



云端协同的智能终端数据加密技术

刘国荣, 刘东鑫, 汪来富, 沈军, 金华敏

(中国电信股份有限公司广州研究院, 广东 广州 510630)

摘要: 不断提升的计算能力和存储能力使得智能终端已逐步成为最重要的个人信息助理, 终端的数据安全也成为用户的关注焦点。对重要的数据进行加密是保障安全的基础, 但当前主要的终端或云端加密存储方案都存在技术成本高等一系列弊端。因此, 提出了云端协同运算的数据加密技术方案, 将数据加密运算过程、密钥信息分别在云端、终端运算和存储, 提升了密钥及数据文件的安全性。

关键词: 云端协同; 智能终端; 数据加密

中图分类号: TP309.7

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2018101

Data encryption technology based on cloud and terminal collaboration

LIU Guorong, LIU Dongxin, WANG Laifu, SHEN Jun, JIN Huamin

Guangzhou Research Institute of China Telecom Co., Ltd., Guangzhou 510630, China

Abstract: With the fast increasing computing and storage capability, the intelligent terminal has gradually become the most important personal information assistant, and the data security of the terminal has turned to be essential for customers. Data encryption is a basic component of security assurance, but currently the mainstream technology scheme has a series of drawbacks, such as high technical cost. Therefore, a data encryption scheme based on cloud and terminal collaboration was proposed to promote the security of keys and data files.

Key words: cloud and terminal collaboration, intelligence terminal, data encryption

1 引言

手机、平板电脑等智能终端计算存储能力的提升和应用的丰富, 使智能终端日益成为个人信息助理、日常生活不可或缺的一部分。机身

存储及扩展存储容量已经普遍提升到几十 GB、上百 GB, 为用户存储大量音视频等大文件提供了可能。由于随身携带的便利性, 智能终端也成为了人们便携的移动存储设备, 用于存储包括照片、音频、视频等私人信息, 甚至工作文

收稿日期: 2017-11-19; 修回日期: 2018-01-30

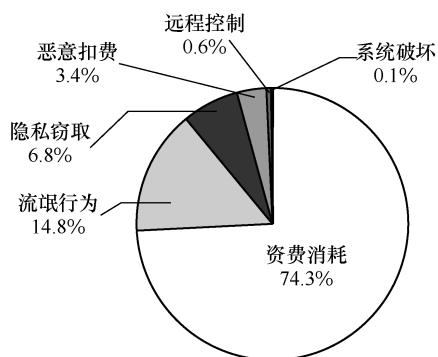
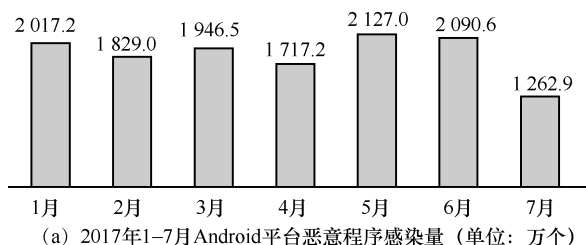
通信作者: 刘国荣, liugr@gsta.com

基金项目: 国家高技术研究发展计划(“863”计划)基金资助项目(No.2015AA017205)

Foundation Item: The National High Technology Research and Development Program of China (863 Program) (No. 2015AA017205)

件等重要信息。

另一方面,智能终端面临的安全形势也日益严峻。据统计报告显示,2017年360互联网安全中心每月监测到移动端用户感染恶意程序超过千万人次,恶意程序已进入平稳高发期,2017年1-7月Android平台恶意程序状况如图1所示,其中,隐私窃取是其中一种主要的恶意行为^[1]。



(b) 2017年1-7月Android平台新增恶意程序类型分布

图1 Android平台恶意程序状况

随着携带自己的设备办公 (bring your own device, BYOD) 等企业移动办公方式的流行,智能终端中高价值的企业数据将更吸引黑色产业的注意,未来企业数据将成为恶意软件攻击的重要目标。同时,伴随着移动平台的大力发展,APT攻击将向全平台化方向发展,成为今后的主要趋势^[2]。智能终端的数据安全,将成为影响其安全性的关键因素。

加密技术是保障数据安全的基础,本文将通过分析智能终端数据加密技术现状,针对其弊端,提出云端协同运算的加密技术、密钥规则与密钥元素分离的数据加密方案两种云端协同的数据加密技术方案,提升智能终端密钥及数据文

