doi:10.11959/j.issn.1000-436x.2016266

基于透明加密的移动终端数据防泄露系统

黄振涛[1]，何暖[2]，付安民[1]，况博裕[1]，张光华[3]
（1. 南京理工大学计算机科学与工程学院，江苏 南京 210094；
2. 中国船舶工业综合技术经济研究院，北京 100081；
3. 河北科技大学信息科学与工程学院，河北 石家庄 050000）

摘 要：企业关键数据向移动终端设备延伸，使移动终端数据泄露成为企业面临的一个新的问题。针对移动终端数据泄露问题，提出了基于预解密的透明加密技术，有效解决移动终端传统透明加密技术只能保证应用层安全的缺陷，并提升了透明加密性能。同时，利用瘦客户端与移动终端数据防泄露相融合的思想，进一步设计面向移动终端的虚拟远程桌面技术，彻底屏蔽数据流传输的弊端，保证了移动终端数据的安全传输。在此基础上，设计与实现了一套面向移动智能终端的数据防泄露系统。
关键词：数据防泄露；透明加密；虚拟远程桌面
中图分类号：TP393 **文献标识码**：A

Data leakage prevention system based on transparent encryption for mobile terminal equipment

HUANG Zhen-tao[1], HE Nuan[2], FU An-min[1], KUANG Bo-yu[1], ZHANG Guang-hua[3]
(1. School of Computer Science and Engineering, Nanjing University of Science and Technology, Nanjing 210094, China;
2. China Institute of Marine Technology & Economy, Beijing 100081, China;
3. College of Information Science and Engineering，Hebei University of Science and Technology，Shijiazhuang 050000, China)

Abstract: With the trend that enterprise key data moves to mobile terminal, data leakage prevention has become an important issue on mobile terminal. To solve the problem, a pre-decryption transparent encryption technology was set up which solved the problem that traditional transparent encryption technology only can ensure application layer security, in addition, performance on mobile was improved. At the same time, taking advantage of the idea of combining thin client and mobile terminal to prevent leakage of data, a virtual remote desktop technology on mobile was proposed, which completely shield the shortcomings of data transmission and ensure the safe transmission of mobile terminal data. Finally, a data leakage prevention system for mobile terminal was set up, which makes the mobile terminal fully and effectively protected.
Key words: data leakage prevention, transparent encryption, virtual remote desktop

1 引言

随着移动终端设备功能日益强大，移动互联网产业得到了迅猛发展，正逐渐渗透到人们生活、工作的各个领域。越来越多的企业员工已经或即将摆脱办公室的约束，通过移动终端设备来处理日常工作事务。当前，企业的“移动化”是大势所趋，市场调研企业高德纳[1]预计，到 2017 年底，企业级移动应用的市场需求增长速度将至少是现有供给速度的 5 倍以上。然而，企业关键数据向

收稿日期：2016-09-15
通信作者：付安民，fam_0522@163.com
基金项目：国家自然科学基金资助项目（No.61572255）；江苏省“六大人才高峰”高层次人才基金资助项目（No.XYDXXJS-032）；中国博士后科学基金资助项目（No.2015M582622）；物联网信息安全技术北京市重点实验室开放课题基金资助项目（No.J6V0011104）
Foundation Items: The National Natural Science Foundation of China (No.61572255), Six Talent Peaks Project in Jiangsu Province (No.XYDXXJS-032), The China Postdoctoral Science Foundation (No.2015M582622), Open Fund of Beijing Key Laboratory of IOT Information Security Technology (No.J6V0011104)

移动终端设备延伸，使移动终端数据泄露成为企业面临的一个新的问题。据 2016 年国家保密网数据分析显示，高达 95%的企业数据泄露是由内部人员造成的。因此，如何实现移动终端的安全办公，预防企业重要数据泄露已经成为当前亟需解决的关键问题。

移动终端数据泄露途径主要分为在使用状态下的泄密、在存储状态下的泄密和在传输状态下的泄密[2]。虽然传统电脑端数据防泄露技术能够较好地解决企业数据防泄露问题，但是，基于移动终端的办公模式与电脑端具有很大差异。在数据防泄露方面，电脑端的数据防泄露技术并不完全适用于移动终端。

目前，移动终端数据防泄露技术刚刚起步，Pistoia 等[3]提出一种实时隐私数据强化保护方案，通过提供配置合适的数据保护策略，实时监控终端数据流向，并提出了一种加强的数据分析算法保护关键数据不泄露。Chow 等[4]提出了一种云环境中基于用户行为的移动终端认证框架，结合基于支持认证决策 TrustCube 的灵活框架和基于行为认证(用户行为翻译为认证分数)的隐式认证，通过决策和动态调整可以权衡可用性和信任之间的平衡。纵观以往方案，大多是针对数据泄露某些特定途径提出的改进方案，缺少针对移动终端数据防泄露问题全面有效的分析并提出合理的解决方案。

