移动智能终端安全

刘家佳　解　军　刘晴晴　编著

西安电子科技大学出版社
http://www.xduph.com

网络空间安全理论与技术研究丛书

移动智能终端安全

刘家佳　解　军　刘晴晴　编著

西安电子科技大学出版社

内 容 简 介

本书从研究移动智能终端安全所需的基础知识、常见的移动智能终端攻击技术及如何防御对智能终端的攻击三个角度介绍了移动智能终端的安全问题，分别对应书中的基础篇、攻击篇及防护篇。

本书可供信息安全研究者以及移动智能终端生产企业从业者学习参考，亦可作为高等学校网络空间安全专业的教材使用。

图书在版编目(CIP)数据

移动智能终端安全 / 刘家佳，解军，刘晴晴编著. —西安：西安电子科技大学出版社，2019.11
ISBN 978-7-5606-5482-9

Ⅰ. ① 移… Ⅱ. ① 刘… ② 解… ③ 刘… Ⅲ. ① 移动终端—智能终端—安全技术—高等学校—教材 Ⅳ. ① TN87

中国版本图书馆 CIP 数据核字(2019)第 241764 号

策划编辑 马乐惠
责任编辑 闵远光 雷鸿俊
出版发行 西安电子科技大学出版社(西安市太白南路 2 号)
电 话 (029)88242885 88201467 邮 编 710071
网 址 www.xduph.com 电子邮箱 xdupfxb001@163.com
经 销 新华书店
印刷单位 陕西日报社
版 次 2019 年 11 月第 1 版 2019 年 11 月第 1 次印刷
开 本 787 毫米×1092 毫米 1/16 印张 16.5
字 数 389 千字
印 数 1～3000 册
定 价 40.00 元
ISBN 978-7-5606-5482-9 / TN
XDUP 5784001-1

前　言

随着移动互联网与物联网的快速融合发展，人们从传统的互联网时代逐步进入物联网时代，网络终端设备如智能手机、智能水表、智能家电等迅猛发展，其中最为普遍的莫过于智能手机。与此同时，信息时代互联网应用领域也从商业、金融、行政及军事延伸到了百姓生活的方方面面，如出现了网购、公交信息查询、旅游信息查询、外卖、移动支付等层出不穷的应用。随之而来的问题是个人安全事件频发，安全问题已从企业、政府、军方及敏感单位的信息安全拓展到了个人隐私、财产及人身安全。个人安全问题频发成为物联网时代的一个突出特点，其涉及的人群之大、范围之广更是前所未有。造成个人信息安全问题的根源是移动智能终端本身存在的安全隐患，因此解决移动智能终端安全问题既是迫在眉睫的问题，又是物联网健康发展的一个重要保障。

由于移动智能终端的多样性，很难通过一本书把所有的移动智能终端都讲清楚，因此本书以应用最广泛的移动智能终端即智能手机为研究对象，介绍了其硬件、系统软件、应用软件三个层面存在的安全问题，其总体思路是：首先介绍相关的基础知识，然后介绍从三个层面形成的攻击，最后介绍如何从这三个层面进行防护。

本书共包括 3 篇 16 章内容：基础篇共 5 章，内容分别为移动智能终端安全概述、移动智能终端硬件体系结构及面临的安全威胁、操作系统安全架构及面临的安全威胁、SQLite 数据库及面临的安全威胁、移动智能终端应用软件及面临的安全威胁；攻击篇共 8 章，内容分别为固件篡改攻击、蓝牙攻击、WiFi 连接攻击、权限提升攻击、通过虚假 App 对手环进行信息窃取及劫持、组件通信漏洞挖掘、SQLite 数据泄露和恶意代码的植入；防护篇共 3 章，内容分别为应用软件的防护、基于系统安全机制的防护和外围接口的防护。

本书的写作目的是让读者系统地、全方位地了解移动终端安全，以弥补目前市面上缺乏这类书籍的缺憾。

编　者

2019 年 7 月

目　录

基　础　篇

攻 击 篇

防 护 篇

基 础 篇

本篇是攻击篇及防护篇的基础。由于篇幅所限，其中所介绍内容的深度可能还达不到实际攻击和防护的要求，仅起着完善读者知识体系结构的作用，希望能达到抛砖引玉的效果。

本篇按照“硬件→操作系统→数据库→应用软件”的线索分别介绍各个层次的模型及架构，并通过分析模型及架构的设计思路和安全机制，描述各个层次所面临的安全威胁或机制的局限性。

