远程办公系统安全综述

杨泽霖[1,3], 王基策[3,4], 徐 斐[1,3], 黄宇航[3], 艾铭超[2,3], 马 慧[1,3], 王 鹤[1,2,3], 张玉清[1,2,3]

[1]西安电子科技大学网络与信息安全学院 西安 中国 710071
[2]西安电子科技大学杭州研究院 杭州 中国 311231
[3]中国科学院大学国家计算机网络入侵防范中心 北京 中国 101408
[4]北京计算机技术及应用研究所 北京 中国 100854

摘要 受新型冠状病毒肺炎的影响, 远程办公这种新型办公方式在短时间内迅速发展并被社会广泛应用, 由此引发的远程办公系统的安全问题显得越发急迫和突出。目前, 远程办公系统安全的相关研究仍处于起步阶段, 其研究结果并未不足以完全解决远程办公系统发展中的安全问题。为使研究人员系统化地了解目前的研究进展, 本文首次归纳总结了远程办公系统的安全问题, 并撰写了本综述。本文首先回顾了远程办公系统的发展历程, 指出了远程办公系统在不同应用场景中特有的安全需求和问题, 然后根据远程办公系统的技术架构将其分为虚拟专用网络、远程桌面控制、团队协作平台三种类型。在调研了近 5 年 EI 数据库、Web of Science 核心数据库和 CCF 推荐网络与信息安全国际学术会议中发表的与远程办公安全相关论文以及其他相关的高水平研究工作的基础上, 本文对以上三类远程办公系统中存在的安全问题进行了系统性的分析和总结, 尤其是重点分析了团队协作平台这种新型办公方式的安全问题。根据团队协作平台的架构和功能以及攻击者常用的攻击方式将团队协作平台的安全风险分为 5 类: 第三方小程序安全、通信协议安全、客户端安全、云服务端安全、侧信道分析。最后进一步指出了远程办公系统安全研究所面临的挑战和机遇, 为远程办公系统安全未来的研究指出了方向。

关键词 远程办公; 安全; 虚拟专用网络; 远程桌面控制; 团队协作
中图法分类号 TP309 **DOI 号** 10.19363/J.cnki.cn10-1380/tn.2022.11.02

Survey of Telecommuting System Security

YANG Zelin[1,3], WANG Jice[3,4], XU Fei[1,3], HUANG Yuhang[3], AI Mingchao[2,3], MA Hui[1,3], WANG He[1,2,3], ZHANG Yuqing[1,2,3]

[1] School of Cyber Engineering, Xidian University, Xi'an 710071, China
[2] Hangzhou Institute of Technology, Xidian University, Hangzhou 311231, China
[3] National Computer Network Intrusion Protection Center, University of Chinese Academy of Sciences, Beijing 101408, China
[4] Beijing Institute of Computer Technology and Applications, Beijing 100854, China

Abstract Affected by the Corona Virus Disease 2019 (COVID-19), telecommuting, a new type of office, has developed rapidly in a short period of time and has been widely used in society, and the resulting security problems of telecommuting systems have become more and more urgent and prominent. At present, the research on the security of telecommuting systems is still in its infancy, and the research results are not enough to completely solve the security problems in the development of telecommuting systems. In order to systematically understand the current research progress researchers, this paper summarizes the security problems of telecommuting systems for the first time, and writes this review. This paper first reviews the development process of the telecommuting system, points out the unique security requirements and problems of the telecommuting system in different application scenarios, and then divides the telecommuting system into virtual private network (VPN), remote desktop control and teamwork platform, according to the technical architecture of the telecommuting system. Based on nearly 5 years of research on telecommuting papers published in the EI Database, Web of Science database and CCF recommended international conference on network and information security, as well as other related high-level research work, this paper systematically analyzes and summarizes the security problems existing in the above three types of telecommuting systems, especially focusing on the security problems of teamwork platforms, a new type of telecommuting. According to the architecture and function of the teamwork platform and the attack methods commonly used by attackers, the security risk of teamwork platforms are divided into five categories: third-party APP security, communication protocol security, client security, cloud server security, and side channel analysis. Finally, the challenges and opportunities faced by the telecommuting system security research institute are pointed out, and the direction for the

通讯作者: 王鹤, 博士, 讲师, Email: hewang@xidian.edu.cn。
本课题得到国家自然科学基金重点项目: 多源漏洞数据智能分析和漏洞智能利用与挖掘研究(No. U1836210)的资助。
收稿日期: 2022-07-05; 修改日期: 2022-09-29; 定稿日期: 2022-09-30

future research of telecommuting system security is pointed out.

Key words telecommuting; security; VPN; remote desktop control; teamwork

1 引言

随着互联网和信息技术的快速发展和普及, 远程协作办公这种新型工作方式开始出现。传统的物理空间工作模式也逐渐扩展至由互联网主导的新型远程办公工作模式, 在家办公、异地办公、移动办公等非本地办公形式得以实现。

远程办公最初满足的需求仅是利用专用网实现远距离通信, 而发展到今天, 远程办公意味着一个满足了非接触、跨时区、跨地域、跨平台、移动化等协同办公需求的综合性功能系统。如图 1 所示, 回顾了远程办公系统 40 年间发展过程中的重要节点。实现远程办公最早的方法是直接架设专线, 如数字数据网(Digital Data Network, DDN), 利用数字信道提供永久性连接电路, 虽然这种方案在传输质量, 传输速率以及安全性方面都堪称绝佳, 但远距离架设专线的成本极高, 大多数企业无法承担, 并未得到大规模推广应用。20 世纪 90 年代, 虚拟专用网(Virtual Private Network, VPN)的出现成为一个转折, 从传统的专线 VPN 到基于用户端设备的 VPN, 再到多协议标签交换(Multi-protocol Label Switch, MPLS)协议 VPN、安全套接层(Secure Sockets Layer, SSL)协议 VPN, 层出不穷的 VPN 技术不断发展, 在很长一段时间内成为大多数公司解决子网通信, 远距离办公的主流方案, 至今仍活跃在大众视野。但 VPN 仍存在严重的安全问题, 仅从 2020 年至今, VPN 的 CVE 漏洞就高达 500 多个[1], 占据 VPN 漏洞总数的 23%。同一时期, 操作系统也开始为计算机终端提供远程桌面服务, 但这一功能更多被专业计算机人员使用。进入 21 世纪, 随着云服务的兴起, 借助第三方平台满足企业的办公需求逐渐受到用户青睐, Zoom、Office 365、Microsoft Teams 等多种远程办公平台应用相继上线, 它们所提供的丰富功能让远程办公进入一个新的时代。

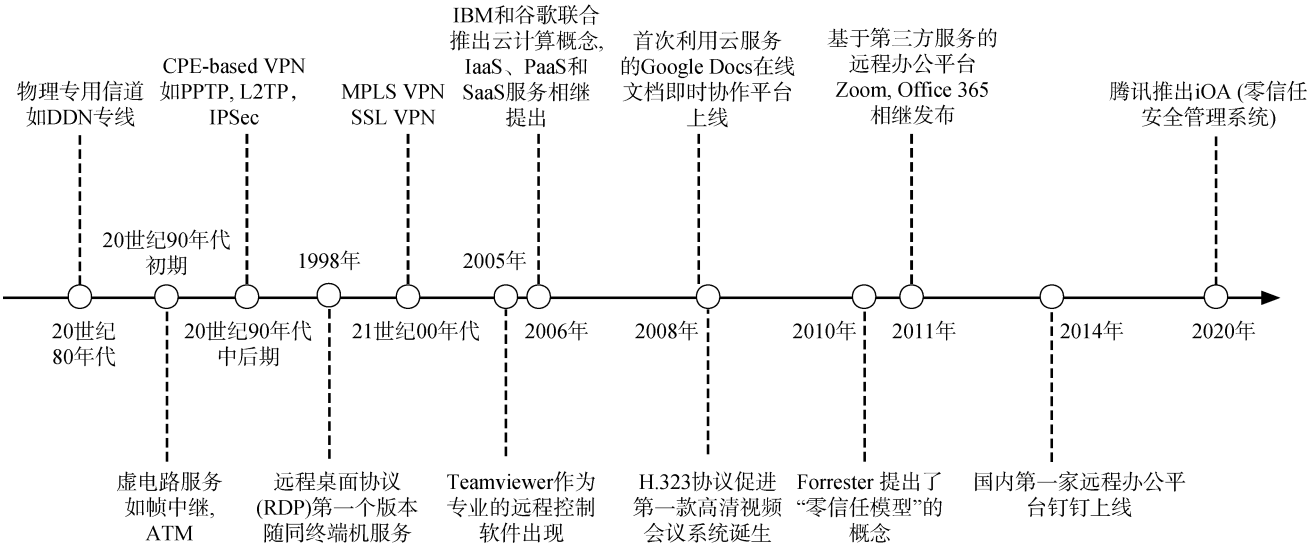

图 1 远程办公发展历程

Figure 1 The history of telecommuting

近几年受新冠疫情影响, 远程办公快速发展, 中国互联网络信息中心发布的第 49 次《中国互联网络发展状况统计报告》显示[2], 截至 2021 年 12 月, 在线办公用户规模达 4.69 亿, 同比增长 35.7%, 成为用户规模增长最快的应用之一。由于远程办公用户的激增, 安全问题也愈发严重。2020 年, Zoom 视频会议被曝出存在严重漏洞, 这些漏洞可被用来监视用户, 升级系统特权以及捕获 Windows 账号[3]。此外, Zoom 网络教室和电话会议频频遭到破坏和“劫持”, “Zoom-bombing(Zoom 轰炸)”受到广泛关注[4], 加剧了公众对远程办公安全性的担忧。文献[5]的研究表明, 团队协作平台仍存在严重的安全风险, 敌手利用平台集成的第三方 APP 可以滥用平台提供的 API 扰乱远程办公的正常秩序。不仅如此, 由于团队协作平台缺乏细粒度的权限管理模型, 用户可以获取自身权限外的信息, 导致机构信息和合法用户身份信

息的泄露。这些安全事件不仅会给员工的正常工作带来困扰, 还会导致机构的敏感信息泄露, 造成不可估量的损失, 阻碍机构的复工复产, 甚至威胁国家的经济发展。尽管远程办公领域的发展已经有 50 余年, 但是现阶段针对远程办公安全的研究较少, 并且尚无专门的综述总结该领域的安全问题及现状。为了使研究人员更加清楚地了解远程办公安全研究现状, 促进远程办公系统安全发展, 本文首次对远程办公系统安全现状进行了深入分析, 撰写了本综述, 并指出了挑战和机遇以及未来的研究方向, 本文主要贡献如下:

1) 系统地介绍了目前被广泛应用的远程办公方案, 根据其架构和原理将远程办公分为三种类型: 基于 VPN 的远程办公、基于远程桌面控制的远程办公、基于团队协作平台的远程办公, 并对远程办公系统中存在的安全风险进行了全面讨论。