目前移动终端数据防泄露技术还存在诸多问题。1) 移动终端透明加密技术问题，基于文件系统的驱动加密技术[5]工作性能不稳定，且需要编译用户移动终端的系统，通用性不强，不适用于企业数据防泄露体系。基于 Hook 技术的透明加密技术[6,7]通用性强，但相比驱动加密技术，文件读写慢、性能较差。2) Android 平台数据隔离技术[8,9]，主要是通过关键数据加密存储、文档数据防泄露（DLP, data leakage prevention）控制[10]、应用锁定[11]等实现数据隔离的安全体系，公私数据并没有做到彻底的环境隔离。存在企业涉密进程遭到信息被劫持的可能，现在的方案并不能有效预防企业关键数据泄露[12~14]。

本文设计与实现了一个面向移动终端的数据防泄露系统，具体贡献如下。

1) 首次提出了基于移动终端的文件预解密透明加密技术。利用基于 Xposed 框架[15]、Hook 技术完成文件系统透明加解密功能，并在此基础上嵌入预解密思想，解决了移动终端传统透明加密技术安全性缺陷问题，并且提升了透明加密性能，节约了文件系统操作过程的开销。

2) 将远程桌面协议应用到移动终端。基于 libfreerdp-android.so 动态链接库设计并实现了虚拟远程桌面方案。提出了瘦客户端理念与移动终端数据防泄露相融合的思想，实现了移动终端远程桌面协议（RDP, remote desktop protocol）技术[16]。

3) 设计并实现了一个以透明加密和虚拟远程桌面为核心的移动终端的数据防泄露系统。系统在实现透明加密和虚拟远程桌面的同时，对接入移动终端实现了安全准入控制、终端设备管控、行为安全审计等有效保护，确保移动终端数据存储、传输、使用的全面安全。

2 算法设计

2.1 预解密透明加密

本节提出了基于移动终端的预解密透明加密算法，改进了传统移动终端透明加密性能不稳定以及安全性差的缺陷，实现了移动终端安全高效的透明加解密功能。

2.1.1 概念定义

预解密透明加密算法建立在以下一些相关概念的基础上。

定义 1 强密文集。强密文的集合 $M=\{M_1, M_2, \cdots, M_i\}$，包含 i 个强密文的项集称为 i 强密文集。

定义 2 预解密临时文件集。预解密临时文件的集合 $P=\{P_1,P_2,\cdots,P_i\}$，包含 i 个预解密临时文件的项集称为 i 预解密临时文件集。

定义 3 明文集。明文的集合 $N=\{N_1,N_2,\cdots,N_i\}$，包含 i 个明文的项集称为 i 明文集。

2.1.2 Xposed 框架

预解密透明加密技术整体是基于 Xposed 框架、Hook 技术和 Android 操作系统文件系统行为实现透明加解密操作，通过覆盖原生的/system/bin/app_process 程序，对 app_process 进行扩展，控制 zygote 进程，使 app_process 在启动过程中会加载 XposedBridge.jar 这个 jar 包，从而完成对 Zygote 进程及其创建的 Dalvik 虚拟机的劫持。在 Android 系统启动的时候，Zygote 进程加载 XposedBridge，将所有需要替换的 method 通过 JNI 方法 HookMethodNative 指向原生方法 XposedCallHandler，此方法再转入

handleHookedMethod 这个 Java 方法执行用户规定的 Hook 函数。从而使终端在开机状态下完成对所有的 Hook 函数的劫持，在原函数执行的前后加上预解密透明加密处理过程，其实质就是改变被劫持对象在 Dalvik 虚拟机中的实现。

2.1.3 预解密透明加密算法形式化描述

本文提出的预解密透明加密算法在基于 Android 开源 Xposed 框架上进行开发。传统移动终端透明加密算法执行效率差，并且算法实现基于 Android 应用层框架，安全性低。预解密透明加密算法根据 Xposed 框架特性，实现在 Android 运行环境层的 Hook 功能调用，算法首先初始化 Hook 模块功能，针对输入项集进行预处理分析，判断文件操作行为模式并根据行为模式执行相应的 Hook 函数，核心内容主要包括了预解密临时文件预处理与更新、1 次密文的 2 次解密、预加密操作以及预解密临时文件的 2 次强加密，预解密透明加密算法步骤如算法 1 所示。

算法 1　文件预解密透明加密算法

输入　*i* 强密文集/*i* 明文集

输出　*i* 明文集/*i* 强密文集

begin

1) init Xposed;

2) for each *i* in *File_Set_Open*

3)　if *pre_verification*(*i*) ∉ *P*

4)　　*update*(*i*)→P_i;