第 1 章　移动智能终端安全概述

1.1　移动智能终端安全现状

移动智能终端设备是传统移动设备智能化、网络化发展的产物，通常具有较小的显示屏幕和触控输入功能，可随时随地访问并获取数据信息。移动智能终端设备多具有开放的操作系统平台，能够进行网络连接，具有多媒体数据采集、传输、控制等功能；对应用软件具有包容和协作能力，允许后续应用系统的开发和安装，便于功能扩充；允许设备终端之间及设备服务端与控制端之间通过 3G 或 4G 网络进行数据和指令交互。

随着移动互联网的发展以及近年来的科技创新，移动智能终端技术发展迅猛，移动智能终端设备也变得十分普及，图 1-1 所示为部分移动智能终端设备。以移动智能手机为例，2010 年全球智能手机出货量为 3.26 亿部，2013 年为 10.042 亿部，2015 年高达 12.927 亿部，2017 年达 14.62 亿部，2018 年达 14.56 亿部，全球智能手机的市场份额已于 2012 年超越传统手机的市场份额。

图 1-1　移动智能终端设备

移动智能终端设备并不局限于常见的智能手机、平板电脑、智能电视等，还包括新一代的智能穿戴设备等新产品，如智能手表、智能眼镜、网联汽车等。

随着移动智能终端设备的发展与普及，移动智能终端设备已深入到日常生活的各个方面，由此产生的信息安全问题也越来越多，因此其安全性变得尤为重要。下面将从硬件安全、操作系统、应用软件及外围接口等四个方面来说明移动智能终端的安全现状。

1. 硬件安全

当前移动智能终端的硬件安全主要指固件安全。固件是指存储在具有永久存储功能器件中的二进制程序。在以微处理器为核心的电子设备中，固件为上层软件使用硬件设备提供调用接口，是电子系统中的重要组成部分。固件芯片作为集成电路芯片的一员，虽然以灵活多样的存在形式方便了用户使用，但也为信息系统的安全埋下了隐患。目前已有黑客

展示了相关研究成果，例如：通过破解苹果键盘固件而成功攻破 Mac 系统；在未使用用户名和密码的情况下登录操作系统，记录用户输入的内容，窃取用户隐私数据等。

2. 操作系统

当前移动智能终端操作系统的安全问题主要是防止权限提升攻击。

权限提升攻击是指恶意软件通过调用合法的、具有更高权限的应用软件来提升自己的权限，以此获得非法权利。此类攻击的本质是利用系统权限申请及管理的漏洞来实施攻击行为。Schlegel 等展示了一种手机木马 Soundcomber，该木马本身不具有操作音频的权限，却能够通过其他应用的权限获取音频数据。Grace 等利用权限提升检测工具 Woodpecker 检测出有些软件不遵守权限机制，将保护隐私数据的权限暴露给其他应用。

3. 应用软件

当前移动智能终端应用软件的安全问题主要是防止恶意代码的威胁及应用软件中组件间通信所造成的信息泄露。

恶意代码是指故意编制或设置的、对网络或系统产生威胁或潜在威胁的软件代码。常见的恶意代码有计算机病毒(简称病毒)、特洛伊木马(简称木马)、计算机蠕虫(简称蠕虫)、后门、逻辑炸弹等。当前信息社会恶意代码泛滥，安全形势不容乐观。我国曾出现过一种专门感染国内智能手机支付银行客户端的洛克蠕虫，该蠕虫可感染某银行客户端，通过二次打包的方式将恶意代码嵌入银行 App，在未经用户允许的情况下私自下载和安装带有恶意代码的银行 App，窃取用户的银行账户和密码，并转移账户中的资金。

移动智能终端操作系统间的组件通信需要配置组件，某些组件可能会被其他应用调用，组件间的通信会在配置组件的文件中暴露，如果此时调用了不恰当的组件，就会造成信息泄露。

4. 外围接口

当前外围接口的安全问题主要来自蓝牙接口及 WiFi 接口的威胁。

蓝牙接口的安全威胁主要有蓝牙漏洞攻击、蓝牙劫持和蓝牙窃听等。

WiFi 接口的威胁主要是 WiFi 的“无线钓鱼”，即普通的无线用户在不知情的情况下连接到伪装成合法接入点的无线网络，但该无线网络是专门为吸引受害者而设立的“蜜罐”或开放网络。用户连接“蜜罐”网络后，攻击者会获得用户无线设备的访问权限，以此窃取用户的敏感数据，给用户造成损失。