2) 调研了近 5 年 EI 数据库、Web of Science 核心数据库和 CCF 推荐网络与信息安全国际学术会议中发表的与远程办公安全相关论文以及其他相关的高水平研究工作, 分析总结了 3 种类型的远程办公系统的安全问题, 通过分类归纳的方式阐述了不同安全问题给远程办公系统带来的安全威胁, 并总结了现有的应对策略和防御方法。

3) 指出了远程办公安全在未来面临的挑战和机遇, 并针对不同挑战提出了不同的解决方案, 为未来远程办公的相关研究人员指出了热点和研究方向。

2 远程办公系统类型及应用场景安全问题

2.1 远程办公系统类型

远程办公系统目前已经被广泛应用于各行各业, 其中 VPN 和远程桌面控制常被应用于互联网相关行业, 帮助用户实现远程资源访问, 但 VPN 和远程桌面控制无法满足企业远程办公的全部需求(例如: 在线会议、共享协作等)。团队协作平台的出现更好地满足了企业远程办公的需求, 并首次帮助企业实现真正意义上的远程办公。尽管 VPN 和远程桌面控制技术早在 20 世纪 90 年就已经出现, 但如今团队协作平台才是企业远程办公的首选[2]。下面对以上 3 种类型远程办公系统进行简要介绍。

2.1.1 VPN 虚拟专用网

VPN 通过模拟点对点专用链接的方式在公共网络上建立了一条安全、稳定、私密的隧道, 利用该隧道可以实现加密数据通信及远程访问, 从而广泛应用于企业远程办公, 帮助远程企业用户与企业内部网建立可信的安全连接。

2.1.2 远程桌面控制

远程桌面控制和 VPN 解决远程办公问题的核心思想十分相似。VPN 借助公共网络实现远程资源访问, 远程桌面控制提供了远程访问工作计算机的途径。因此, 相较于 VPN, 用户利用远程桌面控制可以完全控制工作计算机, 从而使用其全部软硬件资源。这种实时交互的方式为用户使用提供了便利。

随着远程办公需求的增加, 远程桌面控制被广泛使用, 从操作系统直接集成的远程桌面控制协议如 Microsoft 远程桌面协议(Microsoft Remote Desktop Protocol, MS-RDP)到专业的远程桌面控制软件如向日葵(Sunlogin)、Teamviewer 等, 远程桌面控制在系统兼容性, 安全性和操作的便捷性, 流畅性等各个方面进行了不断地更迭和改进以满足远程办公用户的需求。

2.1.3 团队协作平台

针对远程办公问题, 团队协作平台提供一种与 VPN 和远程桌面控制不同的解决思路。团队协作平台的核心思想是将公司内部的资源环境整合在一个第三方可信服务平台上, 通过网络模拟真实办公环境来实现远程协同办公的目的。这种方式不仅降低了企业远程办公的成本, 而且满足了企业远程办公的全部需求。

随着计算机技术、通信技术和网络技术的突飞猛进, 目前团队协作平台的功能也在不断完善(业务流程审批、考勤、在线会议、协作共享等), 帮助用户实现非本地办公: 在家办公、移动办公、异地办公。

2.1.4 小结

VPN 是解决远程办公的传统方案, 但配置 VPN 设备对于企业是一个不小的负担, 远程桌面控制的安全性相对较弱, 因而大多数远程桌面应用程序会通过 VPN 进行隧道传输以增加安全性。这两种方式能实现的功能都非常有限, 而团队协作平台通过整合多方资源可为用户提供多方面服务, 极大地提高了远程办公的安全和效率, 是远程办公未来发展的方向。

2.2 远程办公系统应用场景安全问题

团队协作平台根据不同行业对需求与安全等级的侧重点不同提供了不同类别的服务, 如: 教育领域注重平台的功能性; 企业内部注重平台的安全性; 医疗领域在追求功能性和安全性的同时, 更加注重数据传输的实时性。故本文结合 VPN、远程桌面控制和团队协作平台的使用情况将远程办公系统的应用场景分为教育、企业、医疗, 并指出这三类应用场景的需求和安全问题。

2.2.1 远程教育安全问题

远程教育分为同步交付、异步交付两种模式[6]: 同步交付即实时使用视频会议软件的交互式教学, 异步交付是指学生在教师设定的时间框架内根据自己的合适时间来学习录制好的视频与记录好的讨论板。对 Zoom、Google Hangouts、Microsoft Teams 的调研发现同步交付模式比异步交付模式存在更为严重的安全风险。例如: 学生通常通过点击电子邮件收到的会议链接来进入课堂, 而攻击者可以利用钓鱼邮件的恶意链接诱导学生, 造成信息泄露的风险[7]。文献[8]对远程教育中常用的技术云计算, 学习管理系统(Learning Management System, LMS)以及视频会议系统进行了系统性的安全分析, 其研究结果表明远程办公系统面临的拒绝服务攻击(Denial of service, DoS)/分布式拒绝服务攻击(Distributed Denial of Service, DDoS)、跨站点脚本攻击(Cross Site Scripting, XSS)、未经授权的数据访问、感染恶意程序和用户隐私泄露的风险急剧增加。

除远程授课外, 远程考试的安全和隐私问题也备受关注[9]。远程教育平台必须确保试卷只能在考试期间发布, 并且用户的访问权限需要细粒度的控制, 用户无权查看其他用户的试卷及作答情况, 在保证用户隐私的前提下有效防止作弊。

2.2.2 企业办公安全问题

企业远程办公由来已久, 公司各分部之间的远距离通信以及员工出差时对公司内部资源的访问都属于远程办公的范畴。而疫情造成的地域隔离进一步推动了远程办公系统的大规模部署, 并对协作的高效便捷和安全访问提出了更高的要求。

为确保企业信息的安全, 传统方式是将企业内部网络的业务系统与互联网完全隔离来保障其安全性, 而这显然为在家办公, 异地办公和移动办公等非本地办公形式造成了障碍。因此, 企业常采用 VPN 和远程桌面控制技术, 借助互联网来接入公司内部的业务系统, 但这种方式会导致弱口令攻击、客户信息泄露、网站被攻击篡改、恶意代码攻击等安全问题[10]。2019 年 10 月 Avast 公司发生了一起非面对面环境下的网络泄密事件, 黑客利用员工的用于远程工作的 VPN 账户并通过安全设置中的弱点来入侵公司内部网络并多次绕开了身份验证的过程[11]。此外, 网络环境对远程办公的安全性有至关重要的作用, 不安全的网络环境会造成企业信息泄露, 例如: 攻击者通过嗅探攻击可以窃取企业的信息[12]。

目前 VPN 和远程桌面控制的主要功能是帮助企业、高校、社会机构实现远程资源访问, 而团队协作平台可以帮助企业完成实时交流、在线协作和考勤等多样化的功能需求, 但由于其发展时间相对较短, 安全防护设计方案尚不够完善。例如: 文献[13]的研究表明在线会议的 ID 可被预测, 这导致在线会议的 ID 易被攻击者劫持, 从而造成 Zoom 轰炸, 致使会议无法正常进行。文献[14]指出团队协作平台存在用户隐私信息泄露的安全风险。如何确保用户隐私信息的安全也是团队协作平台急需解决的主要安全问题。

利用人工智能(AI)技术, 通过大数据建模攻击是利用音频实现远程教育和企业远程办公面临的主要安全问题, 攻击者基于社会工程利用摄像头暴露的物理信息推测出用户生活习惯等细节, 从而冒充用户身份[8]。

2.2.3 远程医疗安全问题

远程医疗作为一种医疗卫生服务, 借助信息和通信技术手段使所有的诊断、治疗、咨询、评估等医疗行为可以远程实施, 例如远程病理诊断、远程医学影像诊断、远程监护、远程会诊等服务项目。远程医疗用户数据的传递对时效性具有很高的要求, 医疗数据需要进行跨网络共享, 这个过程中, 用户数据在不同的平台上被操纵, 在不同的网络环境中传输, 使数据暴露给未授权方的风险增加。远程医疗需要用户的实时位置, 以便在紧急情况下使用, 但是这有可能会暴露用户的日常活动[15]。由于健康数据高度敏感, 远程医疗的安全性和私密性应得到严格保护, 防止用户隐私泄露。文献[16]指出恶意的第三方存储凭条可能会导致用户数据泄露, 因此远程医疗要求在整个存储期间保护患者数据的隐私, 防止除患者授权的实体(如医院员工、近亲属等)未经授权访问原始数据或处理数据。

远程医疗使得获取、存储、操作和复制医疗信息和图像变得容易, 但这也为远程医疗引入了新的安全风险, 攻击者可以利用人工智能技术修改、中断或伪造患者图像和信息, 导致用户病情被误诊, 甚至危害用户生命安全。文献[17]针对医疗记录的安全性和认证问题进行了研究, 提出了数字水印技术来解决远程医疗中的认证问题, 有效确保图像真实性并且防止恶意拷贝。

从医院的整体发展需求来看, 传统网络结构无法完全满足医院的发展。文献[18]表明, 应用 VPN 技术可以进一步完善医院信息化建设, 促进医院整体发展, 对患者意义重大。因此 VPN 安全是实现医疗产业完善和长远发展的关键。此外, 随着计算机技术和网络技术的普及, 团队协作平台也成为远程医疗

的常用方式[19]。

3 VPN 虚拟专用网

Cybersecurity Insiders 发布的报告[20]称 2020 年 93%的企业或组织正在使用 VPN 服务来进行远程访问, 但近三年仅 CVE 漏洞库中收录的 VPN 漏洞数量就高达 500 多个[1], 这表明 VPN 仍存在严重的安全问题。本文通过对现有资料的全面分析帮助研究者进一步了解 VPN 安全研究现状。

3.1 VPN 安全风险

隧道是构建 VPN 的关键, 它参与了身份认证、密钥协商、加解密等 VPN 整个生命周期的活动, 因而本文将 VPN 完成远程通信的过程以隧道作为核心分为三个阶段。

3.1.1 隧道建立阶段安全风险

在隧道建立阶段, VPN 主要完成的是身份认证, 密钥协商以及在控制通道中完成的一系列活动。文献[21]通过分析点对点隧道协议(Point to Point Tunneling Protocol, PPTP)VPN 端点和远程认证拨号用户服务(Remote Authentication Dial In User Service, RADIUS)认证服务器之间的通信信息, 分析出受害者客户端和 VPN 端点之间共享的 VPN 会话密钥, 可被用于破坏微软版本的挑战握手认证协议(Microsoft Challenge Handshake Authentication Protocol version 2, MS-CHAP v2)认证, 提升“内部”攻击者权限。文献[22]分析了基于第二层隧道协议(Layer Two Tunneling Protocol, L2TP)/互联网安全协议(Internet Protocol Security, IPSec)的安全机制, 发现 MS-CHAP 的身份认证机制存在漏洞, 可以使攻击者轻易获取登录密码, 而基于网络密钥交换协议(Internet Key Exchange, IKE)的身份认证机制则可能让攻击者获取用于设备验证的共享密钥(Pre-Shared Key, PSK)。文献[23]同样关注到了 IPSec VPN 中 IKE 的密钥协商过程, 研究发现攻击者可通过获得基于最短路径优先(Open Shortest Path First, OSPF)协议网络的访问权限, 发送大量欺骗 IKE 请求数据包到 VPN 服务器实现拒绝服务。文献[24]发现连接 VPN 服务器的机器可能在 VPN 隧道完全建立之前泄露敏感数据, 该研究通过分析大量本地和第三方 VPN 客户端, 发现只有 Mullvad for iOS 在强制网络中可以正常建立连接, 其他均存在死锁或流量泄漏。