件的安全性。

2 智能终端数据加密安全分析

2.1 数据加密技术简述

根据密钥类型的不同,可以将现代密码技术分为两类:对称加密算法(私钥密码体系)和非对称加密算法(公钥密码体系)。

对称加密算法的特点是文件加密和解密使用相同的密钥,即加密密钥也可以用作解密密钥,具有加/解密速度快、效率高的优点,通常需要加密大量数据时使用,但对称加密算法的密钥管理比较困难,数据加/解密需要多方参与或环节较多时,密钥存在较大的泄露风险。

与对称加密算法不同,非对称加密算法需要一对密钥:公钥和私钥。如果用公钥对数据进行加密,只有用对应的私钥才能解密;反之亦然。非对称加密算法的保密性比较好,由于加/解密采用不同密钥,在多方/参与环节较多时,向其他参与方/环节提供公钥,用户保管私钥即可,非对称加密的缺点是花费时间长、速度慢,并不适合于对文件加密,通常用于少量数据加密,如对称密钥分发、数字签名等。

针对大文件数据的加密,主要采用对称加密算法进行保障,密文存储以及密钥管理的安全性是数据安全的关键。

2.2 智能终端数据加密风险

智能终端数据加密,主要采用终端加密存储或云端加密存储两类方案。

云存储是随着云计算技术发展起来的一种新兴的网络存储技术,通过集群应用、网络技术或分布式文件系统等功能,将网络中大量各种不同类型的存储设备通过应用软件集合起来协同工作,共同对外提供数据存储和业务访问服务。云存储具有在任何时间、任何地方,透过任何可连网的装置连接到云上方便地存取数据的便利、负载均衡、故障冗余功能,保障数据存储的可靠性。



云端加密，是将终端数据上传至云端加密并存储，密钥由云端管理，云服务商较强的安全防护措施可降低密钥失窃的风险，但内部管理员可获取该密钥并解密数据，用户可能对服务商存在疑虑。同时，对于大数据文件的上传、下载，需要消耗大量流量，不少用户仅在 Wi-Fi 环境下才能进行操作，限制了使用的自由。

终端加密的数据则由终端直接加/解密、密文存储在终端或上传至云存储服务器，密钥则由用户输入或存储于终端数据库文件，密钥存在较大的泄露、遗忘等丢失风险从而危及数据安全性。

可见，云端加密存储和终端加密存储都存在一定的弊端，将两者结合，密文或者密钥信息一部分存储在终端、另一部分存储在云端，则可充分利用两者的优势，解决相应的问题。

3 云端协同的数据加密技术方案

3.1 云端协同运算的加密技术方案

防止智能终端内密钥存储、运算过程中密钥窃取风险的主要思路是密钥的存储、运算过程与普通运行环境的隔离，终端虚拟化、独立硬件模块，都可以实现独立的安全运行环境。此外，由另一个智能设备协同实现，也可以达到相同的效果，最典型的是采用云计算技术实现数据加/解密，即将智能终端的文件通过网络传输到云平台完成数据的加/解密运算过程。

对智能终端而言，独立硬件模块、云平台都是代理服务模式，需要将待加/解密文件发送给对方，并返回处理结果，期间需要大量的数据文件传输，将给终端带来大流量传输压力，独立硬件模块通常处理能力较弱，还可能成为性能瓶颈，同时，文件传输过程需采取必要的安全措施进行防护，因此，并不适合大数据文件的处理。云端协同的数据加密技术方案，则可以较小的代价平衡上述难题，保障数据安全。

云端协同的数据加密技术方案，是将智能终端中待加密的数据文件切分成若干数据块，抽取其中的部分数据块传输到云端加密，其余部分由智能终端直接加密，两部分加密结果可以统一存储，也可以在终端和云端分离存储。该方案中，云端协同同样适用于智能终端与独立硬件模块的协同，这种情况下，密文统一存储于终端。方案的处理过程如图 2 所示。

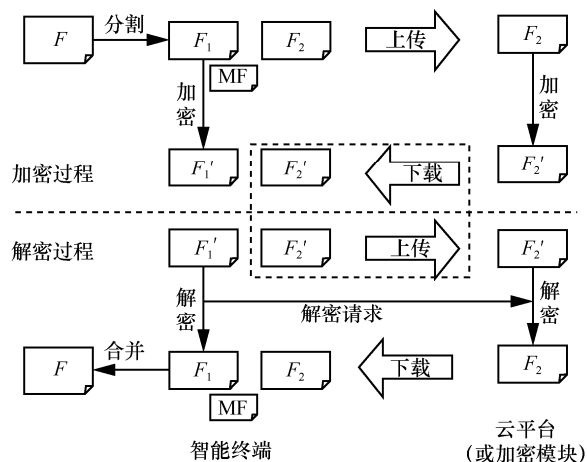


图2 云端协同的数据加/解密过程

处理过程的主要步骤如下。

步骤 1 文件 F 被分割成若干数据块，并重组组成数据文件 F_1 、 F_2 和元数据文件 (MF)；其中，MF 包含数据块分割、文件 F_1/F_2 的组成、文件校验码等信息。