1.2　移动智能终端安全分类

1.2.1　硬件安全

固件是写入 EROM(可擦写只读存储器)或 EEPROM(电可擦除可编程只读存储器)中的程序，也指设备内部保存的设备驱动程序。通过固件，操作系统才能按照标准的设备驱动实现特定机器的运行动作。由此可见，固件承担着一个系统最基础和最底层的工作，同时也决定着硬件设备的功能和性能。

对于独立可操作的电子产品，固件是指操作系统。比如 PSP 的固件，就是指 PSP 的操作系统(iPhone、MP4 同理)。而对于非独立的电子产品，比如硬盘、鼠标、BIOS、光驱、U 盘等设备，固件是指其最底层的、让设备得以运行的程序代码。

当手机用户通过第三方手机操作系统固件进行“刷机”或“越狱”操作时，手机就没有了权限限制，此时恶意软件有可能随着这种不安全的系统固件植入到用户的手机中。通过固件植入的恶意软件会伪装成系统程序进行恶意操作，如恶意吸费、修改用户数据、窃取用户隐私等。由于绝大多数手机安全软件不会主动获取手机的最高权限，因而无法卸载这些恶意软件。

1.2.2 操作系统安全

在移动智能终端面临的安全问题中，操作系统的安全问题是最普遍的。在 2016 年年底时，软件安全公司 Arxan 发现 90%的移动应用中至少存在两项安全问题根源于底层操作系统的漏洞，由此可见移动智能终端的系统安全形势愈加严峻。

移动智能终端操作系统现已成为面向应用服务、构建于硬件之上的完整平台体系。它作为一种开放式平台，任何应用开发者都可以为支持智能操作系统的终端设备开发应用软件。

由于移动智能终端自身特性的要求，其操作系统的安全性显得更加突出和重要。另外，由于移动智能终端的资源和处理能力有限、安全机制不完善、漏洞修复不及时等，又使移动智能终端操作系统极易受到恶意攻击。

移动智能终端操作系统目前存在的安全威胁主要有三类：操作系统漏洞、操作系统后门和操作系统 API 滥用。

1. 操作系统漏洞

操作系统漏洞是指应用软件或操作系统软件在逻辑设计上的缺陷或错误。移动智能终端操作系统存在大量已知的和未知的漏洞，这些漏洞严重威胁操作系统的安全。任何攻击者都可以利用操作系统漏洞对移动智能终端用户发起远程攻击，例如窃取用户信息、盗拨电话、破坏用户数据等。

操作系统漏洞的影响范围十分广泛，既包括系统本身及其支撑软件，也包括网络客户和服务器软件、网络路由器和安全防火墙等。换言之，不同种类的软、硬件设备之间，同种设备的不同版本之间，以及同种系统在不同的设置条件下，都会存在各自不同的安全漏洞问题。

2. 操作系统后门

移动智能终端操作系统后门是指绕过系统的安全性控制而获得程序或系统访问权的程序。

程序员为了后期可以更好地修改程序，会在开发阶段于软件内部创建后门程序。恶意攻击者可以利用操作系统后门进行权限提升、敏感信息查找、远程控制等恶意行为。

大部分恶意攻击者在利用操作系统后门时，会刻意避开操作系统日志，以免引起管理员的注意，以达到即使攻击者正在使用操作系统也不会显示攻击者在线的目的。由此可见，操作系统后门的隐蔽性强，对攻击者的侦查十分困难，造成的安全威胁也极大。

3. 操作系统 API 滥用

API(Application Programming Interface，应用程序编程接口)是一些提前定义的函数，可在无需了解内部工作机制的细节或访问源代码的情况下，为应用程序提供一组访问功能的接口或服务。

移动智能终端操作系统使用开放式架构为开发者提供 API 和开发工具包，开发者既可以调用 API 和开发工具包进行正常的开发，也可以利用恶意代码滥用操作系统的 API 来达到破坏系统、窃取隐私的目的。因此，操作系统 API 滥用为恶意攻击提供了条件。这些威胁存在的根源之一是系统权限机制存在的漏洞，攻击者可以通过权限提升来达到攻击的目的。

