识别场景」第一名

2023 安全 GPT 入选 2023 年世界互联网大会领先科技成果手册《科技之魅》

## 个人获奖情况

2024 入选深圳市南山区十大创新工匠

2023 GeekCon 前沿突破奖

2020 入选深圳 25 周年 25 位优秀博士后

2018 互联网防御奖项 ( Internet Defense Prize from USENIX Symposium ) 首个亚洲获奖团队

2018 深圳市海外高层次人才

2012 国家奖学金