



# 基于证书链验证机制的智能终端安卓系统安全加固方案

江家仁<sup>1,2</sup>, 姜臻<sup>3</sup>, 王渭清<sup>4</sup>

(1. 移动互联网系统与应用安全国家工程实验室, 上海 201315;

2. 中国电信股份有限公司上海研究院, 上海 200122;

3. 中国电信股份有限公司上海分公司, 上海 200120; 4. 中国电信集团公司, 北京 100033)

**摘要:** 在全球信息化的普及和移动互联网蓬勃发展的背景下, 安卓系统的安全加固作为移动互联网和智能终端的新兴领域最为核心的技术之一, 需要结合其所表现出来的安全问题进行深入的分析与研究。结合了证书链机制, 以完整性验证为核心的安全架构, 能够达到最大限度保护智能终端安全的目标。

**关键词:** 智能终端; 安卓安全; 安全加固

**中图分类号:** TP309

**文献标识码:** A

**doi:** 10.11959/j.issn.1000-0801.2017050

## Android security reinforcing scheme of intelligent terminal based on certificate chain authentication mechanism

JIANG Jiaren<sup>1,2</sup>, JIANG Liu<sup>3</sup>, WANG Weiqing<sup>4</sup>

(1. National Engineering Laboratory for Mobile Internet System and Application Security, Shanghai 201315, China

2. Shanghai Research Institute of China Telecom Co., Ltd., Shanghai 200122, China

3. Shanghai Branch of China Telecom Co., Ltd., Shanghai 200120, China

4. China Telecom Corporation, Beijing 100033, China)

**Abstract:** With the prosperous development of information technologies and mobile internet popularity of information-based on a global basis, it is necessary to analyze and research the security problems for Android, which is one of the most important technologies in the emerging field of mobile internet and intelligent terminals. The certificate chain authentication mechanism played a critical role as protecting the core of the terminals against some intrusion attacks in the security phases.

**Key words:** intelligent terminal, Android security, security reinforcing

## 1 引言

智能终端搭载的安卓系统是基于 Linux 开放性内核的操作系统, 并且安卓系统本身具有极大限度的自由和开放性; 由于采用了软件堆层 (software stack) 的架构, 有了比较好的扩展性。所以根据安卓系统广大的市场前景和发展的

可持续性、平台的开放性和优良的扩展性, 以安卓系统为基础建立的移动操作系统已经成为智能终端系统核心的组成部分, 并且受到了开放手机联盟 (Open Handset Alliance) 的大力支持, 使整个系统不断加速发展。IDC 预计, 2019 年安卓市场份额将达到 82.6%, 成为全球市场份额最大的智能手机操作系统<sup>[1]</sup>。

随着智能终端的发展,越来越多的人开始使用并依赖于通过搭载安卓智能操作系统的设备来处理日常生活与工作事务,结合各自应用场景下的安卓应用也因其系统的开放性和碎片化,导致其安全性问题凸显。因此,对安卓系统的安全加固作为移动互联网和移动智能终端的新兴领域最为核心的技术之一,需要结合其所表现出来的安全问题进行深入分析与研究。

本文基于证书链验证机制,结合智能终端所遇到的安全风险,通过对应用程序安全执行技术和数据安全存储技术的研究,提出以完整性验证为核心的安全架构,从而提升智能终端系统的综合安全防护能力。

## 2 安卓系统安全现状

基于安卓系统的智能终端较为广泛,如华为、三星等知名品牌,在对安全性要求较高的应用场景,如移动政务办公、移动商务办公等方面,无一例外地采用通用终端和系统结合行业专用软件工具而形成的专业办公终端,政企行业用户使用这样的智能终端处理事务,可能会时刻处于安全风险中。这些风险将来源于如下两个方面。

- 安卓系统的安全性存在一定的结构性问题,并对用户造成严重的安全隐患。安卓系统可被替换,从而不能保证系统的完整性和可信任性;而安卓系统内核也存在大量安全漏洞,攻击者可以利用这些漏洞窃取用户数据,有些漏洞甚至可以使已安装的安全监控软件关闭,给攻击者长驱直入的机会;攻击者利用信息同步获取用户的隐私信息和位置信息。
- 在智能终端安装安全软件和其他专业软件过程中,系统容易受到恶意软件或仿冒软件的入侵,导致攻击者利用仿冒版本获取信息;在网络传输数据过程中,攻击者利用网络漏洞,监听空口信令窃取智能终端的国际移动用户识别码(international mobile subscriber identification number, IMSI),甚至篡改数据,从而发布伪造信息;利用网络对智能终端进行 IP 地址攻击,导致终端无法使用数据业务甚至不能正常工作。无论是安卓系统本身还是安卓终端使用模式,都存在大量风险,主要包括信息泄露、系统篡改、数据篡改、通信骚扰、漏洞利用等,如图 1 所示。