3.1.2 数据传输阶段安全风险

在数据传输阶段, 最重要的是确保信息不会被篡改和破解。虽然大多数 VPN 都会对数据提供加密服务, 但这并不意味着安全, 文献[25]分析了 2017 年 5 月 Google Play 中收集到的 84 款 VPN 应用, 发现一些应用程序在 VPN 中添加了新的隧道协议以隐藏特性和逃避网络审查技术, 如深度数据包检测(Deep Packet Inspection, DPI)。然而, 修改后的协议经常采用脆弱的密钥协议或用自定义混淆替换标准加密导致攻击者非常容易解密 VPN 流量。IPv6 流量也常常被 VPN 提供商所忽视[26], 文献[27]对 Google Play 应用中提取的 283 个 Android VPN 应用进行了深入分析, 结果表明有 84%的应用程序泄露了 IPv6 流量。文献[28]的研究表明, 攻击者虽然无法直接看到 VPN 隧道内被加密的数据包, 但可以通过数据包的大小及客户端响应时间对一些关键信息进行猜测从而劫持被 VPN 保护的协议如 TCP, DNS。

此外, VPN 在这一阶段最容易遭受拒绝服务攻击。文献[29]提出了一个使用数据平面开发套件(Data Plane Development Kit, DPDK)实现的能够对 VPN 实现发起和评估泛洪攻击的框架, 攻击者试图用相互之间没有因果关系的数据包(无状态)来耗尽受害者的资源, 以此评估 VPN 对基于洪水的 DoS 攻击的弹性。

3.1.3 隧道终止阶段安全风险

基于安全的角度考虑, 本文所指的终止是指意外终止, 当 VPN 隧道由于各种原因断开连接时安全防护显得尤为重要。文献[30]开发了一个通用的测试套件并应用于 62 个不同的 VPN 提供商, 其研究结果表明当隧道出现故障时, 共有 25 个 VPN 服务的用户流量发生泄漏, 一些评价良好的 VPN 提供商虽然在客户端中设置了杀死开关。但是, 它要么被默认禁用, 要么被设计为只针对选定的应用程序。文献[26]设计了一款 VPNalyzer 测试工具, 针对 80 家桌面平台 VPN 软件测试其 VPN 服务的安全性, 研究结果表明, 当 VPN 掉线时, 18 家服务商没有将连接强制中断, 任其转到普通网络上, 且很多软件考虑到可用性, 往往会在连接中断的时候启用标准 DNS 服务, 直接导致用户大量的网络浏览信息被泄露。

3.2 小结

在 VPN 通信的整个生命周期中, 最易受到攻击的是数据传输阶段, 分析流量和执行拒绝服务攻击是攻击者常常采用的手段。攻击危害最大的是隧道建立阶段, 一旦身份认证失效, 内网大门将会向攻击者完全敞开。隧道终止阶段的安全问题最容易被忽视, 此阶段缺乏强制防护措施会导致用户在不安全的通路上传输信息。

实行多身份认证方式叠加, 加强网络审查, 识别恶意流量, 实施强度更高的加密算法, 完善全阶

段的网络安全保护机制是解决目前 VPN 面临的安全威胁的主要办法, 而隧道协议的不断改进以及新的安全架构的提出也是提高 VPN 安全性的未来趋势。

4 远程桌面控制

远程桌面控制技术在被广泛应用的同时, 其安全风险也不应被忽视。远程桌面控制实时交互的功能在方便用户使用的同时, 也为攻击者提供了获取隐私的途径。远程桌面控制应用的多样性旨在为不同环境下的用户提供更多选择, 却为远程桌面控制系统带来了多样化的漏洞, 如 RDP、VNC(Virtual Network Computing)这两种广泛使用的远程桌面控制应用程序存在严重的安全问题, 包括且不限于远程代码执行、权限提升等。本文通过对现有资料的分析帮助研究者进一步了解远程桌面控制的安全研究现状。

4.1 远程桌面控制的安全风险

在远程桌面控制应用及协议中, 流量加密机制不足以防止隐私信息泄漏, 且远程桌面系统可被破解或欺骗, 成为攻击者的突破口。本文将远程桌面控制的安全风险分为隐私信息泄露和系统脆弱性分析。

4.1.1 隐私信息泄露

文献[31]的研究结果远程桌面流量加密机制不足以防止侧信道信息泄露。攻击者利用机器学习技术, 使用逻辑回归、支持向量机、梯度提升决策树、随机森林以及流爆发的统计特征等方式可以获取 Teamviewer、RealVNC 等远程桌面应用中用户的日常活动。文献[32-33]研究表明 Teamviewer 的加密网络流量中, 依旧存在可以区分文件传输、语音会议、视频会议、文本聊天和普通远程会话的方法。文献[34]表明在 Microsoft 远程桌面协议中, 即使流量经过加密处理, 还是可以检测到进行的活动。远程控制平台的用户和提供者都应对这些隐私泄露问题给予更多的关注。

4.1.2 系统脆弱性分析

文献[35]指出远程桌面控制协议的使用难以确保外部工具的安全性, 也难以对加密后的流量内容进行监督审计, 容易造成资源滥用和失信等问题, 远程桌面控制也被攻击者用作攻击的手段, 需要完善桌面控制平台的监督审计机制。

文献[36]表明, 使用暴力破解 RDP 协议登录受害者主机来传播病毒是攻击者的一种重要攻击手段。文献[37]提出 RDP 协议存在中间攻击的缺陷在于单向认证模式, 客户端不会对服务端的身份进行验证, 使用 ARP(Address Resolution Protocol)欺骗可以作为代理控制通信。文献[38]证明 RDP 和 SMB (Server Message Block)协议的蜜罐技术是可以被探测的, 攻击者也可以使用类似方法避开低交互和高交互的蜜罐。

4.2 攻击检测与防御

远程控制平台作为实现远程办公的一个重要手段, 为用户在任何地点和任何设备上工作提供了方便, 但是由于上述漏洞的存在, 对于一个组织来说, 这可能不是一个安全的选择。文献[39]提出了一个基于网络的入侵检测系统(Network Intrusion Detection System, NIDS), 利用基于机器学习的异常检测技术, 来检测针对 RDP 服务端的恶意 TCP 报文, 专门用于保护远程桌面连接的安全。文献[40]提出了一种基于强化学习的隐藏攻击序列检测方法, 通过将网络管理员建模为一个智能代理, 从与网络空间环境的交互中学习其行动方式来应对可能存在的攻击。按照深度确定性策略梯度(Deep Deterministic Policy Gradient, DDPG), 智能代理不仅可以发现隐藏在合法行动序列中的隐藏攻击者, 还可以减少网络空间管理成本。文献[41]使用蜜罐技术, 结合多层神经网络, 识别潜在危险流量, 将网址(Uniform Resource Locator, URL)重定向到设置的陷阱服务器, 通过获取攻击者行为, 调查分析攻击者的意图。文献[42]提出双因子认证(Two-factor Authentication, 2FA)的正确实施将作为加强用户认证作用的第一线机制, 从而提高远程访问的安全性。

4.3 小结

远程桌面控制存在的安全问题多样化, 例如: 远程桌面控制协议缺乏保密性导致用户隐私泄露, 登录认证机制简单导致暴力破解的风险。此外。远程桌面控制应用程序的漏洞也为远程桌面控制带来了新的安全风险。加强认证机制、检测异常行为等方法, 是远程桌面控制安全问题的主流解决方案、未来提供更可靠的远程桌面通信协议也为解决远程桌面安全问题提供了新的可能。

5 团队协作平台

团队协作与具有共享物理空间的真实世界团队协作相同, 团队协作平台为团队协作提供了虚拟环境, 国内外常见团队协作平台及其下载量和 API 数量如表 1 所示(下载量来源于 Google Play、应用宝, API 数量来源于各平台官网[43])。

表 1 流行团队协作平台及其 API 数量

Table 1 Popular teamwork platforms and the amount of API in the platforms

平台	下载量	API 数量
Slack	10M+	224
Microsoft Teams	100M+	170
Zoom	100M+	400
Facebook Workplace	10M+	74
Webex Teams	1M+	134
Flock	100000+	22
Twist	50000+	119
企业微信	20M+	242
钉钉	81M+	353
微信	149M+	935

团队协作平台具有三个突出特点:

1) 团队协作平台关注工作区中用户的聊天系统(群聊、私聊)。在团队协作平台中, 每个人都能看到公共频道的对话, 例如在钉钉中同一家公司员工通常是“工作区”的所有成员, 在工作区中, 可以进一步划分频道, 即工作组(私有频道), 用来讨论不同的项目, 只有受邀成员才能参与。

2) 团队协作平台支持在线会议, 工作区中的每位用户可以在公共频道和其所在的私有频道内主持在线会议, 在线会议有两种形式: 视频会议、电话会议。不仅平台自身提供了在线会议的功能, 平台中集成的第三方应用程序也为用户提供了该功能。例如: Slack 提供的视频通话功能和 Slack 中集成的 Zoom 都可以满足用户在线会议的需求。

3) 团队协作平台支持共享协作, 例如, 文件/屏幕共享等, 这些功能通常使用第三方应用程序(即用户基于平台开发的程序、机器人, 扩展程序)集成其他协作工具来支持。例如, 钉钉的工作台中集成了很多小程序, 例如文件共享, 表单审批等。

5.1 团队协作平台架构

团队协作平台主要的应用有综合协作、在线会议、文档协作、任务管理和云存储五大类[53], 其访问控制系统是基于角色的访问控制以保护数据和用户信息。通常, 团队协作平台存在三种交流通道: 公有通道、私有通道、直接消息通道。对于公共通道, 团队的所有成员都可以自行加入和离开频道, 所有的数据和资源都是公开的。对于私有通道, 只有被邀请的人员才能参与。团队成员也可以选择一对一直接消息来聊天, 这种直接消息通道对其他人是不可见的。

图 2 展示了团队协作平台的服务架构, 包括客户端、服务器架构以及平台上集成的第三方 APP(又称为插件、小程序)三部分。远程办公平台主要由客户端和平台服务器两部分构成, 其中, 客户端应用是用户本地安装的应用软件, 提供用户交互功能, 包括桌面应用、移动 APP 和 Web 应用, 它们都利用 Web 技术进行开发, 使用本地的浏览器代码解析引擎解析网页。服务端为客户端进行服务, 提供绝大部分的数据存储和后台处理逻辑。此外每个平台都基于超文本传输协议(Hyper Text Transfer Protocol, HTTP)和超文本安全协议(Hypertext Transfer Protocol Secure, HTTPS)开发了一系列符合 REST-API 规范[54]的自适应 API, 帮助用户和开发人员实现对平台的高效访问。用户和开发人员还可以利用 API 实现对小程序生命周期的控制。远程办公平台还支持用户开发自定义小程序以丰富平台功能, 满足特定的用户需求。小程序与平台服务端通过预先设计好的 REST-API 进行连接, 同时平台也设计了一套权限系统限制小程序在客户端和服务端的敏感操作。