5)　　*re_decrypt*(P_i)→(*i*,*N*);

6) for each *i* in *File_Set_Close*

7)　*str_ecrypt*(*i*,*M*);

8)　*update*(*i*)→P_i;

end

1) 初始化 Xposed 框架，加载文件系统 Hook 模块。

2) 遍历文件标识符，判断 *i* 是否属于强密文子集。

3) 遍历预解密临时文件集 *P*，判断强密文是否属于 *P*。

4) 预解密子集 *i* 并实时更新预解密临时文件集 *P*。

5) 2 次解密预解密临时文件子集，并生成明文对象赋值对象 *i*，更新明文集 *N*。

6)~8)遍历文件标识符，并将明文子集 2 次加密为强密文，更新强密文集 *M* 和预解密临时文件集 *P*。

2.2 虚拟远程桌面

本节提出了基于移动终端的虚拟远程桌面技术，提出了瘦客户端理念与移动终端数据防泄露相融合的想法，相比传统移动终端数据防泄露方案，彻底屏蔽了数据流传输的弊端，保证了移动终端数据的安全传输。

2.2.1 概念定义

虚拟远程桌面框架设计建立在以下一些相关概念的基础上。

定义 4　鼠标事件集。鼠标事件集合 $Cursor\_Event\_Set=\{C_1,C_2,\cdots,C_i\}$，指定移动终端向 RDP 服务端 3389 端口发送的鼠标操作指令，并接收 3389 端口返回的操作集。

定义 5　键盘事件集。键盘事件集合 $Key\_Event\_Set=\{K_1,K_2,\cdots,K_i\}$，指定移动终端向 RDP 服务端 3389 端口发送的键盘值集，并接收 3389 端口返回的键盘值集。

定义 6　位图更新。位图更新集合 $Update\_Graphics\_Set=\{U_1,U_2,\cdots,U_i\}$，指定移动终端向 RDP 服务端 3389 端口发送的位图封信请求，并接收在电脑端生成封装位图更新数据分组集。

2.2.2 框架概述

本文将 PC 端远程桌面控制协议移植到 Android 移动终端，采用以 libfreerdp-android.so 动态链接库为基础的 RDP 技术实现虚拟远程桌面方案。本方案的客户端包括 3 个模块：鼠标事件模块、键盘事件模块和位图事件更新模块，采用 freerdp 的核心源码编译得到 libfreerdp-android.so 动态链接库[20,21]，实现与 RDP 协议的兼容通信，通过 TCP 层采用握手过程建立稳定的网络连接，保证移动端与 PC 端安全可靠通信，虚拟远程桌面结构如图 1 所示。

2.2.3 虚拟远程桌面算法形式化描述

本文提出的 Android 平台虚拟远程控制算法虚拟远程桌面以 libfreerdp-android.so 动态链接库为基础，首先将终端事件分为 RDPSocket 事件和 UISocket 事件，分别处理 RDP 网络通信数据和终端 RDP 行为，通过精确的多路复用行为进行分类处理，其次将分类行为通过 rdp_main_loop 实现实时 RDP 通信和事件更新，表现到终端顶层则为鼠标、键盘以及位图等实时的更新与显示，虚拟远程桌面算法步骤如算法 2 所示。

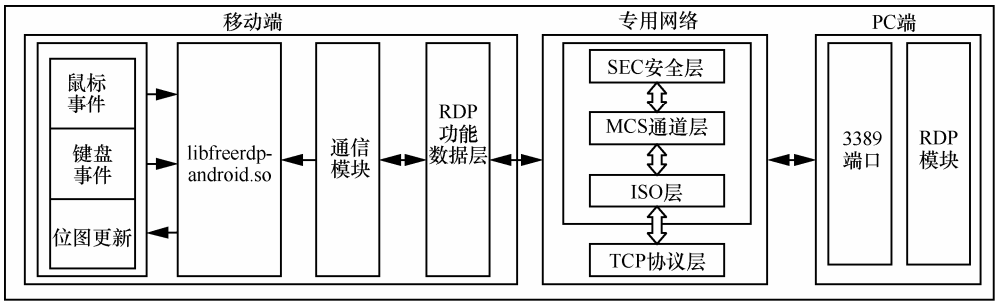


图 1 虚拟远程桌面结构

算法 2 虚拟远程桌面算法

输入 C（鼠标事件集），K（键盘事件集）

输出 U（位图更新集）

begin

1) event_list *el* = *rdp_connect*()

2) do *rdp_main_loop*(*el*)

3) for each μ in *el*

4) *process_events*(μ,*C*,*K*,*U*)