权限提升分为水平权限提升和垂直权限提升。

(1) 水平权限提升。水平权限提升是指某个权限较小的应用(调用方)可以无限制地访问另外一个具有更高权限的应用(被调用方)，即系统中某个实体获取了另一个同类实体的权限。

(2) 垂直权限提升。垂直权限提升是指实体获得系统保留的更高级别权限。通常，实体利用内核的 Bug 获得超级用户管理权限。攻击者可以利用手机操作系统中的软件漏洞来实现权限提升。

1.2.3　应用软件安全

应用软件是用户使用各种程序设计语言编制的应用程序的集合。移动智能终端通过下载应用软件来为用户提供更完善的功能服务。

工信部发布的数据显示，至 2013 年 5 月，我国手机上网用户已达 7.83 亿，iOS 设备的 App Store 中的应用数量高达 90 万个，下载量突破 500 万次，其他应用渠道的移动应用总量突破 600 万；至 2014 年 6 月，我国手机网民规模就已达 5.27 亿，占全国网民总数的 83.4%；到了 2019 年 4 月，手机上网用户规模达 12.9 亿，移动互联网累计流量达 351 亿 GB。我国移动互联网已进入全民时代。但是，移动智能终端的大规模使用也造成了恶意收费、窃取用户隐私数据等安全事件的发生，严重损害了用户的利益，给社会带来了巨大的经济损失。

这些安全问题存在的根源可以归纳为两个方面：首先是恶意软件的威胁，恶意软件主要利用应用软件本身安全措施薄弱的缺陷，完成恶意代码的植入；其次是应用软件内部组件间的通信缺乏保护，从而被恶意程序窃取，造成信息泄露。

1. 恶意软件及其威胁

恶意软件的威胁主要指破坏系统和消耗资源、窃取用户重要信息、恶意扣费和诱使用户定制收费业务、恶意推广非法应用软件等行为。它具备以下特征：

1) 强制安装

(1) 在安装过程中未提示用户。

(2) 在安装过程中未提供明确的选项以供用户选择。

(3) 在安装过程中未给用户提供退出安装的功能。

(4) 在安装过程中提示用户不充分、不明确(明确、充分的提示信息包括但不限于软件

作者、软件名称、软件版本、软件功能等)。

2) 难以卸载

(1) 未提供明确的、通用的卸载接口。

(2) 软件卸载时附有额外的强制条件，如卸载时需要联网、输入验证码、回答问题等。

(3) 在不受其他软件影响或人为破坏的情况下，不能完全卸载，仍有子程序或模块在运行(如以进程方式运行)。

3) 浏览器劫持

(1) 限制用户对浏览器设置的修改。

(2) 对用户所访问网站的内容擅自进行添加、删除、修改等操作。

(3) 迫使用户访问特定网站或不能正常上网。

(4) 修改用户浏览器或操作系统的相关设置，导致出现以上三种现象。

4) 广告弹出

广告弹出是指未明确提示用户或未经用户许可，利用安装在用户终端上的软件弹出广告的行为。具体包括：

(1) 安装时未告知用户该软件的弹出广告行为。

(2) 弹出的广告无法关闭。

(3) 广告弹出时未告知用户该弹出广告的软件信息。

5) 恶意收集用户信息

(1) 收集用户信息时，未提示用户会有收集信息的行为。

(2) 未提供用户选择“是否允许收集信息”等相关选项。

(3) 用户无法查看自己被收集的信息。

6) 恶意卸载

恶意卸载是指在未明确提示用户或未经用户许可的情况下，误导、欺骗用户卸载其他软件的行为。

2. 应用软件的信息泄露

应用软件组件间通信的过程主要指 Activity、Service、Broadcast Receiver 和 Content Provider 四类组件之间的通信依赖于 Intent，该通信可以是双向或单向的。如果 Intent 指定了接收者的组件名，则 Intent 是显式的；否则，Intent 是隐式的，系统会根据 Intent 的其他参数选择接收者，即接收者的组件名是匿名的。如果攻击者伪造某个组件替代系统中的某个匿名组件，从而产生组件劫持攻击，就会泄露隐私数据，甚至污染返回的数据。