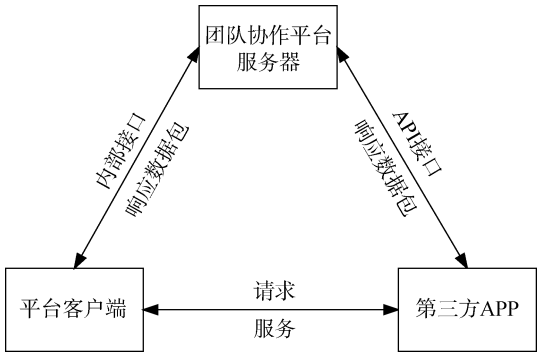

图 2 团队协作平台架构

Figure 2 Architecture of teamwork platform

5.2 团队协作平台的安全风险

基于团队协作平台架构和功能以及攻击者常用的攻击方式, 本文将团队协作平台的安全风险分为 5 部分: 第三方小程序安全、通信协议安全、客户端安全、云服务端安全、侧信道分析。本节将详细介绍这 5 类安全风险。

5.2.1 第三方小程序安全

团队协作平台为用户提供的小程序允许用户基于自主需求定制化平台, 这为团队协作平台引入了新的安全风险。研究表明, 恶意的攻击者已经将攻击的注意力从 Android 和 IOS 应用商店转移到各类平台和程序中集成的小程序中[55]。截至目前为止, 针对各类平台中集成的小程序还没有一套公认的管理规范。这也间接导致平台中集成的小程序会引入隐私泄露的风险。

文献[56]指出, 在现实使用中, 用户在授予小程

序敏感数据和高权限前, 得不到足够的详细信息(用户无法确定是谁在控制这些小程序, 不知道这些数据如何存储和存储在哪里, 也不知道他们使用这些信息的目的), 导致小程序获得过高权限。文献[57]指出应用程序经常会有意或者无意地将系统资源提供给小程序, 而对于小程序是否能够正确使用系统资源这一点难以确定, 可能导致位置、麦克风、照片等隐私信息的泄露。

团队协作平台中集成的小程序会主动申请额外的权限, 该权限与其提供的服务并无任何关系。文献[58]中发现, 一些小程序会申请获取用户通信录信息, 并将通信录的相关信息上传至这些小程序的服务器中, 导致用户社会关系隐私泄露。攻击者也可利用该漏洞向用户发起爬虫攻击, 非法获取用户隐私数据。

文献[59]对 App-in-app 模式下的应用资源管理进行了系统性的研究, 发现如权限提升、敏感数据泄露、子窗口欺骗、小程序生命周期劫持等一系列安全问题, 揭示了小程序生态下特有的安全缺陷, 这些缺陷允许敌手秘密升级权限(例如, 访问摄像头、照片库、麦克风等)或获取敏感数据。在微信中攻击者可以利用恶意小程序(通过模拟微信支付界面的UI)调用与支付功能相关的 API 盗取用户的支付密码。文献[60]也展示了用户界面管理不当将导致恶意应用程序通过模仿正常小程序的界面, 从而实现网络钓鱼攻击。

目前, 这种 App-in-app 模式[59]已被广泛应用于团队协作平台中, 帮助用户实现更为便捷的远程办公, 但这种 App-in-app 模式也为团队协作平台引入了新的安全问题。文献[5]首次针对用户在团队协作平台(Slack、Twist、Webex Teams 等)中开发的“自适应的 APP”和平台中集成的第三方 APP(例如: Slack 中集成的 Zoom、文件共享小程序等)进行了系统性的研究, 并证明了团队协作平台中集成的第三方应用程序确实会引入新的安全威胁, 例如: 权限提升、Slash Command 命令劫持、DDOS 攻击等。

文献[61]提出利用团队协作平台中集成的“文件共享”小程序可分发恶意软件, 该风险不仅让攻击者可以访问特定通道并诱骗其中的人下载恶意软件, 而且一旦上传了包含恶意代码的文件, 攻击者还可以获取该文件的可自由访问链接, 将该文件托管在聊天系统的服务器上, 攻击者就可以通过网络钓鱼电子邮件、误导性文本或他们拥有的任何其他接触潜在受害者的方法将该链接发送给受害者。

明确小程序的安全风险并提出合理的防御方案是目前远程办公领域重点的研究方向之一, 文献[62]提出了基于权限的访问控制隐私模型, 需要对程序内的不同组件进行更加灵活和细粒度的隐私访问控制。允许内部组件访问隐私数据, 禁止外部组件访问隐私数据, 从而增强隐私可控性并且维持必要功能。

文献[5]提出了两条缓解小程序安全风险的常识安全策略: 1)小程序在安装和更新过程中必须经过彻底的安全审查, 并应明确通知受影响的用户; 2)对小程序的访问控制应遵循最小权限原则, 避免授予任何可能给团队协作平台中的其他用户带来安全风险的不必要的权限。

文献[59]表明小程序和团队协作平台之间应实现更高程度的UI窗口隔离, 小程序的UI窗口应始终与团队协作平台的窗口分离。针对小程序生命周期的劫持, 短期防御措施是将所有小程序应用资源放置于团队协作平台所在系统的内部存储中, 以防止攻击者通过监控外部存储, 获取小程序的生命周期。但从长远来看, 研究人员需要考虑如何使子程序任务动态可扩展, 以确保小程序回收不再可追溯才是根本的解决办法。

目前, 小程序已经成为团队协作平台不可或缺的一部分, 在方便用户操作的同时, 完善小程序的访问控制模型、明确小程序的安全风险, 保证用户隐私安全(隐私数据收集采用最小必要原则问题)和平台自身安全是下一步研究的重点工作。

5.2.2 通信协议安全

通信协议是团队协作平台重要的组成部分, 只有确保通信协议安全, 才能保证平台用户的隐私安全和数据安全, 但目前表明, 团队协作平台存在严重的安全风险, 例如: 文献[58]的研究表明, 三种流行的团队协作软件(WhatsApp、Signal 和 Telegram)中的联系人功能存在严重的隐私问题, 其实验表明大规模的爬虫攻击会造成用户隐私泄露。文献[63]表明即使团队协作平台部署了先进的加密机制, 但仍存在流量分析攻击, 敌手能够以高精度识别目前团队协作频道中的管理员和成员。

如今安全通信逐渐成为大众需求, 其中端到端加密通信协议如 Signal 协议为 10 亿活跃用户提供通信上的安全。Signal 提供了一些强大的安全属性, 例如后泄露安全[64], 实现和密钥已经被泄露的一方进行安全的交流。文献[65]对 Signal 协议的安全性进行调查后显示其满足安全属性的同时实现了后泄露安全。文献[66]指出 Signal 协议在群消息的泄露安全方面考虑不足, 一旦攻击者获得一个成员密钥, 攻击者可以始终使用该成员密钥进行攻击。为防御这种

攻击方式, 该研究基于树的 Diffie-Hellman 密钥交换协议设计的 ART(Asynchronous Ratcheting Trees)方案结合了群消息传递的带宽优势和端到端协议的强大安全保证, 为群消息的传递提供了安全保证。文献[67]进一步对跨组后泄露安全进行研究, 提供了一个基于 EUF-CMA 签名的可证明安全的 RSIG (Ratcheting Digital Signature)结构, 使用更新长期密钥的方式来实现全局 PCS(Post-Compromise Security)。

文献[68]提出 Signal 端到端加密协议存在统计披露攻击, 主要由于发送方协议的接收者和时间是暴露的, 而 Signal 收到消息后立即向发送方发送自动收据导致双方隐私泄露, 该文章提议使用盲签名实现匿名凭证, 保护用户信息。

文献[69]分析 Zoom 的端到端的加密协议(E2EE, 2.3.1 版), 对其进行了系统性的安全评估, 并证明 Zoom 中存在以下三种安全风险: 一是参加会议的恶意人员在内部人员不知情的情况下可以发起冒名攻击; 二是内部的恶意人员与参加会议的恶意人员勾结, 他们可以在目标会议中冒充任何 Zoom 用户; 三是利用多用户共享的设备可以冒充该设备上的其他用户。

文献[70]对 Zoom、Google Meet 和 Microsoft Teams 进行了研究, 虽然这些平台使用了最先进的加密方法, 但它们没有提供端到端加密, 第三方供应商可以访问最终用户的通信数据。Houseparty、Discord 和 Doxy.me 等软件并没有提供端到端的加密, 用户和远程服务器或小程序之间直接采用明文传输的方式, 导致用户的隐私泄露[71]。文献[72]提出端到端加密通信协议在提供良好的隐私性的同时, 通过其发送的错误或恶意信息难以被溯源, 容易造成严重后果。文献[73]发现, 当服务器提供商是恶意或者被强迫时, 服务提供商可以向发送者提供自己的公钥, 使发送者无法正确检索收件人公钥, 进行中间人攻击。

为保证数据在传输过程的安全性、完整性, 文献[74]提出了一种同态加密的方案来保护病人的隐私与医疗数据的安全, 文献[75]提出了团队协作平台可以通过使用传输层安全性协议(Transport Layer Security, TLS), 作为底层协议来保护信息的传输, 从而确保信息的机密性。

通信协议安全是团队协作平台的基石, 只有通信协议安全才能保证用户数据安全, 如何保证数据在传输过程中的安全性、完整性是下一步研究的重点工作。

5.2.3 客户端安全

团队协作平台客户端存在的安全问题大致可以分为两个攻击面: 一是客户端软件本身存在的安全问题, 二是利用人工智能技术对特征数据进行建模的方式从外部攻击客户端。

ZOOM 中存在 0DAY 漏洞, 该漏洞可以让任意网站在未经用户允许的情况下闯入 ZOOM 会议并开启摄像头[76-77]。文献[78]指出 ZOOM 与 Google Meet 等团队协作平台普遍存在群体轰炸的现象, 由于其进入会议不需要进行授权, 因此非内部人员可以随意进入会议并发布不良信息和危险信息阻碍会议的正常进行, 不仅如此攻击者还可以非法获取会议的内容。

Zoom 轰炸攻击主要针对实时会议, 因此主动识别此类攻击并进行防御是难以实现的, 文献[78]认为可以允许在线会议主持人为每一个参与者创建独特的会议链接来防止 Zoom 轰炸, 虽然这会影响 Zoom 的可用性, 但可以从根本上防止 Zoom 轰炸的攻击。除此之外, 在线会议设置会议密码也是防止 Zoom 轰炸的主要防御策略。