不难发现,智能终端的安全风险主要体现在信息泄露、系统篡改、数据篡改、伪造信息、通信骚扰和漏洞利用等方面,如何判断系统本身的可信性和可靠性是解决智能

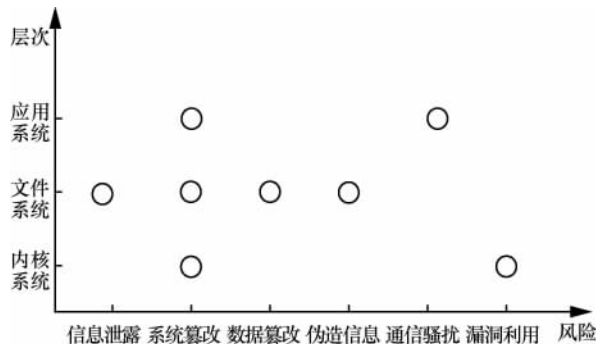


图 1 智能终端面临的安全风险

终端安全防护问题的关键<sup>[2]</sup>。为此,本文提出了一种基于证书链验证机制的智能终端安卓系统安全加固方案。

## 3 安全加固方案

本文方案针对智能终端安全加固关键技术的研究是基于 Google 公司和开放手机联盟领导及开发的开源移动智能操作系统——安卓系统,以国内 GB/T 20272-2006、GB/T 30284-2013 等相关安全标准为依据,研究以基于证书链的完整性验证为核心的安全架构,旨在达到最大限度保护智能终端安全的目标。

本文方案主要针对安卓智能终端进行安全防护,包括应用程序安全执行、安全存储等功能模块领域技术进行研究,制定安卓系统加固核心模块关键技术方案,为行业用户提供终端安全服务,并为各类移动互联网业务应用的安全性提升奠定基础。

### 3.1 系统完整性验证

系统完整性验证是整个系统安全框架的基础,以 CPU 内置根证书为信任链依据对内核引导程序完整性校验,引导程序内嵌二级证书对内核、文件系统、安卓应用系统进行完整性校验,确保终端操作系统的不可篡改和完整性。

证书链验证机制以内置根证书为信任依据,采用 SHA-1 签名和 RSA 加密算法对内核引导程序完整性校验,引导程序内嵌二级证书对内核、文件系统、安卓应用系统进行完整性校验,确保终端操作系统的不可篡改和完整性,如图 2 所示。对于证书链的管理与存储,其所有证书和签名均存储在保密的存储区域内。

将系统镜像(image)通过数字证书签名,并将签名结果和公钥证书保存在 CPU 的启动代码中,如图 3 所示,再用芯片厂商的数字证书对 CPU 的启动代码签名,最后将签名结果和该数字证书所对应的公钥证书保存在不可重写模块中,该不可重写模块为整个系统完整性验证的锚点,即安全的起点。

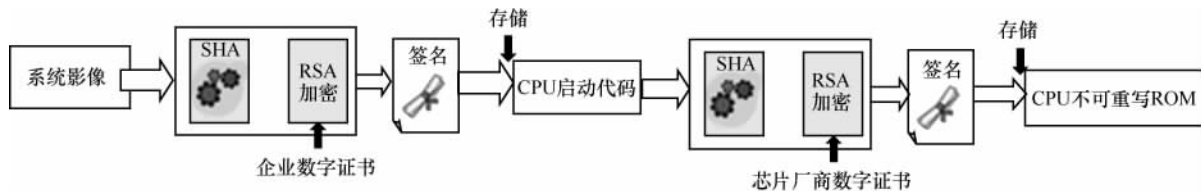


图2 证书链验证机制

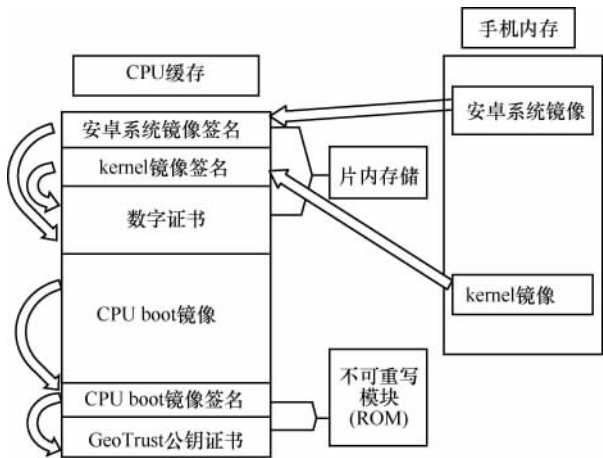


图3 证书链存储区结构

证书链存储结构为两级存储:CPU 片内存储和不可重写模块。不可重写模块存放根证书和 CPU boot, 放置在 CPU 内置的一个 512 byte 的一次性烧录逻辑电路中,只能由片内加载程序代码读取,不能被更换,也不能被其他应用代码读取,将是这个系统完整性的锚点。其他加载镜像和系统镜像的签名和证书放在 CPU 片内存储区。

