5G移动终端安全关键技术研究

Research on Key Technologies of 5G Mobile Terminal Security

齐　霄，侯玉华（中讯邮电咨询设计院有限公司，北京 100044）
Qi Xiao，Hou Yuhua（China Information Technology Designing & Consulting Institute Co.，Ltd.，Beijing 100044，China）

摘　要：
首先分析了5G时代移动终端和移动通信面临的主要安全风险，进而对目前主流的终端安全技术如系统隔离技术和虚拟专网技术的现状和不足进行了总结。提出了满足高安全移动通信和移动办公要求的终端安全解决方案，包括基于硬件的系统隔离、门卫式内网VPN接入和系统间安全通信方案3个组成部分，系统性解决移动终端硬件、操作系统、应用、数据和网络通信安全问题。

关键词：
移动终端；双系统；硬件隔离；内网接入
doi：10.12045/j.issn.1007-3043.2023.04.007
文章编号：1007-3043（2023）04-0029-04
中图分类号：TN915.08
文献标识码：A
开放科学（资源服务）标识码（OSID）：

Abstract：
It first analyzes the main security risks faced by mobile terminal and mobile communication in 5G era，then it summarizes the current status and shortcomings of mainstream terminal security technologies such as system isolation technology and virtual private network technology. It proposes terminal security solutions that meet the requirements of high-security mobile communication and mobile office，including three components：hardware-based system isolation，doorman-style intranet VPN access，and system-level security communication solutions.These solutions comprehensively solve the security issues of mobile terminal hardware，operating systems，applications，data and network communication.

Keywords：
Mobile terminal；Dual-system；Hardware isolation；Intranet access

引用格式：齐霄，侯玉华. 5G移动终端安全关键技术研究[J]. 邮电设计技术，2023（4）：29-32.

0 引言

随着5G移动终端类型和应用场景不断丰富，移动终端从传统的通话短信功能为主的通信终端发展到应用于日常生活和工作各领域的智能终端。终端技术架构也发生了很大变化：终端芯片集成度更高、功能模块更加丰富；操作系统智能化趋势越来越强，可承载的应用和业务越来越复杂。与此同时，各行业充分利用移动通信的移动特性、便捷性、灵活性等优点，将移动终端接入企业内部网络，利用移动终端处理工作和生产事务，并在移动终端中存储企业内部数据。

5G移动终端存在信息安全风险，如何在利用移动通信便捷性的同时，保障通信安全、数据安全，保护个人隐私、保护企业商业秘密、保护国家信息安全，成为当前移动信息安全领域必须面对的重点问题，也正因如此，移动终端安全关键技术具有重要研究意义。本文深入分析5G移动终端面临的安全风险和当下主流的终端安全技术，创新性提出5G终端双硬件双系统的门卫式隔离防护和内部网络安全接入技术方案，为保护个人隐私、商业秘密和国家密码提供信息安全保

收稿日期：2023-02-16

障。

1 安全风险分析

工作人员使用移动终端接入办公内网访问内网数据,并将内网数据存储在本地。如果移动终端与办公内网之间的数据通信以及移动终端数据存储没有有效的安全防护,那么办公内网的数据将暴露于互联网,存在很大的信息安全风险。因此无论是移动终端还是办公内网,以及两者之间的通信过程,都急需具备安全防护能力。移动终端和办公内网进行通信时,主要面临如下安全问题。

a)身份认证安全风险。无论是密码、验证码还是生物识别,均存在被破解和仿冒的风险,如果移动终端被假冒接入内网,那么内网存在数据泄露的隐患。

b)数据存储安全风险。移动终端对于数据存储缺少精细化的管控措施,数据通常以明文形式保存在存储设备中,缺少机密性和完整性保护,极易被病毒、木马、恶意程序篡改和窃取。此外,一旦手机遗失,数据泄露风险很高。

c)通信安全风险。移动通信提供了数据传输的链路,包括无线数据、语音、短消息等,此外还有蓝牙、红外、NFC等近场通信。通信网络和设备不可控因素较多,用户通信数据易被不法分子截获篡改。

d)终端软硬件安全风险。移动终端通常采用iOS、Android、Arm等软硬件平台,根据披露,以上软硬件平台均存在安全漏洞及后门,有极大的安全隐患。

2 安全技术概述

目前主流的终端安全技术方案主要有2种方式,一种是通过终端虚拟化系统隔离技术实现一个终端硬件运行多个操作系统,不同系统相互隔离,保证终端的数据安全和运行环境安全;另一种是通过虚拟专用网络技术,如VPDN、VPN等技术手段,保证移动终端和企业内网的接入安全和网络传输安全。