5) ui_sync

end

1) RDP 通信过程初始化，建立通信连接，并配置连接信息、数据目录、行为属性等，将事件列表序列化为 *el* 集合。

2)~3) 遍历 *el* 事件集合，并依次取出事件子集，赋值对象 μ。

4) 匹配对应子集，并在 *Cursor_Event_Set*、*Key_Event_Set*、*Update_Graphics_Set* 相应事件集中回调 μ 的动作函数，并最终进行进程事件处理 *process_events*(μ,*C*,*K*,*U*)。

5) 接受 4)中的处理结果对象，并进行 UI 视图同步，提取给上层用户。

3 系统设计与实现

本系统采用 C/S 架构开发，客户端含有 2 个核心模块：透明加密模块和虚拟安全桌面模块，服务端主要完成对客户端的远程管控。

3.1 系统框架

本文提出的面向移动智能终端的数据防泄露系统框架由移动终端客户端和远程服务器组成，移动终端客户端是一款基于移动终端的办公管理程序，远程服务端负责远程管控客户端，包含下发办公文件、管理指令、收集客户端数据等数据防泄露控制，系统总体结构如图 2 所示。

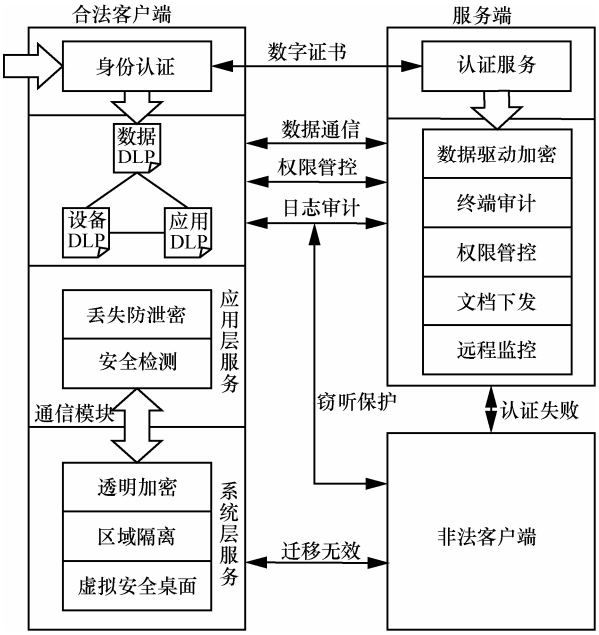


图 2 系统总体结构

移动终端的主要功能模块有：透明加密模块、区域隔离模块，同时还具备虚拟安全桌面模块、身份认证模块、丢失防泄密模块、安全检测模块。其中，透明加密模块采用预解密透明加密技术实现透明加解密；区域隔离模块采用基于动态沙箱技术[19]的公私域隔离框架，在移动终端上建立了一个安全、独立的工作区，将需保护的数据存储在受保护的安全区内，避免非法存取核心数据；虚拟安全桌面模块采用 RDP 技术实现移动终端远程办公功能；身份认证模块负责实时认证客户端的合法性身份；丢失防泄密模块负责当移动终端丢失或者进行违规操作时，及时对移动终端进行锁死、清除关键数据、实时定位移动终端等功能；安全检测模块采用恶意代码静态检测技术，负责对移动终端进行全盘安全扫描，发现并查杀可能导致企业数据泄露的恶意代码[20]。

服务端的功能是负责远程管控客户端，主要

包括：数据驱动加密模块、终端审计模块、权限管控模块、文档下发模块、远程监控模块。其中，数据驱动加密模块采用基于 minifilter 微驱动过滤框架的电脑端驱动加密技术[21]，完成与移动终端相对应的透明加密模块；终端审计模块负责为企业提供集中监管移动终端敏感操作行为的功能，通过实时记录移动终端可能造成关键数据泄露的行为，使管理员能够高效快速识别安全事件并做出响应；终端管控模块负责对指定移动终端进行指定策略控制、权限赋予等操作，保证移动终端时刻被远程监控；文档下发模块负责企业关键数据的下发管理；远程监控模块负责实时定位移动终端的位置，掌握终端运行状态以及监控其行为模式，起到对办公终端的监管作用。

3.2　预解密透明加密

服务端的主要工作是负责定义办公文档数据格式，并将办公文档通过 2 次加密成为强密文状态。其中，16 位校验符负责区分办公文档与用户个人文档，16 位预解密偏移值负责指向移动终端上预解密临时文件的具体路径位置，16 位权限标识符负责制定可以阅读此办公文档的最低权限要求，16 位总长度负责制定此办公文档具体长度，32 位可选项留空，可供后期维护使用。从明文状态预加密到 1 次密文状态采用加密性能较好的 DES 加密算法，然后将 1 次密文状态的文档通过安全系数较高的 AES 加密算法加密为强密文状态。至此，强密文状态的办公文档具备下发到客户端的条件。办公文档数据定义如图 3 所示。