分割重组示例如图 3 所示。

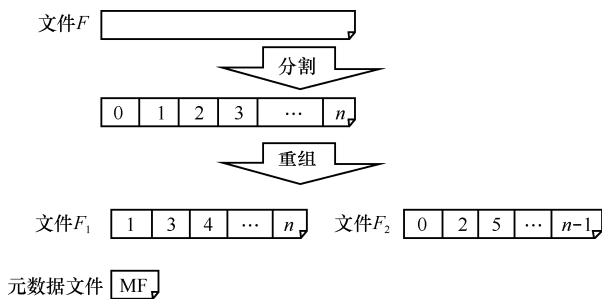


图3 文件分割重组示例

(1) 文件 F 被分割为数据块 $0 \sim n$ ，其中，数据块 0 为原文件头；

(2) 数据块 1、3、4、 $\dots$ 、 n 重组数据文件 F_1 ；数据块 0、2、5、 $\dots$ 、 $n-1$ 组成数据文件 F_2 ；同时生成元数据文件 (MF)，记录分割、重组信息。

步骤 2 文件 F_1 和 MF 由智能终端直接加密，生成密文 F_1' 并存储，密钥由智能终端存储。

步骤 3 文件 F_2 经网络上传至云平台，由平台生成随机密钥加密，密钥存储于云平台，密文 F_2' 可根据需要存储于云平台，或者下载至智能终端存储。

解密过程与上述过程相反，终端先解密文件 F_1' ，得到 F_1 、MF 文件明文，然后请求云平台解密 F_2' 文件，得到 F_2 文件明文，根据元数据文件 MF 信息，对 F_1 、 F_2 重组文件 F 并校验，完成解密过程。

云端协同的数据加密方案，将文件的加密过程分解，计算过程由两个实体分别完成，使用不同的加密密钥甚至不同的加密算法，计算过程、密文都具有更高的安全性，任一部分密钥、密文的泄露都不至于影响文件的安全性；同时，可根据文件的大小、数据密集程度、各实体的计算/存储能力等因素综合考虑数据文件的分割方式，在安全性和数据传输能力、计算能力之间取得平衡。

方案适用于采用网络侧云平台或终端内独立加密模块等多种场合，特别是智能终端大文件的加/解密。

3.2 密钥规则与密钥元素分离的数据加密方案

传统的数据加/解密中，数据明文、加密密钥直接经加密算法运算后，得到密文，解密过程相

反。密钥规则与密钥元素分离的数据加密方案，则将密钥的生成分解为密钥规则和密钥元素，两部分分别存储于云端和终端，任一部分的泄露，都不会导致密钥的泄露。

终端数据加密运算前，产生密钥规则，并由密钥规则作用于密钥元素产生密钥，数据加密后，将密钥规则采用终端标识或用户口令等加密，并上传至云存储服务器存储、管理。其中，密钥规则是指密钥产生的规则、方法描述及文件加解密的元数据。密钥元素，是指产生密钥的素材，可以是存储的文本、图像、视频等各类数据文件，也可以是终端 ID、IMSI 等终端、网络配置信息甚至是网络服务器上的文件。

数据加/解密过程如图 4 所示。

数据加密过程如下：

- 密钥元素 E 依据密钥规则 R ，生成密钥 K ；
- 明文 F 、密钥 K 依据密钥规则 R 进行加密运算，产生密文 F' ；
- 密钥规则 R 采用用户口令或终端标识等密钥加密，形成密钥规则密文 R' ；
- 密钥规则密文 R' 上传至云存储服务器存储、管理；数据密文 F' 可根据需要存储于终端，也可存储于云端。

数据解密过程与上述过程相反：

- 从云存储服务器下载密钥规则密文 R' ；如果数据密文 F' 存储于云端，同时下载该密文；
- 密钥规则密文 R' 使用用户口令或终端标识解密，得到密钥规则明文 R ；