2.1 终端系统隔离

当前主流的移动终端中,同一套硬件下仅支持一套操作系统,不同的应用软件间使用软件沙箱技术隔离。例如,Android系统中扩展了Linux内核安全模型的用户和权限机制,将多用户间的隔离机制应用于程序间隔离。每一个应用程序均被系统分配单独的Linux系统用户标识(UID),使得Android应用程序运行于独立的Linux进程空间。

随着虚拟化技术的发展和终端硬件能力的提升,在终端中使用虚拟机(Virtual Machine,VM)隔离多个应用成为可能。使用VM的目的在于创建一个隔离的、受控的运行环境,使应用程序不受VM外安全风险的影响。不同VM间的访问必须通过系统间接口才可完成,因此更容易监控,也更安全。虚拟化平台可通过探针对VM中的操作系统和应用软件进行监控,进行病毒查杀。同时必须保证VM中的应用不能穿透虚拟机访问虚拟化平台的数据,保护虚拟化平台免遭网络攻击。

终端双系统主要指的是在1个终端中运行2个相互隔离、彼此独立的操作系统,兼顾工作使用和个人使用的不同需求,如图1所示。2个系统中,1个为安全系统(工作系统),1个为个人系统(生活系统),具有彼此独立的运行环境、文件系统和数据存储,实现应用和数据的隔离。安全系统根据安全需求,从硬件驱动层对终端的部分功能进行限制(例如限制工作系统调用话筒、摄像头、蓝牙等功能)。进一步地,移动终端可以定义双系统切换管理策略,并为2个系统设置各自独立的安全策略管控,减少信息安全风险。

图1 虚拟机共享终端硬件

2.2 虚拟专网技术

在经历了多年的发展后,虚拟专用网络(VPN)技术形成了2种成熟的技术架构,分别是互联网安全(Internet Protocol Security,IPSec)协议和安全套接层(Secure Sockets Layer,SSL)协议。在TCP/IP分层模型中,IPSec协议是工作在网络层的安全协议,通过重建网络层中的IP包来实现安全的虚拟网络传输通道,通过密码算法对IP层数据包进行机密性以及完整性保护。SSL协议及其后继版本传输层安全(Transport Layer Security,TLS)协议是工作在传输层和应用层之间的安全协议,为网络通信提供安全及数据完整性。

采用虚拟专网技术可实现移动终端安全接入企业内网并保证网络传输安全。首先企业内网对接入终端的身份合法性进行认证,检查方式有多种形式,比如通过MAC地址、IP地址、用户名和密码、生物识

别、PKI公钥证书体系、USBKey等，或者是几种形式的组合运用。身份认证通过后才可继续进行VPN通信。在VPN通信过程中，IPSec协议或SSL协议可提供如下安全能力。

a）数据机密性。发送方通过密码算法对数据进行加密计算，在传输通道中进行传输的是密文数据，合法接收方可以通过密码算法对数据进行解密计算获得明文数据。即使数据在传输过程中被窃取截获，窃取方也无法对密文数据正确解密获取明文数据。

b）数据完整性。发送方通过密码算法对数据进行摘要计算和签名计算，将摘要值和签名值与数据同时进行传输。接收方可以通过密码算法对接收到的数据进行验签计算，验证数据来源以及没有被篡改。

c）防止重放。数据接收端可以检测过时的或者已经收到过的报文。

2.3 存在问题

无论是采用终端系统隔离技术还是虚拟专用网络技术，硬件层面都受到移动终端硬件结构的限制，移动终端的安全机制和安全策略均需通过CPU来实现。在软件层面，安全机制受到操作系统控制，数据的处理、传输和存储均通过操作系统来实现。因此，系统隔离和安全通信协议只是在移动终端中被CPU和操作系统调用式实现，如果CPU或者操作系统本身存在漏洞和后门，那么所有的安全机制可能会被旁路，从而丧失安全性。