注：Intent 是 Android 程序中各组件间交互的一种重要方式，常用于启动组件和传递数据。

1.2.4 外围接口安全

移动智能终端外围接口存在的安全问题主要来源于蓝牙接口和 WiFi 接口。

蓝牙接口的安全威胁主要是针对旧版蓝牙设备的漏洞攻击、劫持攻击和窃听攻击等。

1. 蓝牙接口的安全威胁

(1) 蓝牙漏洞攻击：攻击者利用旧设备的固件漏洞来访问并开启蓝牙设备的攻击方式。

(2) 蓝牙劫持攻击：攻击者通过向已开启蓝牙功能的设备发送未经请求的消息来发起攻击。该攻击方式类似于对电子邮件用户进行垃圾邮件或网络钓鱼的攻击。

(3) 蓝牙窃听攻击：攻击者通过利用旧设备固件上存在的漏洞来获取设备地址和命令使用权限并进行信息窃取。该攻击方式无需通知用户就可以对设备进行窃听，从而使攻击者能够访问数据、拨打电话或窃听通话等。

2. WiFi 接口的安全威胁

WiFi 连接过程是：用户加入一个无线网络，找到该无线网络的服务集标识(SSID，用来区分不同的网络)；用户输入密码并连接成功后，将该无线网络的 SSID 和密码存入系统配置文件中；当终端开启 WiFi 查找功能时，终端会根据系统配置文件中的无线网络的 SSID 和密码进行匹配，并自动尝试连接和存储无线网络。

WiFi 接口的安全威胁主要是：在公共场合，攻击者利用自己提供的无线网络引诱用户连接，当用户的终端连接进入后，用户终端就会和攻击者处于同一个无线局域网中，如果用户通过该不安全的网络进行数据传输，则传输内容很有可能会被攻击者截获，从而损害用户的利益。

针对移动智能终端外围接口存在安全威胁的问题，我国应重视外围接口的保护，提高安全性，并加强外围接口安全防护技术的研发和体系的建设。

小　结

本章首先概述了移动智能终端安全的现状，然后依据移动智能终端的结构层次，按照由下到上的顺序分别介绍了移动智能终端硬件层、系统层及应用软件层的安全问题。硬件层主要介绍了固件安全，系统层主要介绍了权限提升及 API 调用安全问题，应用软件层主要介绍了面临恶意代码植入的安全问题。最后介绍了移动智能终端与网络连接的两个主要接口(蓝牙接口与 WiFi 接口)的安全问题。

第 2 章　移动智能终端硬件体系结构及面临的安全威胁

2.1　硬件体系结构概述

移动智能终端硬件体系结构如图 2-1 所示。

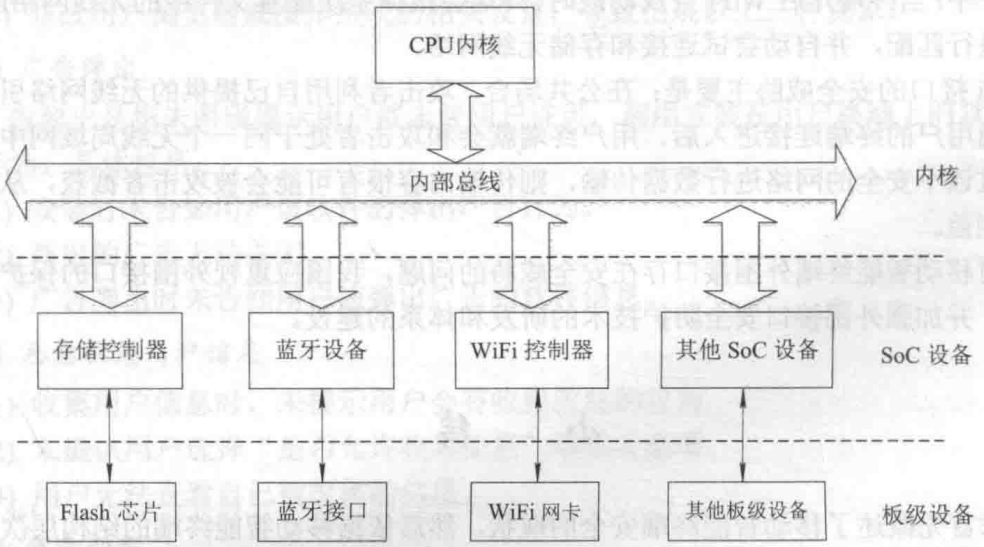

图 2-1　移动智能终端硬件体系结构图

以中央处理器(CPU)内核为核心，移动智能终端硬件系统可分为三个层次：内核、SoC 设备和板级设备。

(1) CPU 和内部总线构成移动智能终端硬件系统的内核，提供核心的运算和控制功能。目前智能终端使用的 CPU 内核以 ARM 居多，主要有 ARM9、ARM11 等架构。