团队协作平台存在用户隐私泄露的风险, 研究[79]表明 Zoom 允许管理员查看每个参与者的操作系统、IP 地址、位置数据和设备信息。这些设备信息包括机器的类型(PC/Mac/Linux/mobile/etc), 外围视听设备(如相机或扬声器)的制造/型号规格, 以及这些设备的名称(例如, AirPods 的用户可配置名称)。攻击者可以利用这些信息推测出用户的相关信息, 从而间接导致用户隐私的泄露。研究[80]表明 ZOOM 提供的快速会议并不是端到端加密的, 这直接导致了用户隐私的泄露, 更严重是 Zoom 聊天会将 UNC 路径转化为 Windows 客户端上的可点击链接, 攻击者可以利用这一缺陷来安装有后门、有漏洞的旧版本 ZOOM 客户端。

文献[81]发现 Google chat, Slack, Mattermost, Webex Teams, Microsoft Teams 中均存在冒名顶替攻击, 攻击者可以成功伪造合法用户显示的姓名、头像、以及其他的个人信息来混淆合法用户的识别, 并且可以邀请外部成员来冒充合法的内部成员。研究[82]表明 Slack 中存在 HTML/JavaScript 代码注入的漏洞, 会造成远程执行恶意代码的风险, 此外研究[79]表明 Slack 的免费用户无法看到在 10000 消息标记之前发送的消息, 但 Slack、执法部门和任何第三方黑客仍然可以获取这些消息, 造成用户隐私泄露。

AI 技术已经成为攻击者常用的攻击手段, 攻击者通过收集的海量数据进行建模, 从而分析出同类数据的独有特性, 基于数据分布的特征, 攻击者可以分析出用户的隐私数据。文献[83]提出不需要使用

受害者的麦克风, 仅仅使用有限的击键数据就可以获取受害的击键内容, 比如密码、用户名、电子邮件地址等。与这一种方式相似, 文献[84]通过远程视频软件中截取到的呼叫击键的视频流(包括击键声音与肢体活动)可以更加准确预测出受害者发送的内容。文献[85]的研究结果表明团队协作平台视频会议摄像头拍摄的信息在一定程度上泄露用户在房间内陈设的具体物品等隐私信息。文献[33]论述了通过在网络上抓包可以获取用户的通信类型比如文本, 语音, 视频等。文献[86]中描述了通过深度学习的技术可以获取 Zoom 远程办公软件的加密图像的特征以及加密的密钥。文献[87]描述了恶意攻击者通过公共渠道上获取到的受害者的视频或者图像, 使用人工智能技术来伪造一些视频或者音频来进行电信诈骗。

如何防御人工智能攻击也是团队协作平台面临的主要安全问题, 文献[63]表明添加覆盖流量等标准对抗技术会降低本文中介绍的流量攻击的有效性。针对篡改用户的语音、视频的安全问题, 文献[87]提出名为 LiveScreen 的检测方案, 通过在帧粒度上检测语音与视频的活性来鉴别原始音频和图像是否被篡改。对于泄露用户背景隐私数据的攻击案例, 文献[85]提出了可以更改用户的背景图像来达到保护的目的。

客户端的安全问题不仅体现在 PC 端, 移动 APP 应用端的安全问题也应被给予更多的关注。如何有效地防御利用人工智能技术发动的攻击是目前客户端安全面临的最为严重的问题。

5.2.4 云服务端安全

云端数据非常容易受到恶意服务商和恶意用户的攻击, 如何保证云端数据的安全一直以来都是客户/服务器模型(C/S 模型)面临的棘手问题, 云端数据始终面临丢失或泄露的风险, 如 2014 年, google driver 中的数据通过 URL 外泄[88]。

文献[89]提出了云存储上文件共享的组密钥管理协议(Group Key Management Protocol, GKMP), 基于混合加密技术的组密钥生成方案防止来自公共渠道的网络攻击, 并采用验证方案防止共享文件受到云提供商和群组成员合谋攻击的攻击。文献[90]提供了一种保护数据的新方案(Titanium), 它是一个可以提供隐藏元数据的端到端文件共享系统, 在保护用户身份信息安全的同时, 实现系统的机密性和完整性。

文献[91]认为云服务器提供商对数据存储和处理过程不透明, 导致用户甚至无法知晓自己的信息遭到泄露, 用户对自身数据的权限可能丢失。文献[92]提到当用户的身份凭证遭到钓鱼攻击窃取时, 由于凭证的可重用性, 攻击者将可以监听用户的隐私信息。

文献[93]表明, 云存储环境下用户失去了对自身数据的物理掌控, 用户无法确定自己数据存储的位置以及是否彻底删除; 同时复杂的技术如数据库、操作系统、网络环境、虚拟化等为云存储带来了许多的安全风险, 云数据共享可能将数据泄露给未经授权的人员, 并且由云服务通常同时提供给多个用户, 这种多用户的特点导致不同用户资源可能存在同一物理设备上, 攻击者更容易获得对用户数据的访问权限。

为丰富远程办公的功能, 团队协作平台不仅引入了第三方小程序库, 还提供了遵循 REST API 规范[54]的 API 来提升平台的可用性。团队协作平台利用类似 Single-Sign-On 系统[94]的基于权限的访问控制来管理小程序, 它利用唯一的访问令牌和权限列表来控制小程序可以接触到的信息, 许可权限列表指定小程序可以调用的 API。用户和开发者可以通过小程序来调用平台提供的 API 来访问平台中的资源或调用平台提供的功能。除此之外, 部分团队协作平台还允许用户基于平台提供的 API 开发自适应的 APP, 但这也为团队协作平台引入了综合性的安全问题。

文献[5]首次针对团队协作平台提供的 API 进行了系统性的研究, 并为 API 提供了完整的测试方案, 证明了团队协作平台中的用户开发的“自适应”小程序通过调用平台提供的 API 会引入新的安全威胁。例如: 越权访问、URL 欺骗、DDOS 攻击、钓鱼攻击等。

为缓解云端 API 存在的安全问题, 文献[5]针对团队协作平台的设计方案和权限分配提出了两点意见, 1)团队协作平台应阐明其对敏感用户数据的访问控制设计原则(例如, 工作区管理员是否可以访问私人消息)。因此, 团队协作平台应对用户权限进行细粒度的划分来保证用户隐私安全。2)以 URL 欺骗为例, 如果呈现的 URL 文本与其重定向的实际文本不同, TACT 系统应提供足够的警告。团队协作平台应加强对各类网络攻击的检测来保证平台的整体安全性。

文献[59]表明研究人员应该采用自然语言处理技术(Natural Language Processing, NLP)更全面地分析 API 相关文档以获取有关 API 权限策略更完整的信息, 其分析可以涵盖更广泛的文献, 包括 iOS 文档、研究论文、技术报告等, 这将有助于获得有关资源管理政策的最新知识, 从而降低 API 存在的安全

风险。

云端数据安全是团队协作平台的核心, 多年来, 云端数据安全一直是热点研究方向。而如今, 云端 API 的安全问题也显得愈发突出, 深入分析 REST-API 访问控制机制、细粒度的权限模型、数据加密和隐私泄露管控等防护方案是目前急需解决的问题。

5.2.5 侧信道分析

侧信道攻击是指在远程办公中不仅利用团队协作平台, 还利用一些其他的物理设备如摄像头, 麦克风或者是其他类型传感器来辅助进行攻击等。文献[83]基于远程办公软件中键盘声学的侧信道攻击提出了 offense-defense 系统, 在受害者进行基于 IP 的语音传输(Voice over Internet Protocol, VoIP)通话时窃取随机密码, PIN 等敏感用户数据的输入。文献[95]中描述了未经授权的远程访问监控摄像头可以任意改变易受攻击摄像头的配置, 使其无法执行预期的监控功能或覆盖范围, 不仅如此, 攻击者还可以自由控制摄像头拍摄角度和范围, 通过这样的方式非法获取用户的隐私数据。文献[96]描述了通过非法远程更改起搏器的配置可能会导致病人的死亡。文献[84]中论述了通过远程视频软件中截取到的外部摄像头与麦克风所收集的呼叫击键音频与肢体动作的视频流可以准确预测出受害者发送的内容。

目前侧信道攻击常与机器学习结合在一起, 通过大数据对用户行为进行建模, 从而分析出用户隐私信息, 如何防止设备泄露物理信息应为未来研究的方向之一。

5.3 小结

团队协作平台面临的安全风险是多方面, 明确团队协作平台权限的划分策略、完善团队协作平台的访问控制模型是目前急需解决的安全问题。未来研究人员应关注现有团队协作平台的信息存储和访问方式、团队协作平台隐私数据的合理收集使用问题和 API 访问控制模型才能从根本上解决平台自身存在的安全问题。

利用人工智能技术的攻击不仅是团队协作平台面临的安全问题, 也是计算机相关领域面临的公共问题。因此, 如何有效抵抗利用人工智能技术的攻击是计算机相关领域面临的棘手问题。

6 远程办公系统安全挑战和机遇

基于对远程办公系统的系统性分析, 本节指出了关于远程办公系统安全研究所面临的机遇和挑战, 图 3 展示了挑战和机遇的对应关系。

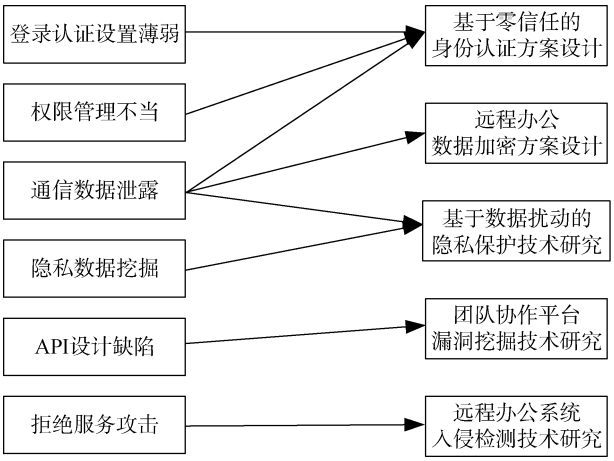

图 3 挑战和机遇

Figure 3 Challenges and opportunities

6.1 目前面临的主要挑战

6.1.1 登录认证设置薄弱

身份认证是进行远程办公的关键防线, 一旦被攻破则其他安全手段也都将丧失作用, 所有资源都将完全暴露在攻击者面前, 给公司带来难以估量的损失。然而, 大多数远程办公系统的登录认证机制仍然比较传统和单一, 远程攻击者可借助各种漏洞绕过身份验证, 或者通过中间人攻击等手段冒充合法用户通过登录检验。此外, 员工的终端设备往往处于较低的安全状态, 在执行远程办公任务时非常容易被攻击者利用。因此, 接入环境的网络安全性在登录认证的过程中应该受到更多重视。