3 终端安全解决方案

本文在现有技术方案的基础上对5G移动终端的安全架构进行创新优化设计。第一，基于硬件的系统隔离。在1台移动终端中集成2套硬件（主要包括CPU、内存和存储），分别用于运行安全系统和生活系统，将操作系统或虚拟机建立在独立的硬件系统之上，使得应用运行环境和存储空间的隔离更加彻底。第二，门卫式内网VPN接入。采用门卫式方式实现VPN内网接入，在基带芯片与安全系统CPU之间放置加密协处理器，实现终端CPU与基带芯片之间的门卫式物理隔离，使得通信数据在CPU和基带芯片之间的交互必须通过安全协处理器，保证VPN通路不会被旁路和替代。第三，系统间安全通信方案。安全系统和生活系统的CPU借助加密协处理器进行通信，并采用加密通信协议进行控制信号和通信数据的交互。

3.1 基于硬件的系统隔离

安全移动终端在1台移动终端中集成2套硬件（主要包括CPU、内存和存储），分别用于运行2套操作系统和上层应用，硬件结构如图2所示。安全移动终端在硬件层面可分为安全系统、生活系统、安全通信模块（加密协处理器）、通用通信模块（基带处理器和射频模块）、系统外设等。

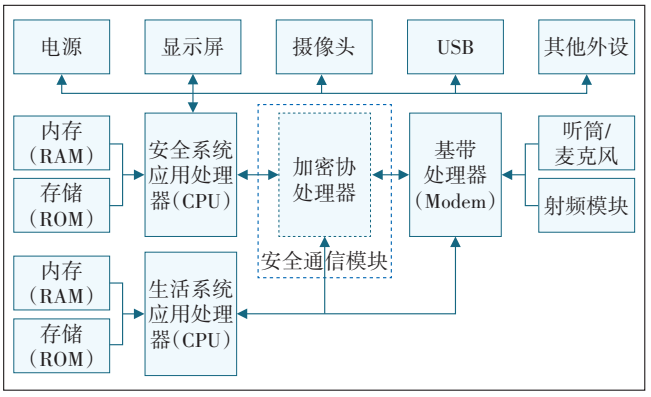

图2　终端硬件结构

安全通信模块是安全移动终端的安全核心，分别连接安全系统、生活系统和通用通信模块。安全通信模块的核心器件是加密协处理器，通过硬件的方式实现安全系统与通用通信模块、安全系统与生活系统之间的安全数据通信，实现安全移动终端双系统之间的硬件隔离。

安全系统主要包括应用处理器（CPU）、内存和存储，为办公应用提供运行环境、文件系统和数据存储。安全系统的CPU与安全协处理器直接相连，所有与通用通信模块或生活系统的交互数据均需通过安全通信模块的处理，与通用通信模块或生活系统无直接的物理连接。安全系统无法进行普通的网络通信，必须通过安全通信模块建立门卫式的VPN通信通道，才可与办公内网连接。安全系统与系统功能外设直接连接，直接控制外设功能。

生活系统主要包括应用处理器（CPU）、内存和存储，与通用通信模块直接连接，基本功能与普通智能手机的相关模块没有区别。生活系统与安全系统没有直接的物理连接。生活系统与安全系统之间的控制信号和通信数据交互是受控的，通过安全通信模块完成。安全系统与系统外设之间没有物理连接，当需要调用外设功能时，需要安全系统的授权，并在安全系统的监控下进行功能调用。

通用通信模块主要包括基带处理器和射频模块，与普通智能手机的通信模块没有区别。该模块负责

将安全系统通过安全通信模块发送的通信数据或者生活系统的通信数据进行网络传输。

系统外设主要包括电源、显示屏、摄像头、听筒、麦克风、USB等,其功能与普通智能手机的系统外设基本一致。系统外设直接受安全系统控制,在受控条件下可以间接被生活系统调用。