(2) SoC 设备与内核集成在同一芯片上，通过内部总线与 CPU 内核互连，SoC 设备一般包含存储控制器(如 Flash 控制器)、蓝牙设备、WiFi 控制器等。

(3) 板级设备通过 SoC 设备与 CPU 连接，板级设备通常是一些功能独立的处理单元，如 Flash 芯片、蓝牙接口、WiFi 网卡等。

2.2　MCU

1. 概述

MCU(MicroController Unit，微控制单元/单片机)是将中央处理器(CPU)的频率和规格做

适当缩减，并将内存、计数器、USB、A/D 转换器、UART、PLC、DMA 等接口整合在单一芯片上所形成的芯片级计算机。MCU 可以为不同应用场合做不同的组合控制。MCU 的特点主要有：

(1) 高集成度，体积小，可靠性高。MCU 将各功能部件集成在一块晶体芯片上，集成度高，体积很小；MCU 将程序指令等固化在 ROM(只读存储器)中以达到不易被破坏的特点，从而可靠性很高。

(2) 控制性能强。MCU 具有非常丰富的指令系统，适用于专门的控制功能。

(3) 低电压，低功耗，便于生产便捷式产品。MCU 的工作电压仅为 1.8～3.6 V，工作电流仅为几百微安。

(4) 易扩展。MCU 外部有供扩展用的三根总线和管脚，容易组成各种规模的计算机应用系统。

(5) 优异的性能价格比。MCU 性能优越，销量大，价格低，性价比极高。

2. ARM

ARM 芯片是 MCU 的一种。ARM 芯片具有功耗低、成本低的特点，特别适用于移动设备。ARM 目前主要授权 ARM9、ARM11 和 Cortex 三个系列的芯片设计。

ARM9：采用冯·诺依曼体系结构和三级流水线，提供 0.9 MIPS(在工作频率为 1 MHz 情况下)的指令执行速度。

ARM11：采用哈佛体系结构，指令和数据分属不同的总线，可以并行处理，采用五级流水线。

Cortex：目前 ARM 公司最新的指令集结构，表示的是 ARM11 之后的一系列处理器。

3. MCU 的主要分类

1) 按用途分类

通用型：将可开发的资源(ROM、RAM、I/O、 EPROM)等全部提供给用户。

专用型：硬件及指令按照某种特定用途来设计。例如录音机机芯控制器、打印机控制器、电机控制器等。

2) 按处理的数据位数分类

根据总线或数据暂存器的宽度，MCU 又分为 1 位、4 位、8 位、16 位、32 位甚至 64 位等不同类别。

4 位 MCU 应用于计算器、车用仪表、无线电话、CD 播放器、LCD 驱动控制器等；8 位 MCU 应用于电表、马达控制器、电动玩具、键盘及 USB 等；16 位 MCU 应用于移动电话、数字相机及摄录放影机等；32 位 MCU 应用于激光打印机与彩色传真机中，工作于网络操作、多媒体处理等复杂处理的场合；64 位 MCU 应用于多媒体互动系统、高级电视游戏机及高级终端机等。

目前，4 位 MCU 已经退出历史舞台。8 位 MCU 工作频率在 16～50 MHz 之间，强调简单效能、低成本应用，目前在 MCU 市场中仍占有一定地位。16 位 MCU 以 16 位运算、16/24 位寻址能力及 24～100 MHz 频率为主流规格，部分 16 位 MCU 额外提供 32 位加/减/乘/除的特殊指令。32 位 MCU 是市场的主流，工作频率大多在 100～350 MHz 之间，执行效能更佳，应用类型也相当多元。64 位 MCU 价格昂贵，应用面窄，未普遍应用。