校验符（16位）	预解密偏移值（16位）
权限标识符（16位）	总长度（16位）
可选项（32位）	
强密文数据	

图 3　文档数据定义

移动终端的主要工作是针对存储于本设备上的办公文档进行本文提出的基于 Xposed 框架的文件预解密透明加密。读文档时，首先打开文档，Hook 模块提取 16 位校验符，判断当前文档是否为办公文档，若否，则直接跳过 Hook 作用域，返回文档内容给用户，若是，则提取 16 位权限标识符并进行实时数字证书认证；若当前终端不合法，则返回强密文状态数据给用户，若合法，则提取 16 位预解密偏移值，对当前文档进行预解密文件验证；若验证不通过，不存在 1 次密文，则对当前缓存中的强密文进行预解密，并生成相应预解密临时文件，若验证通过，存在相应 1 次密文，则提取预解密文件并替换缓存中的强密文。然后，针对缓存中的 1 次密文进行 2 次解密。最终输出明文到应用层。在修改并存储文档时，首先，提取 16 位权限标识符并进行实时数字证书认证，若当前终端不合法，则无权修改数据，直接返回原强密文，若合法，则对明文数据 1 次加密，并进行预解密文件更新；然后进行 2 次强加密，并将强密文存储到终端内存中。方案步骤如图 4 所示。

3.3　虚拟远程桌面

本文方案的 RDP 通信连接过程如下。首先各种功能数据都是通过创建单独的虚拟通道进行传输，在初始连接后，进一步的信息通信前，需要开辟相应的通道。客户端首先发送一个建立连接独立空间请求，再发送一个用户绑定请求，若服务器同意，将发送用户绑定确认（且含有需要申请的虚拟通道总数 $total_{\text{channel}}$），随后客户端申请虚拟通道。虚拟通道号从 1 001+2=1 003 开始到 1 001+$total_{\text{channel}}$ 结束，每次申请都应返回一个申请结果。当通道申请通过后，开始建立系统登录的初始连接，进行数据通信交换。其中，关于位图数据的连接，服务器首先发送关于图形方面的基本参数设置，客户端应该对这些设置进行反馈，并返回鼠标事件和键盘事件数据。此后的处理是顺序发送同步信息、控制信息分组、输入信息分组、字体信息分组等，同时顺序接收同步信息分组、两控制信息分组，完成事件的通信过程。

4　测试与结果分析

本文的测试移动终端部署在 Android v4.0 的 Mi2 实验机上，并搭建了 LASS (Linux、Apache、SQlServer、Servlet/JSP)框架，其中，操作系统版本为 Debian Linux 7，Linux 内核为 3.2.0-4-AMD64，Apache 版本为 Apache 2.2.24，SQLServer 版本为 Microsoft SQL Server 2008 (RTM)，Servlet/JSP 版本为 3.0/2.2。系统首先分析比较当前数据防泄露产品与本系统的区别，然后针对透明加密模块比较了传统透明加密方案与本文预解密透明加密方案的安全性与效率；针对区域隔离和虚拟远程桌面方案的有效性进行了讨论，最终测试了核心模块的有效性。