6.1.2 权限管理不当

权限管理一直是互联网相关领域面临的棘手问题。在远程办公中, 一方面, 用户可能通过非法手段将自己的权限提升至根级或系统级, 从而在系统上执行任意命令以达到自己的恶意目的, 另一方面, 由于权限划分模糊, 合法用户通过 VPN 接入内网后也可能给系统安全造成严重威胁, 例如: 如果普通用户拥有更改系统配置的权限, 并在无意间删除和修改系统敏感文件, 则在严重情况下会使系统无法正常运行。不仅如此团队协作平台也缺乏细粒度的权限划分, 例如在团队协作平台中, 用户可以为其基于平台开发的 APP 赋予任何权限, 从而获取非自身权限的额外信息, 恶意用户可以利用平台权限管理的缺陷获取其他用户的信息、阻止其他用户的正常使用。

6.1.3 通信数据泄露

如何保证传输过程中的数据安全性、完整性不仅是利用 VPN 实现远程办公面临的危害最为严重的问题, 也是团队协作平台中需要解决的一个关键问

题。文献[97]指出, 在 VPN 的使用过程中攻击者截获和伪造报文从而获取通信双方的信息, 除此之外, 文献[28]指出, 攻击可以利用响应数据包的大小和响应时间推测出数据包中的关键信息, 并进行数据注入。文献[5]指出, 团队协作平台中用户所发送的消息可以被非法用户获取, 不仅如此, 非法用户还可以篡改用户已发送的信息。

6.1.4 隐私数据挖掘

随着机器学习和深度学习的不断发展, 人工智能技术在成为攻击者的一种主流手段, 侵犯了团队协作平台用户的隐私。文献[84]指出音视频通话会有泄露用户数据隐私的风险, 攻击者基于远程视频会议中截取的视频流分析甚至可以预测出用户在视频通话期间输入的文本。Zoom, Slack 等远程办公软件均已进行了背景模糊化的处理来保护用户隐私, 但是用户击键仍然可能会造成用户的隐私泄露, 如用户通过键盘输入的登录用户名, 密码, 银行卡号等多种敏感信息。文献[85]中描述了通过在远程办公中对摄像头拍摄的信息使用人工智能技术进行过滤与提取会在一定程度上泄露用户的隐私数据, 如用户在房间内陈设的具体物品。

6.1.5 API 设计缺陷

团队协作平台云服务端提供了大量的 API 服务, 但其 API 存在的接口设计缺陷对远程办公平台用户数据的安全和隐私造成极大威胁。文献[5]指出, 团队协作平台的用户利用 API 获取频道中的历史消息、篡改其他用户在频道发布的消息、更改已发布链接的 URL(使用钓鱼网站的 URL 替换正常的 URL), 除此之外, 利用 API 可以不停地中断其他成员通话, 从而导致拒绝服务攻击。除了上述 API 的设计缺陷, 基于团队协作平台 API 开发的自适应 APP 也为远程办公系统引入了新的安全问题。

6.1.6 拒绝服务攻击

近年来, DoS 攻击的攻击规模及频率呈快速增长的态势, 给远程办公也带来了不小的影响。DoS 攻击所导致的系统不稳定性将会严重影响工作效率和员工的工作热情, 特别是当安全防护系统因受到影响停止运行时会给攻击者造成可乘之机。而如何在最大程度上保证系统正常运行的同时能够阻挡恶意流量和数据则需要更多的实践和研究。

6.2 未来研究机遇

6.2.1 基于零信任的身份认证方案设计

零信任的基本理念是“持续验证, 永不信任”, 它是一个全面的安全模型, 它涵盖了网络安全、应用安全、数据安全等各个方面, 致力于构建一个以身份为中心的策略模型以实现动态的访问控制。

零信任身份认证基于多身份凭证管理(生物特征、行为特征、口令等)可以确保用户的身份信息唯一, 有效地抵抗远程办公中的假冒攻击。零信任身份认证为用户提供身份的全生命周期管理, 确保用户在职期间的身份合法性, 一旦离职撤销其合法身份, 有效的保证企业数据安全; 不仅如此, 身份的全生命周期管理还为用户提供了细粒度权限分配, 确保用户的权限可以实现细粒度地控制, 从而避免越权访问和权限提升的安全问题。此外, 在零信任的身份认证模型下, 企业可以实现对用户动态访问的控制, 用户行为时刻处在监控之下, 因此用户在进行高危敏感操作时会立即触发动态授权和二次认证, 并发布风险预警, 以便管理员及时发现异常情况。

6.2.2 远程办公数据加密方案设计

密码学一直是安全领域的中流砥柱, 在保障数据安全方面具有重要作用。例如: 文献[98]提出的用于 VPN 数据包中的有效负载加密的多阶段加密算法, 加强了数据在公共通信网络中的机密性, 文献[99]基于椭圆曲线密码算法设计加密通信协议以保证团队协作平台客户端至客户端和客户端至服务器的安全通信。

2020 年的研究表明 Zoom 的加密和解密在 ECB 模式下使用 AES[100], 这为 Zoom 引入了严重的安全风险。因此, 提升加密算法的健壮性对远程办公系统的数据安全具有极大的帮助, 加密算法的健壮性帮助平台建立了难以逾越的屏障, 使攻击者无法轻易窃取用户的隐私数据, 同时也不会明显影响到系统的运行效率。

6.2.3 基于数据扰动的隐私保护技术研究

数据扰动又分为 3 种方式: 分别是输入扰动、输出扰动和客观扰动, 通过增加干扰数据来保证真实数据的安全。因此数据扰动是未来应对利用人工智能技术实现攻击的主要防御方法之一。不仅如此, 在传输过程中为真实数据添加扰动也可以有效地防止信息泄露, 即使攻击者获取传输的数据也无法获取有效信息。

目前, 通过数据扰动来保护用户隐私数据安全的方式已被应用于远程医疗领域, 例如: 文献[101]提出一种基于组合聚类和几何数据扰动的隐私保护方法以改善混合云中医疗保健数据, 文献[102]提出一种随机数据扰动模型用以保护真实世界医学数据集。未来, 通过数据扰动实现隐私保护的方式将被广泛应用于隐私保护领域, 以有效提升远程办公系统隐私安全。

6.2.4 团队协作平台漏洞挖掘技术研究

模糊测试(Fuzzing)是一种安全测试技术, 常被用于软件测试, 通过自动化策略实现对种子(输入样例)的变异来覆盖程序执行的所有可能性, 并基于程序的执行结果分析其可能存在的漏洞。

Fuzzing 已被应用于 API 安全问题的测试中, 例如: 文献[103]介绍了一种用于 REST API 的自动、有状态的模糊测试工具, 该工具分析 REST API 的 Swagger 规范以自动推断请求类型之间的依赖关系, 并根据服务响应的反馈动态生成测试。文献[5]设计了一种 Fuzzing 团队协作平台 API 的工具 TAPIS, TAPIS 首先采用 NLP 对 API 文档进行分析, 提取 API 依赖关系并对其进行分类。在 Fuzzing 阶段, TAPIS 根据 API 的文档要求生成符合 API 测试基本需要的种子, 在保证必要参数(例如: 频道 ID、token 等)不变的情况下, 对其他非必要参数进行随机变异, 保证输入样例的有效性。

由于 API 对输入样例的格式有严格的要求; API 存在限制访问次数, 因此通用 Fuzzing 方案无法满足 API 测试的需求。未来, 研究人员可以为 API 定制化 Fuzzing 工具以提升 API 测试的准确性和代码覆盖率, 实现对 API 的全面检测。

6.2.5 远程办公系统入侵检测技术研究

入侵检测系统基于用户访问行为进行建模, 再从链路流量的实时监测中提取统计特征, 与内置知识库进行对比以迅速发现异常, 被普遍应用于公司的安全防护。例如: 文献[23]利用 Suricata 作为 IDS/IPS 来检测和保护 VPN 服务器。进一步降低入侵检测系统的漏报率和误报率是需要持续研究的重点。

目前, IDS 在一定程度上帮助远程办公系统减轻了网络威胁, 但是缺乏对于未知威胁的检测手段, 未来 IDS 可以借助神经网络和人工智能的帮助, 更智能地进行攻击检测和防御。

6.3 小结

作为一种新兴的办公方式, 远程办公的用户不断增长, 机遇与挑战并存。登录认证机制和权限管理环节的薄弱催生了零信任概念的诞生。加密算法则继续为数据安全保驾护航。数据扰动在保护数据安全的同时也为防范隐私数据挖掘攻击提供了保障。API 存在的缺陷可以在 Fuzzing 漏洞挖掘中被发现, 进行完善和改进。拒绝服务攻击作为一种传统的攻击手段仍在影响着远程办公系统的运行, 同时也促进入侵检测系统在新场景下的不断发展和应用。

7 总结

本文调研了现阶段远程办公的主流解决方案和研究成果并分析了其面临的主要安全威胁和相应的缓解策略, 经过大量调研后, 从虚拟专用网(VPN)、远程桌面控制、团队协作平台三方面对远程办公系统进行了分类总结, 指出了目前远程办公系统的痛点和面临的挑战, 为未来针对远程办公系统安全问题的研究指明了方向。

远程办公系统是疫情背景下保障机构能够正常运转的重要手段, 也是未来机构办公的发展趋势, 只有保证远程办公系统的安全才能保证机构的健康发展, 确保社会经济稳定。

参考文献

[1] CVE - Search results – VPN. NVD. https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=VPN. May. 2022.

[2] CNNIC Releases the 49th Statistical Report on the Development Status of the Internet in China[J]. *Journalism Tide*, 2022(2): 3. (CNNIC 发布第 49 次《中国互联网络发展状况统计报告》[J]. 新闻潮, 2022(2): 3.)

[3] Everybody seems to be using Zoom. But its security flaws could leave users a trisk. Drew Harwell. https://www.washingtonpost.com/technology/2020/04/02/everybody-seems-be-using-zoom-its-security-flaws-could-leave-people-risk/. Apr. 2020.

[4] Aiken A. Zooming in on Privacy Concerns: Video App Zoom is Surging in Popularity. in our Rush to Stay Connected, we Need to Make Security Checks and not Reveal more than we Think[J]. *Index on Censorship*, 2020, 49(2): 24-27.

[5] Zha M, Wang J, Yuhong Nan, et al. Hazard Integrated: Understanding the Security Risks of App Extensions on Team Chat Systems[C]. *Network and Distributed Systems Security Symposium*, 2022: 24-28.

[6] Spathis P, Dey R, Processing C A, et al. Online teaching amid COVID-19: The case of zoom[C]. *2021 IEEE Global Engineering Education Conference*, 2021: 1398-1406.

[7] Muheidat F, Tawalbeh L, Processing C A. ZOOM sandwich: an adaptable model for distance learning[C]. *2020 International Conference on Computational Science and Computational Intelligence*, 2021: 1004-1008.

[8] Alexei A, Alexei A. Cyber Security Threat Analysis in Higher Education Institutions as a Result of Distance Learning[J]. *International Journal of Scientific & Technology Research*, 2021, Volume 10(3): 128-133.

[9] Draaijer S, Jefferies A, Somers G. Online Proctoring for Remote Examination: A State of Play in Higher Education in the EU[M]. Technology Enhanced Assessment. Cham: Springer International Publishing, 2018: 96-108.

[10] Li Y, Lai S S, Dong C L. Risk Analysis and Solution of Financial Telecommuting Security[J]. *Financial Computer of China*, 2021(8): 68-71.