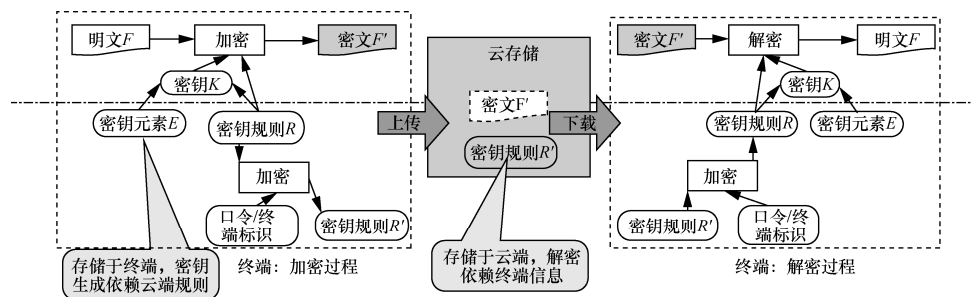


图 4 密钥规则与密钥元素分离的数据加/解密流程



表 1 改进方案与传统方案比较

方案	说明	特点
传统方案	密钥直接存储于终端（或云平台）	处理过程简单，但密钥易失窃
本文方案	• 密钥由密钥规则作用于密钥元素产生； • 密钥规则与密钥元素分离，分别由终端和云平台管理	• 密钥元素样本空间非常大、规则可任意设计，密钥产生具有很强的随机性； • 密钥元素与密钥规则分离存储，难以同时取得； • 密文无论存储于云平台或终端，都具有很高的安全性

- 密钥元素 E 依据密钥规则 R 生成密钥 K ；
- 密文 F' 、密钥 K 依据密钥规则 R 进行解密运算，得到明文 F 。

与传统方案相比，本方案的特点见表 1。

本文方案中，智能终端的数据加密密钥由密钥规则作用于密钥元素产生，且密钥元素和密钥规则分别由云平台和终端进行管理，密钥的产生和使用依赖对端信息，任一部分密钥信息的失窃，都难以恢复密钥，从而提升数据文件安全性。

4 结束语

随着智能终端应用的丰富化，特别是支付、企业移动办公等的流行，智能终端存储、处理高价值数据的应用日益增多，数据安全性愈发重要，保障其安全，需要从终端运行环境安全、应用安全、数据安全防护等多个层面上实施。云端协同是解决智能终端安全问题的一个重要方向，本文提出的云端协同的智能终端数据加密技术，提供了密钥管理及数据安全保障的一种可行方案。

参考文献：

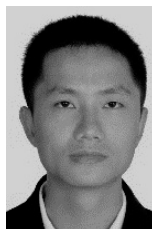
- [1] 中国泰尔实验室、360 互联网安全中心. 2017 中国手机安全生态报告[EB/OL]. (2017-09-28)[2017-10-20]. <http://zt.360.cn/1101061855.php?dtid=1101061451&did=210412109>. China Telecommunication Technology Labs, 360 Internet. 2017 Ecological report on the safety of mobile phone in China[EB/OL]. Security Center (2017-09-28)[2017-10-20].<http://zt.360.cn/1101061855.php?dtid=1101061451&did=210412109>.
- [2] 360 互联网安全中心. 2016 年 Android 恶意软件专题报告[EB/OL]. (2017-02-27)[2017-10-28]. <http://zt.360.cn/1101061855.php?dtid=1101061451&did=490301065>.

360 Internet Security Center. 2016 Android malware report[EB/OL]. (2017-02-27)[2017-10-28]. <http://zt.360.cn/1101061855.php?dtid=1101061451&did=490301065>.

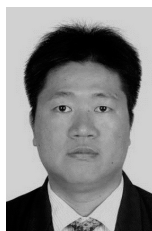
[作者简介]



刘国荣（1978-），男，中国电信股份有限公司广州研究院高级工程师，主要研究方向为移动互联网安全、云计算安全。



刘东鑫（1985-），男，中国电信股份有限公司广州研究院工程师，曾获得 CCIE、CISSP 和 CISA 等认证。主要研究方向为网络与信息安全、大数据安全。



汪来富（1976-），男，中国电信股份有限公司广州研究院高级工程师，主要研究方向为 IP 网、云计算、大数据安全、网络安全。

沈军（1976-），女，中国电信股份有限公司广州研究院高级工程师，主要研究方向为云计算安全、移动互联网安全及 SDN/NFV 安全等。

金华敏（1972-），男，中国电信股份有限公司广州研究院高级工程师，主要研究方向为 IP 网、云计算、大数据安全、网络安全。