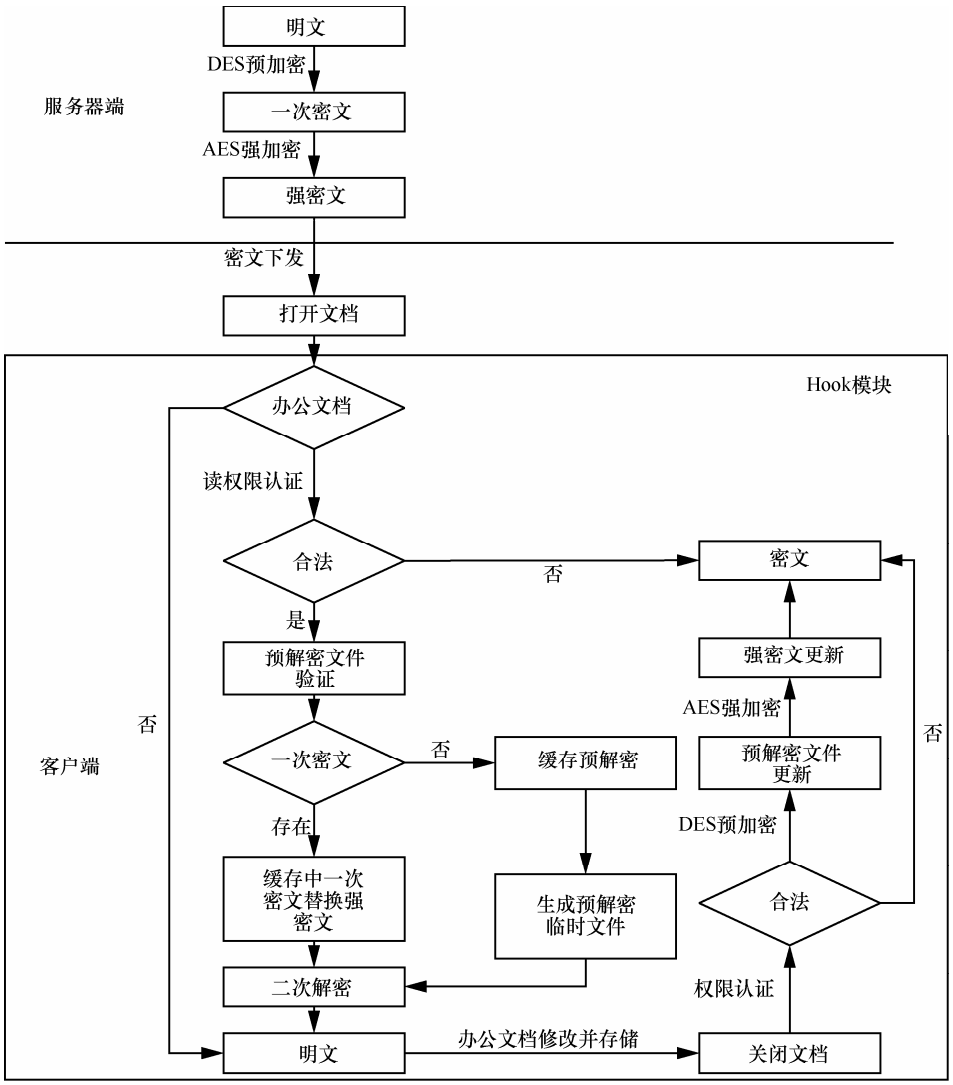


图 4　预解密透明加密方案步骤

4.1　系统对比分析

为了突出本系统设计合理性与创新性，本文使用 360 天机、MobileArk 以及 CS&S 这 3 种不同类型企业安全系统作为比较对象，比较结果如表 3 所示。

表 3　本系统与其他企业安全系统的比较

功能模块	360 天机	MobileArk	CS&S	本文系统
透明加密	✓	✓	✓	✓
区域隔离	✓	✓	✓	✓
远程桌面			✓	✓
丢失防密	✓	✓	✓	✓
安全检测	✓			✓
终端审计	✓			✓
终端管控	✓	✓	✓	✓

如表 3 所示，本文系统相较其他安全系统，数据保护覆盖范围更为广泛，并且创新地将瘦客户端理念引入到数据防泄露中来，引入虚拟远程桌面模块，彻底保证数据的防泄露。

4.2　预解密透明加密分析

4.2.1　性能分析

传统透明加密技术在打开加密文件时，采用一次性解密过程。Android 操作系统对软件性能要求高，企业如果采用加密强度高的加密算法（如 AES、RSA 等），当这种透明加密方案移植到移动终端时会引起性能耗损问题。本文方案采用 2 次解密的预解密透明加密方案，规避高性能损耗的解密操作，当在合法移动终端上打开加密文件时，只进行简单的 2 次解密，大大提高透明加密技术在移动终端上的性能，预解密透明加密性能比较结果如图 5 所示。

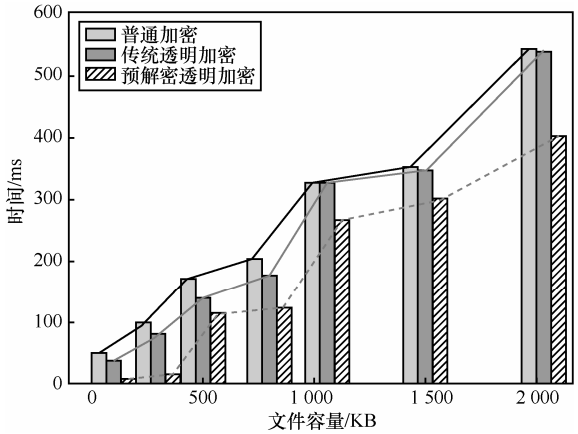


图 5　预解密透明加密性能比较

4.2.2　安全性分析

本方案采用 Xposed 框架 Hook 技术，通过覆盖原生的/system/bin/app_process 程序，对 app_process 进行扩展，控制 zygote 进程，使 app_process 在启动过程中会加载 XposedBridge.jar 这个 jar 包，从而完成对 Zygote 进程及其创建的 Dalvik 虚拟机的劫持。在 Android 系统启动的时候，Zygote 进程加载 XposedBridge，将所有需要替换的 method 通过 JNI 方法 HookMethodNative 指向 XposedCallHandler，XposedCallHandler 在转入 handleHookedMethod 这个 Java 方法执行用户规定的 Hook 函数，从而使终端在开机状态下完成对所有的 Hook 函数的劫持，在原函数执行的前后加上自定义代码。因此方案安全性保证在 Android 框架的 RUNTIME 层（Android 系统第 3 层）。安全性比较结果如表 4 所示。