(李燕, 赖胜枢, 董传丽. 金融行业远程办公安全风险分析及解决方案[J]. *中国金融电脑*, 2021(8): 68-71.)

[11] Jason S. The Future of Security in a Remote-Work Environment[J]. *Network Security*, 2021, 2021(10): 15-17.

[12] Malecki F. Overcoming the Security Risks of Remote Working[J]. *Computer Fraud & Security*, 2020, 2020(7): 10-12.

[13] Okereafor K, Manny P. Understanding cybersecurity challenges of telecommuting and video conferencing applications in the COVID-19 pandemic[J]. *International Journals of Multi Dimensional Research*, 2020, 8(6): 13-23.

[14] Obada-Obieh B, Huang Y, Beznosov K. Challenges and Threats of Mass Telecommuting: A Qualitative Study of Workers[C]. *Seventeenth Symposium on Usable Privacy and Security*, 2021: 675-694.

[15] Jin Z P, Chen Y. Telemedicine in the Cloud Era: Prospects and Challenges[J]. *IEEE Pervasive Computing*, 2015, 14(1): 54-61.

[16] Pramanik P K D, Pareek G, Nayyar A. Security and Privacy in Remote Healthcare[M]. Telemedicine Technologies. Amsterdam: Elsevier, 2019: 201-225.

[17] Olanrewaju R F, Ali N, Khalifa O, et al. ICT in telemedicine: Conquering privacy and security issues in health care services[J]. *Electronic Journal of Computer Science and Information Technology*, 2013, 4(1): 19-24.

[18] Jin H. Analysis on the Effective Application of VPN Technology in Hospital Information Construction[J]. *Modern Electronic Technology*, 2017, 1(1): 28.

[19] Jalali M S, Landman A, Gordon W J. Telemedicine, Privacy, and Information Security in the Age of COVID-19[J]. *Journal of the American Medical Informatics Association*, 2021, 28(3): 671-672.

[20] Cybersecurity Insiders(2021). https://www.cybersecurity-insiders.com/portfolio/2021-vpn-risk-report-zscaler/. May. 2022.

[21] Horst M, Grothe M, Jager T, et al. Breaking PPTP VPNS via RADIUS Encryption[M]. Cryptology and Network Security. Cham: Springer International Publishing, 2016: 159-175.

[22] Luo J, Ji Q B, Communication N A B T. Password acquisition and traffic decryption based on L2TP/IPSec[C]. *2020 IEEE 20th International Conference on Communication Technology*, 2020: 1567-1571.

[23] Sawalmeh H, Malayshi M, Ahmad S, et al. VPN remote access OSPF-based VPN security vulnerabilities and counter measurements[C]. *2021 International Conference on Innovation and Intelligence for Informatics*, *Computing*, *and Technologies*, 2021: 236-241.

[24] Burkert C, McDougall J A, Federrath H, et al. Analysing leakage during VPN establishment in public Wi-Fi networks[C]. *ICC 2021 - IEEE International Conference on Communications*, 2021: 1-6.

[25] Zhang Q, Li J R, Zhang Y Y, et al. Oh-Pwn-VPN! Security Analysis of OpenVPN-Based Android Apps[M]. Cryptology and Network Security. Cham: Springer International Publishing, 2018: 373-389.

[26] Ramesh R, Evdokimov L, Xue D, et al. VPNalyzer: Systematic Investigation of the VPN Ecosystem[C]. *Network and Distributed System Security*, 2022: 24-28.

[27] Ikram M, Vallina-Rodriguez N, Seneviratne S, et al. An Analysis of the Privacy and Security Risks of Android VPN Permission-Enabled Apps[C]. *The 2016 Internet Measurement Conference*, 2016: 349-364.

[28] William J. Tolley, Beau Kujath, et al. Blind In/On-Path Attacks and Applications to VPNs[C]. *30th USENIX Security Symposium*, 2021: 3129-3146.

[29] Streun F, Wanner J, Perrig A. Evaluating Susceptibility of VPN Implementations to DoS Attacks Using Adversarial Testing[EB/OL]. 2021: arXiv: 2110.00407. https://arxiv.org/abs/2110.00407.

[30] Khan M T, DeBlasio J, Voelker G M, et al. An Empirical Analysis of the Commercial VPN Ecosystem[C]. *The Internet Measurement Conference 2018*, 2018: 443-456.

[31] Jiang M H, Gou G P, Shi J Z, et al. I know what You are doing with remote desktop[C]. *2019 IEEE 38th International Performance Computing and Communications Conference*, 2020: 1-7.

[32] Nurse J R C, Williams N, Collins E, et al. Remote Working Pre- and Post-COVID-19: An Analysis of New Threats and Risks to Security and Privacy[M]. HCI International 2021 - Posters. Cham: Springer International Publishing, 2021: 583-590.

[33] Altschaffel R, Clausing R, Kraetzer C, et al. Statistical pattern recognition based content analysis on encrypted network: Traffic for the TeamViewer application[C]. *2013 Seventh International Conference on IT Security Incident Management and IT Forensics*, 2013: 113-121.

[34] Lapczyk L, Skillicorn D B. Activity Detection from Encrypted Remote Desktop Protocol Traffic[EB/OL]. 2020: arXiv: 2008.02685. https://arxiv.org/abs/2008.02685.

[35] Huang S H, Lin C, Luo A A, et al. Proxy-based security audit system for remote desktop access[C]. *2009 Proceedings of 18th International Conference on Computer Communications and Networks*, 2009: 1-5.

[36] Sinitsyn F. Kaspersky security bulletin: Story of the year 2017[M]. *Technical Report. Kaspersky, Inc*., 2017.

[37] He J S, Xu C, Zhang Y X, et al. A Strategy for Middleman Attack Prevention in Remote Desktop Protocol[J]. *Journal of Shanghai Jiaotong University* (*Science*), 2015, 20(1): 82-85.

[38] Franzen F, Steger L, Zirngibl J, et al. Looking for honey once again: Detecting RDP and SMB honeypots on the Internet[C]. *2022 IEEE European Symposium on Security and Privacy Workshops*, 2022: 266-277.

[39] Bitton R, Shabtai A. A Machine Learning-Based Intrusion Detection System for Securing Remote Desktop Connections to Electronic Flight Bag Servers[J]. *IEEE Transactions on Dependable and Secure Computing*, 2021, 18(3): 1164-1181.

[40] Zhang L, Pan Z S, Pan Y, et al. A Hidden Attack Sequences Detection Method Based on Dynamic Reward Deep Deterministic Policy Gradient[J]. *Security and Communication Networks*, 2022, 2022: 1-13.

[41] Danchenko N M, Mazurenko G A, Bioengineering, et al. Detecting and analysis malicious activity on remote desktop protocols using integrated security system[C]. *2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering*, 2018: 40-41.

[42] Yeboah-Boateng E O, Kwabena-Adade G D. Remote Access

Communications Security: Analysis of User Authentication Roles in Organizations[J]. *Journal of Information Security*, 2020, 11(3): 161-175.

[43] Web API methods. Slack. https://api.slack.com/methods.

[44] Use the Microsoft Graph API to work with Microsoft Teams. Microsoft. https://docs.microsoft.com/en-us/graph/api/resources/teams-api-overview?view=graph-rest-1.0. Jan. 2022.

[45] Zoom REST API. https://zoom.github.io/api-v1/. Nov. 2018.

[46] Account Management API (Graph). Facebook. https://developers.secure.facebook.com/docs/workplace/reference/account-management-api/graph-api?locale=zh_CN.

[47] WebexTeamsAPI. WebexTeams. https://webexteamssdk.readthedocs.io/en/latest/user/api.html.

[48] API Reference – FlockOS. Flock. https://docs.flock.com/display/flockos/API+Reference.

[49] Introduction – API Documentation | Twist Developer. Twist. https://developer.twist.com/v3/.

[50] Overview - Interface Documentation: Enterprise WeChat Developer Center. Enterprise WeChat. https://developer.work.weixin.qq.com/document/path/90556.
(概述- 接口文档- 企业微信开发者中心. 企业微信. https:// developer.work.weixin.qq.com/document/path/90556.)

[51] Overview of old server-side APIs: Ding Talk Open Platform. DingTalk. https://open.dingtalk.com/document/orgapp-server/server-api-overview. Jan. 2022.
(旧版服务端 API 总览: 钉钉开放平台. 钉钉. https://open.dingtalk.com/document/orgapp-server/server-api-overview. Jan. 2022.)

[52] API:WeChat Open Document. WeChat. https://developers.weixin.qq.com/miniprogram/dev/framework/app-service/api.html.
(API: 微信开放文档. 微信. https://developers.weixin.qq.com/miniprogram/dev/framework/app-service/api.html.)

[53] EO Intelligence 2020 Teleworking Research Report. EqualOcean. https://www.iyiou.com/research/20200320699. Mar. 2021.
(《亿欧智库 2020 远程办公研究报告》. 亿欧. https://www.iyiou.com/research/20200320699. Mar. 2021.)

[54] Overview of restful api description languages. Wikipedia. https://en.wikipedia.org/wiki/Overview of RESTful API Description Languages. Feb. 2021.

[55] Attackers blowing up discord, slack with malware. Threat Post. https://threatpost.com/attackers-discord-slack-malware/165295/. Apr. 2021.

[56] Shezan F H, Cheng K M, Zhang Z, et al. TKPERM: cross-platform permission knowledge transfer to detect overprivileged third-party applications[C]. *Proceedings 2020 Network and Distributed System Security Symposium*, 2020.

[57] Felt A P, Chin E, Hanna S, et al. Android Permissions Demystified[C]. *The 18th ACM conference on Computer and communications security*, 2011: 627-638.

[58] Hagen C, Weinert C, Sendner C, et al. All the numbers are us: Large-scale abuse of contact discovery in mobile messengers[J]. *Cryptology ePrint Archive*, 2020.

[59] Lu H R, Xing L Y, Xiao Y, et al. Demystifying Resource Management Risks in Emerging Mobile App-in-App Ecosystems[C]. *The 2020 ACM SIGSAC Conference on Computer and Communications Security*, 2020: 569-585.

[60] Aonzo S, Merlo A, Tavella G, et al. Phishing Attacks on Modern Android[C]. *The 2018 ACM SIGSAC Conference on Computer and Communications Security*, 2018: 1788-1801.

[61] Discord and slack are becoming potent toolsfor malware attacks. Steven Melendez. https://www.fastcompany.com/90622606/discord-and-slack-are-becoming-a-potent-tool-for-malware-attacks. 2022.

[62] Cheng Y, Park J, Sandhu R. Preserving User Privacy from Third-Party Applications in Online Social Networks[C]. *The 22nd International Conference on World Wide Web*, 2013: 723-728.

[63] Xue Y J, Xue K P, Gai N, et al. An Attribute-Based Controlled Collaborative Access Control Scheme for Public Cloud Storage[J]. *IEEE Transactions on Information Forensics and Security*, 2019, 14(11): 2927-2942.

