张明明

13820960306 | zmm18@mails.tsinghua.edu.cn

教育经历

清华大学 2018.09 - 2023.06

网络安全 博士 网络研究院 网络与信息安全实验室 导师：段海新教授 北京

南开大学 2014.09 - 2018.06

信息安全与法学双学位 本科 计算机与控制工程学院 天津

研究方向

概述：主要进行网络协议相关的安全研究，包括对HTTP、DNS、TLS等基础协议在协议设计、协议部署中的漏洞挖掘和测量分析；特别是对身份认证相关的安全策略在云服务、CDN、Web和DNS托管服务等实际场景中的部署实践展开实证性研究。

1. 基于公钥基础设施的身份认证机制的安全缺陷分析

a. 研究发现基于Web PKI中共享证书的生态缺陷，攻击者可以绕过HTTPS的安全防护，破坏通信过程的安全性。针对这类攻击模型展开了实证研究，对国内外主流网站展开了测量与实证分析，发现很多流行应用可被劫持，包括在线支付、第三方登录、邮件服务等。多家国内外知名厂商可受影响，包括微软、京东、网易等。

b. 研究成果已形成学术论文发表在网络安全四顶会之一、CCF A类会议 ACM CCS 2020中。

2. 公共云托管服务对域名身份认证的安全缺陷分析

a. 研究发现公共托管服务在域名接入环节存在安全缺陷，攻击者可以利用这些服务劫持用户域名，并进一步实施钓鱼、Cookie泄漏或域名滥用等攻击。提出半自动化方法，发现并检测出多类主流服务存在此类漏洞，可影响多家国内外知名厂商，包括亚马逊云、阿里云、腾讯云等。

b. 基于上述公共服务及海量被动DNS日志数据，首次设计并实现了一个针对域名接管的大规模检测系统。与其他工作相比，该系统具备较高的检测效率和结果覆盖率。目前该检测系统已得到工业界的实际部署。

研究成果

学术论文 (一作3篇，合作5篇；其中A类会议5篇)

- **Mingming Zhang**, Xiaofeng Zheng, Kaiwen Shen, Ziqiao Kong, Chaoyi Lu, Yu Wang, Haixin Duan, Shuang Hao, Baojun Liu, Min Yang. Talking with Familiar Strangers: An Empirical Study on HTTPS Context Confusion Attacks. **(ACM CCS 2020, CCF A、网络安全四大顶会之一, 录用率 121/715=16.9%)**
- **DareShark: Detecting and Measuring Security Risks of Hosting-Based Dangling Domains.** (SIGMETRICS 2023, 高性能领域A类会议，2rd-round review)
- **Mingming Zhang**, Baojun Liu, Chaoyi Lu, Jia Zhang, Shuang Hao, Haixin Duan. Measuring Privacy Threats in China-Wide Mobile Networks. **(FOCI 2018)**
- Xiang Li, Baojun Liu, Xuesong Bai, **Mingming Zhang**, Qifan Zhang, Zhou Li, Haixin Duan and Qi Li. Ghost Domain Reloaded: Vulnerable Links in the Domain Name Delegation and Revocation. **(NDSS 2023, CCF A、网络安全四大顶会之一)**
- Chuhan Wang, Kaiwen Shen, Minglei Guo, Yuxuan Zhao, **Mingming Zhang**, Jianjun Chen, Baojun Liu, Xiaofeng Zheng, Haixin Duan, Yanzhong Lin, Qingfeng Pan. A Large-scale and Longitudinal Measurement Study of DKIM Deployment. **(Usenix Security 2022, CCF A、 网络安全四大顶会之一, 录用率 256/1492=17.2%)**
- Kaiwen Shen, JianYu Lu, Yaru Yang, Jianjun Chen, **Mingming Zhang**, Haixin Duan, Jia Zhang, Xiaofeng Zheng. HDiff: A Semi-automatic Framework for Discovering Semantic Gap Attack in HTTP Implementations. **(DSN 2022, CCF B，录用率 49/262=18.7%, Best Paper Runner-Up).**

- Yiming Zhang, Mingxuan Liu, **Mingming Zhang**, Chaoyi Lu, Haixin Duan. Ethics in Security Research: Visions, Reality, and Paths Forward. **(EthiCS 2022, 最佳学生论文奖Best Student Paper获奖论文(比例1/5))**
- Chaoyi Lu, Baojun Liu, Zhou Li, Shuang Hao, Haixin Duan, **Mingming Zhang**, Chunying Leng, Ying Liu, Zaifeng Zhang, Jianping Wu. An End-to-End, Large-Scale Measurement of DNS-over-Encryption: How Far Have We Come?. **(IMC 2019, THUCPL A, IRTF ANRP 2020 Award Winner, 录用率156/625=25%, 最佳论文提名(比例3/39)，社区贡献奖提名(比例2/39))**

标准专利

- 郑晓峰, **张明明**, 沈凯文, 陈震宇, & 段海新. (2021). 网络通信安全性的识别方法,装置,电子设备及存储介质. CN112311884A.

荣誉奖励

龙湖学术新星奖学金	2022.09
清华大学研究生二等奖学金	2020.10
GeekPwn国际极客安全挑战赛第一名（入选名人堂）	2019.10
中国互联网发展基金会 网络安全奖学金	2018.08
南开大学优秀毕业生、优秀本科生学位论文	2018.06
国家奖学金	2017.11
南开大学一等奖学金、三好学生	2014-2016
互联网研究任务组应用网络研究奖（IRTF ANRP 2020）	2020.07
DSN会议最佳论文奖提名	2022.07
IMC会议最佳论文奖提名	2019.10
IMC会议社区贡献奖提名	2019.10
EthiCS'22最佳学生论文	2022.08
清华大学信息化技术中心优秀共产党员	2021-2022
全程参加中宣部和国家广电总局主办的《伟大征程》建党100周年专项	2021.07

其他项目和科研经历

1. **华为技术有限公司研究项目. 加密流量分析**
   - 主要负责恶意样本流量SSL特征分析、客户端指纹与服务端证书特征提取
2. **论客科技（广州）有限公司研究项目. 邮件协议与内容安全**
   - 主要参与DKIM协议部署和验证的测量分析
3. **HTTP透明代理的隐私威胁研究**
   - 主要分析HTTP透明代理的网络劫持行为和安全威胁，对中国范围内移动互联网环境下的透明代理展开大规模测量
4. **参与撰写《网络安全国际学术研究进展》人民邮电出版社**
5. **参与撰写《互联网基础设施与软件安全：年度发展研究报告(2020)》 人民邮电出版社**

实习经历

奇安信技术研究院 2018.07 - 至今

羲和实验室 北京

- 参与设计和搭建公钥证书数据库，负责解析、处理并分析亿级证书数据

学术服务

会议外部审稿：NDSS'22 & '21, CCS'19，ACSAC'21, ESORICS'20, ICDSC'21

竞赛组织：参与DataCon大数据安全分析竞赛中加密流量检测赛道出题