表 4　　安全性比较

安全层级	传统加密	传统透明加密	预解密透明加密
网络层	✓	✓	✓
应用层		✓	✓
框架层			✓
运行层			✓

4.3　虚拟远程桌面有效性分析与讨论

本节针对 Android 平台实现的虚拟远程桌面方案进行有效性分析，并进行性能评估。表 5 列出了本模块各项性能评估的计算式，其中 Re_Time 和 Con_Time 分别表示了单次实验终端与服务器间的请求时间戳和连接时间戳。使用本地测试机在不同网络状态条件下对电脑端进行请求连接，统计其连接应答时间，并针对虚拟远程桌面的鼠标事件、键盘事件和位图更新事件向用户提供 UI 更新的速率进行平均值统计，表 6 展示了虚拟远程桌面访问服务器应答时间的测试结果。可以看出，虚拟远程桌面请求及应答时间控制在毫秒级。

表 5　　虚拟远程桌面性能计算式

计算分类	计算式	实验次数
请求时间	Sum(Re_Time1,－Re_Time2)	5
连接时间	Sum(Con_Time1, －Con_Time2)	5
鼠标更新相应	avg(Cursor_Event_Set)	10
键盘更新相应	avg(Key_ Event_Set)	10
位图更新相应	avg(Update_ Graphics_Set)	10

表 6　虚拟远程桌面连接应答时间性能耗损

范围	请求时间/ms	连接时间/ms	鼠标更新响应时间/ms	键盘更新响应时间/ms	位图更新响应时间/ms
5	0.00	0.00	0.00	0.00	0.15
10	0.4	0.4	0.22	0.22	0.38
20	0.9	≈1	≈4	≈4	≈7
50	≈200	≈250	≈600	≈600	≈1 000

4.4　系统有效性分析与讨论

针对 BYOD 移动办公场景可能造成的各种数据泄露途径集进行分析，选取了文献[4]和文献[21]中提出的数据泄露途径集，如表 7 所示，实验表明，基于透明加密的移动终端数据防泄露系统能有效防御移动办公环境下可能造成的数据泄露。

表 7　　本系统数据防泄露有效性

泄露途径	攻击尝试	预防尝试	预防
操作失误	6	6	✓
传输泄露	12	12	✓
存储泄露	1	1	✓
使用泄露	3	3	✓

4.5　实验验证分析

主要针对预解密透明加密和虚拟远程桌面功能的有效性进行验证，模块按照系统设计编码实现，通过不同用户机的多次测试，各模块调用正常，基本功能运行正常，达到性能稳定要求。

5　结束语

本文针对企业办公移动终端面临的数据泄露威胁，设计与实现了一套面向移动智能终端的数据防泄露系统。首先在传统透明加密技术的基础上改进并设计了一套预解密透明加密方案。其次，设计并实现了基于动态沙箱技术的区域隔离方案。最后，创新地将瘦客户端理念引入到移动终端数据防泄露体系中，将 RDP 远程桌面协议移植到 Android 平台数据防泄露系统中，形成了以这 3 块为核心技术的移动终端数据防泄露系统。实验结果显示，本系统具备完善的数据泄露能力，并且相比于传统移动终端数据防泄露系统在性能和

安全性方面都有提高。

后续工作需要在移动终端虚拟远程桌面技术的开发上，进一步研究提高本地位图更新事件的速度以及减轻 RDP 通信负担的问题来进一步提高此模块的稳定性。

参考文献：

[1] GARTNER. Mobile opplications & enterprise mobility management[EB/OL]. http://www.gartner.com/technology/topics/mobile.jsp.

[2] 张玉清, 王凯, 杨欢, 等. Android 安全综述[J]. 计算机研究与发展, 2014, 51(7): 1385-1396.
ZHANG Y Q, WANG K, YANG H, et al. Survey of Android OS security[J]. Journal of Computer Research and Development, 2014, 51(7): 1385-1396.

[3] PISTOIA M, TRIPP O, CENTONZE P, et al. Labyrinth: visually configurable data-leakage detection in mobile applications[C]//2015 16th IEEE International Conference on Mobile Data Management. 2015, 1: 279-286.

[4] CHOW R, JAKOBSSON M, MASUOKA R, et al. Authentication in the clouds: a framework and its application to mobile users[C]// Proceedings of The 2010 ACM Workshop on Cloud Computing Security Workshop. 2010: 1-6.

[5] XIE Y, DING W, WANG Y. A more extensible transparent encrypt file system based on filter driver[J]. Journal of Communications, 2016, 11(4): 383-387.