[64] Cohn-Gordon K, Cremers C, Garratt L, et al. On post-compromise security[C]. *2016 IEEE 29th Computer Security Foundations Symposium*, 2016: 164-178.

[65] Cohn-Gordon K, Cremers C, Dowling B, et al. A Formal Security Analysis of the Signal Messaging Protocol[J]. *Journal of Cryptology*, 2020, 33(4): 1914-1983.

[66] Cohn-Gordon K, Cremers C, Garratt L, et al. On Ends-to-Ends Encryption: Asynchronous Group Messaging with Strong Security Guarantees[C]. *The 2018 ACM SIGSAC Conference on Computer and Communications Security*, 2018: 1802-1819.

[67] Cremers C, Hale B, Kohbrok K. The Complexities of Healing in Secure Group Messaging: Why {Cross-Group} Effects Matter[C]. *30th USENIX Security Symposium (USENIX Security 21)*, 2021: 1847-1864.

[68] Martiny I, Kaptchuk G, Aviv A J, et al. Improving Signal's Sealed Sender[C]. *Network and Distributed Systems Security Symposium*, 2021: 21-24.

[69] Isobe T, Ito R. Security Analysis of End-to-End Encryption for Zoom Meetings[J]. *IEEE Access*, 9: 90677-90689.

[70] Gauthier N H, Husain M I. Dynamic Security Analysis of Zoom, Google Meet and Microsoft Teams[M]. Silicon Valley Cybersecurity Conference. Cham: Springer International Publishing, 2021: 3-24.

[71] Which Video Call Apps Can You Trust? The Mozilla Blog. Ashley Boyd. https://blog.mozilla.org/en/privacy-security/which-video-call-apps-can-you-trust/. Apr. 2020.

[72] Tyagi N, Miers I, Ristenpart T. Traceback for End-to-End Encrypted Messaging[C]. *The 2019 ACM SIGSAC Conference on Computer and Communications Security*, 2019: 413-430.

[73] Chase M, Deshpande A, Ghosh E, et al. SEEMless: Secure End-to-End Encrypted Messaging with less Trust[C]. *The 2019 ACM SIGSAC Conference on Computer and Communications Security*, 2019: 1639-1656.

[74] Jiang L Z, Chen L Q, Giannetsos T, et al. Toward Practical Privacy-Preserving Processing over Encrypted Data in IoT: An Assistive Healthcare Use Case[J]. *IEEE Internet of Things Journal*, 2019, 6(6): 10177-10190.

[75] Atlidakis V, Godefroid P, Polishchuk M, et al. RESTler: stateful REST API fuzzing[C]. *2019 IEEE/ACM 41st International Conference on Software Engineering*, 2019: 748-758.

[76] Zoom Explodes Serious Vulnerability: Any Website Can Hijack Mac Cameras, Hurting 4 Million Users. Oskarsv. https://doc. xuwenliang.com/docs/it/4186. Jul. 2019.
(Zoom 爆出严重漏洞: 任何网站可劫持 Mac 摄像头, 祸及 400 万用户. Oskarsv. https://doc.xuwenliang.com/docs/it/4186. Jul. 2019.)

[77] Mac Zoom vulnerability details analysis. FreeBuf. https://www.freebuf.com/vuls/208177.html. Jul. 2019.
(Mac Zoom 漏洞细节分析. FreeBuf 网络安全行业门户. https://www.freebuf.com/vuls/208177.html. Jul. 2019.)

[78] Ling C, Stringhini G, Balcı U, et al. A first look at zoombombing[C]. *IEEE Security & Privacy*, 2021: 22-30.

[79] What You Should Know About Online Tools During the COVID-19 Crisis. Lindsay Oliver. https://www.eff.org/deeplinks/2020/03/what-you-should-know-about-online-tools-during-covid-19-crisis. Mar. 2020.

[80] Dispelling Zoom Bugbears: What You Need to Know About the Latest Zoom Vulnerabilities. Tod Beardsley. https://www. rapid7.com/blog/post/2020/04/02/dispelling-Zoom-bugbears-what-you-need-to-know-about-the-latest-Zoom-vulnerabilities/. Apr. 2020.

[81] Große-Kampmann M, Gruber M. Business Chat is Confused. It Hurt Itself in its Confusion-Chishing[EB/OL]. 2021: ResearchGate Preprint DOI:10.13140/RG.2.2.26864.79365.

[82] Remote Code Execution in Slack desktop apps + bonus. Oskarsv. https://hackerone.com/reports/783877. Jan. 2020.

[83] Compagno A, Conti M, Lain D, et al. Don't Skype & Type!: Acoustic Eavesdropping in Voice-over-IP[C]. *The 2017 ACM on Asia Conference on Computer and Communications Security*, 2017: 703-715.

[84] Sabra M, Maiti A, Jadliwala M. Zoom on the Keystrokes: Exploiting Video Calls for Keystroke Inference Attacks[EB/OL]. 2020: arXiv: 2010.12078. https://arxiv.org/abs/2010.12078

[85] Sato S, Kageyama Y, Ishizawa C, et al. Person Region Extraction and Background Replacement in Images for Privacy Protection[J]. *International Journal of the Society of Materials Engineering for Resources*, 2018, 23(2): 162-166.

[86] Saxena G, Mishra G, Shrotriya N. Application of Deep Learning in Classification of Encrypted Images[M]. Communications in Computer and Information Science. Cham: Springer International Publishing, 2021: 711-719.

[87] Liu H B, Li Z H, Xie Y C, et al. LiveScreen: video chat liveness detection leveraging skin reflection[C]. *IEEE INFOCOM 2020 - IEEE Conference on Computer Communications*, 2020: 1083-1092.

[88] Cloud drive Latest To Leak Users' Data. Shanahan, E. (2014). https://www.encryptedcloud.com/blog/google-drive-latest-leak-users-data/. Jan. 2017.

[89] Zhang S Y, Han S, Zheng B K, et al. Group Key Management Protocol for File Sharing on Cloud Storage[J]. *IEEE Access*, 8: 123614-123622.

[90] Chen W, Hoang T, Guajardo J, et al. Titanium: A Metadata-Hiding File-Sharing System with Malicious Security[C]. *Network and Distributed Systems Security Symposium*, 2022: 1-18.

[91] Li H W, Dai Y S, Tian L, et al. Identity-Based Authentication for Cloud Computing[M]. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009: 157-166.

[92] Anand P, Ryoo J, Kim H, et al. Addressing security challenges in cloud computing—a pattern-based approach[C]. *2015 1st International Conference on Software Security and Assurance*, 2017: 13-18.

[93] Akhtar D N, Kerim D B, Perwej D Y, et al. A Comprehensive Overview of Privacy and Data Security for Cloud Storage[J]. *International Journal of Scientific Research in Science, Engineering and Technology*, 2021: 113-152.

[94] de Clercq J. Single Sign-on Architectures[M]. Infrastructure Security. Berlin, Heidelberg: Springer Berlin Heidelberg, 2002: 40-58.

[95] Pan J, Communication N A B T, Components C, et al. Physical integrity attack detection of surveillance camera with deep learning based video frame interpolation[C]. *2019 IEEE International Conference on Internet of Things and Intelligence System*, 2020: 79-85.

[96] Heydari V, Aerospace, Communication N A B T, et al. A new security framework for remote patient monitoring devices[C]. *2020 International Symposium on Networks, Computers and Communications*, 2020: 1-4.

[97] Liang X Y. Security Analysis of Virtual Private Network[J]. *Secrecy Science and Technology*, 2017(7): 40-41.
(梁向阳. 虚拟专用网络安全性分析[J]. *保密科学技术*, 2017(7): 40-41.)

[98] Singh K K V V, Gupta H. A New Approach for the Security of VPN[C]. *The Second International Conference on Information and Communication Technology for Competitive Strategies*, 2016: 1-5.

[99] Yang C H, Kuo T Y, Ahn T, et al. Design and implementation of a secure instant messaging service based on elliptic-curve cryptography[J]. Journal of Computers, 2008, 18(4): 31-38.

[100] Zoom concedes custom encryption is substandard as Citizen Lab pokes holes in it. Chris Ducketthttps://www.zdnet.com/article/zoom-concedes-custom-encryption-is-sub-standard-as-citizen-lab-pokes-holes-in-it/. April 5, 2020.

[101] Reddy V, University K L, Rao B, et al. A Combined Clustering and Geometric Data Perturbation Approach for Enriching Privacy Preservation of Healthcare Data in Hybrid Clouds[J]. *International Journal of Intelligent Engineering and Systems*, 2018, 11(1): 201-210.

[102] Geetha M A. Fuzzy-Based Random Perturbation for Real World Medical Datasets[J]. *International Journal of Telemedicine and Clinical Practices*, 2015, 1(2): 111.

[103] Atlidakis V, Geambasu R, Godefroid P, et al. Pythia: grammar-based fuzzing of rest apis with coverage-guided feedback and learning-based mutations[EB/OL]. 2020: ArXiv Preprint ArXiv:2005.11498.

杨泽霖 于 2021 年在宁夏大学网络工程专业获得学士学位。现在西安电子科技大学网络空间安全专业攻读硕士学位, 研究兴趣包括: 物联网安全, 软件安全, 人工智能安全。Email: zelinyang@stu.xidian.edu.cn

王基策 于 2022 年在中国科学院大学信息安全专业获得博士学位, 现为北京计算机技术及应用研究所工程师。研究兴趣领域包括: 软件安全、移动安全等。Email: wangjc@nipc.org.cn

徐斐 于 2021 年在华北电力大学软件工程专业获得学士学位, 现在西安电子科技大学电子信息专业攻读硕士学位, 研究领域为信息安全。研究兴趣包括: 人工智能安全, 流量分析。Email: xuf@nipc.org.cn

黄宇航 于 2021 年在西安电子科技大学网络工程专业获得学士学位。现在于中国科学院大学电子信息专业攻读硕士学位, 研究领域为移动安全。研究兴趣:安卓安全, 小程序安全。Email: huangyh@nipc.org.cn

艾铭超 于 2022 年在浙江工商大学信息安全专业获得学士学位。现在西安电子科技大学电子信息专业攻读硕士学位, 研究领域为物联网安全。研究兴趣包括: 网络空间安全、系统安全等。Email: aimingchao@hotmail.com

马慧 于 2021 年在江苏大学信息安全专业获得学士学位。现在西安电子科技大学电子信息专业攻读硕士学位。研究领域为物联网安全。研究兴趣包括: 隐私计算、区块链安全。Email: hui_ma@stu.xidian.edu.cn

王鹤 于 2016 年在西安电子科技大学信息安全专业获得博士学位。现任西安电子科技大学网络与信息安全学院讲师。研究领域为应用密码、量子密码协议。研究兴趣包括: 威胁信息交换共享、量子密码协议。Email: hewang@xidian.edu.cn

张玉清 于 2000 年在西安电子科技大学获得博士学位。现任中国科学院大学教授, 博士生导师。主要研究方向为网路与信息系统安全。Email: zhangyq@nipc.org.cn