安全移动终端在软件层面可分为安全系统、生活系统和VPN模块,结构如图3所示。安全系统和应用系统具备独立的硬件抽象层、操作系统层和应用层,彼此独立运行,VPN模块负责安全系统的网络通信功能。因为将操作系统或虚拟机建立在独立硬件系统之上,应用运行环境和存储空间的隔离更加彻底。

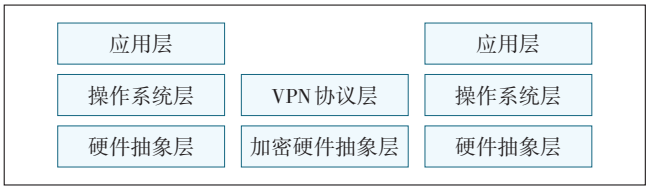

图3 终端软件结构

3.2 门卫式内网VPN接入

安全移动终端可以实现终端与办公内网之间的安全通信,为终端的内网接入以及数据传输提供门卫式安全能力。在具备移动通信快捷、灵活优势的同时,安全移动终端可以有效防止各类外部攻击、非授权用户访问和信息泄露。办公内网结构以及在移动互联网中的位置如图4所示。

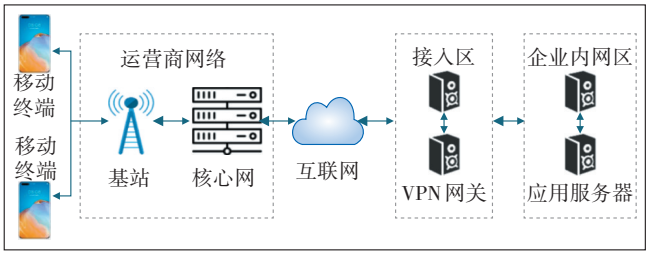

图4 网络结构

接入区是办公内网安全接入功能的核心模块,主要包括VPN网关。VPN网关部署在应用服务器与互联网之间,作为外部用户进入办公内网的入口,实现接入用户身份认证、虚拟网络通道协议和密码安全功能。安全移动终端与VPN网关之间通过VPN通信协议进行内网数据的安全通信。

业务区是办公内网各项业务的承载模块,主要包括应用服务器,应用服务器与互联网应用服务器没有重大区别。

门卫式内网VPN接入的核心是移动终端与内网VPN网关之间的通信通道无法被旁路和恶意替换。在网络侧,办公内网与内网接入区(VPN网关)物理连接,保证办公内网与互联网物理隔离。普通互联网用户无法访问办公内网。在终端侧,安全移动终端的安全系统通过安全通信模块(加密协处理器)与基带连接,加密协处理器建立与办公内网VPN网关之间的虚拟网络通信通道。安全系统与办公内网之间的虚拟网络通信通过移动互联网进行传输,所有通信数据均可保证机密性、完整性和来源可靠性。

3.3 系统间安全通信方案

安全移动终端内安全系统和生活系统之间是物理隔离的,二者之间无法直接访问。但是,双系统之间需要相互配合,存在控制指令和部分业务数据的交互需求。所以,在受控条件下完成双系统之间有限的安全通信尤为关键。

加密协处理器是双系统之间安全通信的实现模块,为双系统建立类似于服务器之间的安全通信协议。只有在符合安全策略的前提下双系统之间才可进行数据交互,实现安全系统向生活系统的系统外设使用授权和双系统之间的消息提醒。

4 总结

本文介绍了移动终端在企业应用中面临的安全风险,分析了常用的终端安全技术和存在问题。基于虚拟化系统隔离技术和虚拟专网技术,提出基于硬件的系统隔离、门卫式内网VPN接入和系统间安全通信方案,分析安全移动终端和办公内网的软硬件结构和功能。本文提出的安全移动终端和办公内网已在对信息安全有较高要求的政务通信和办公领域中实际应用,为保障国家信息安全起到了重大作用。

参考文献:

[1] 徐厦杰. 移动安全专用通信模块研究与实现[D]. 北京:中国电子科技集团公司电子科学研究院,2021.

作者简介:
齐霄,硕士,主要从事移动安全应用开发和密码技术应用工作;侯玉华,高级工程师,硕士,长期从事移动终端和可信安全相关技术的研发和标准研究工作。