[6] 韩心慧, 丁怡婧, 王东祺, 等. Android 恶意广告威胁分析与检测技术[J]. 清华大学学报(自然科学版), 2016, 65(5): 468-477.
HAN X H, DING Y J, WANG D Q, et al. Android malicious AD threat analysis and detection techniques[J]. Journal of Tsinghua University (Science and Technology), 2016, 65(5): 468-477.

[7] LI Y, FANG J, LIU C, et al. Study on the application of Dalvik injection technique for the detection of malicious programs in Android[C]// 2015 5th International Conference on Electronics Information and Emergency Communication (ICEIEC). 2015: 309-312.

[8] YANG T, CUI H, NIU S, et al. An analysis on sensitive data passive leakage in Android applications[C]//2015 IEEE 16th International Conference on Communication Technology (ICCT). 2015: 125-131.

[9] MCDANIEL P, JAEGER T, LA PORTA T F, et al. Security and science of agility[C]//The First ACM Workshop on Moving Target Defense. 2014: 13-19.

[10] ASNAR Y, HENDRADJAYA B. Confidentiality and privacy information security risk assessment for Android-based mobile devices[C]//2015 International Conference on Data and Software Engineering (ICoDSE). 2015: 1-6.

[11] CAM N T, VAN HAU P, NGUYEN T. Android security analysis based on inter-application relationships[C]//Information Science and Applications (ICISA) 2016. 2016: 689-700.

[12] JIA P, HE X, LIU L, et al. A framework for privacy information protection on Android[C]// 2015 International Conference on Computing, Networking and Communications (ICNC). 2015: 1127-1131.

[13] KATZ G, ELOVICI Y, SHAPIRA B. CoBAn: A context based model for data leakage prevention[J]. Information Sciences, 2014, 262: 137-158.

[14] GAJRANI J, SARSWAT J, TRIPATHI M, et al. A robust dynamic analysis system preventing SandBox detection by Android malware[C]//8th International Conference on Security of Information and Networks. 2015: 290-295.

[15] SALMAN A, ELHAJJ I H, CHEHAB A, et al. Mobile malware exposed[C]//2014 IEEE/ACS 11th International Conference on Computer Systems and Applications (AICCSA). 2014: 253-258.

[16] HUANG Z, JIANG H, ZHOU K. An improved decoding algorithm for generalized RDP codes[J]. IEEE Communications Letters, 2016, 20(4): 632-635.

[17] 文伟平, 梅瑞, 宁戈, 等. Android 恶意软件检测技术分析和应用研究[J]. 通信学报, 2014, 35(8): 78-85.
WEN W P, MEI R, NING G, et al. Malware detection technology analysis and applied research of Android platform[J]. Journal on Communications, 2014, 35(8): 78-85.

[18] MENG Y X, DONG J Y, YIN Y H, et al. Transparent encryption technique for Word documents based on USB Key in manufacturing system[C]//Applied Mechanics and Materials. 2013: 323-326.

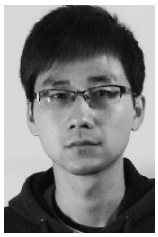
[19] PARK J H, KIM D, PARK J S, et al. An enhanced security framework for reliable Android operating system[J]. Security and Communication Networks, 2013, 9(6): 528-534.

[20] JOVESKI B, MITREA M, GANJI R R. MPEG-4 solutions for virtualizing RDP-based applications[C]//IS&T/SPIE Electronic Imaging, International Society for Optics and Photonics. 2014.

[21] 刘洋, 邵旭东, 潘程达, 等. 立体安全防御系统 TDSD—Droid 的实现[J]. 计算机科学, 2013, 40(11A): 228-234.
LIU Y, SHAO X D, PAN C D, et al. Implementation of three-dimensional security defense system[J]. Computer Science, 2013, 40(11A): 228-234.

[22] XIAO H Y, YU B S, FEI C. Android's sensitive data leakage detection based on API monitoring[C]// International Conference on Cyberspace Technology (CCT 2014). 2014: 1-4.

作者简介：



黄振涛（1991-），男，江苏淮安人，南京理工大学硕士生，主要研究方向为信息安全、移动互联网安全等。

何暖（1982-），男，江苏扬州人，中国船舶工业综合技术经济研究院高级工程师，主要研究方向为电子对抗、人因工程、信息安全等。

付安民（1981-），男，湖北通城人，博士，南京理工大学副教授，主要研究方向为无线网络安全、云计算/大数据安全、移动互联网安全等。

况博裕（1994-），男，四川绵阳人，南京理工大学硕士生，主要研究方向为信息安全、移动互联网安全等。

张光华（1979-），男，河北深州人，博士，河北科技大学副教授，主要研究方向为网络与信息安全。