### 3.2 密钥体系

本文方案采用两种算法,一个是 SHA-1,用于产生摘要;另一个是 RSA-1024,结合证书的密钥对摘要加密,即签名。由于芯片商指定证书发放者为 GeoTrust,故对 CPU 的 boot 签名所使用的证书和 USB token 均由 GeoTrust 提供。美国 GeoTrust 公司是全球第二大数字证书颁发机构(CA),也是身份认证和信任认证领域的领导者,该公司各种先进的技术使得任何大小的机构和公司都能安全、低成本地部署 SSL 数字证书和实现各种身份认证,从而确保电子商务交易的安全。全球 150 多个国家有超过 10 万个用户在使用 GeoTrust 的产品来进行安全的电子交易和确认并保护

网上真实身份,为全球用户的电子商务保驾护航。故 GeoTrust 是可信任的。本文方案系统的证书体系见表 1。

### 3.3 应用程序安全执行

用于对应用程序进行安全认证,只有通过安全检测并授权安装的应用才能在系统上使用。首先应用供应商必须将应用发送至安全检测机构对应用的安全性进行检测。如果通过检测,使用安全检测机构的证书对应用进行签名。应用程序安全执行采取的技术是提供定制的应用安装器和应用签名过滤器,通过与存储在系统安全存储区中的证书链进行度量,对于没有签名或者签名不是专用签名的应用程序不给予安全认证,认为非法,并禁止安装该应用。验证流程如图 4 所示。

由于在固化封装前,会对系统镜像进行签名,并将签名结果和公钥存放在安全存储空间。因此,开机时对内存上的系统进行 SHA-1 摘要计算,获取摘要和对应存储区域中保存的签名,使用公钥对签名做 RSA-1024 计算获取原始摘要。将两个摘要进行比较,如果符合,则验证通过授权允许安装,否则拒绝安装。

### 3.4 安全存储

安全存储是用来对用户关心的数据进行加密存储,保护用户的隐私数据和敏感文件。如图 5 所示,系统采用堆叠式企业级文件加密系统(enterprise cryptographic filesystem, eCryptFS)来对文件系统进行加密,该文件系统基于 openPnP 设计,具有企业级安全性,可以对文件夹/文件名/文件数据加密,eCryptFS 插在虚拟文件系统层(virtual file system, VFS)和下层物理文件系统之间,充当一个“过滤器”的角色,对应用的读写需求进行转换。

用户应用程序对加密文件的写请求,经系统调用层到达 VFS 层,VFS 转给 eCryptfs 文件系统组件处理,处理完

表 1 证书类型说明

| 证书名   | 发放者      | key 存储位置      |          | 描述                         |
|-------|----------|---------------|----------|----------------------------|
|       |          | 公钥            | 私钥       |                            |
| 根 CA  | GeoTrust | 放置在 CPU 内置芯片中 | GeoTrust | 用于身份 CA,芯片商认证 CA 和代理商的认证证书 |
| 身份 CA | GeoTrust | 管理系统服务器上      | GeoTrust | 用于管理系统授权芯片商或代理商            |
| 公钥    | 电信运营商    | 中级证书          | 电信运营商    |                            |

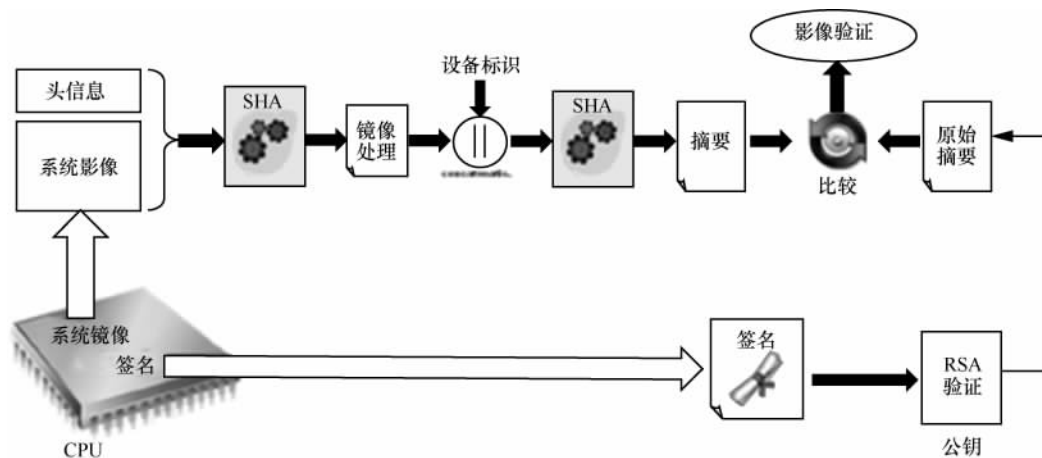


图4 验证流程

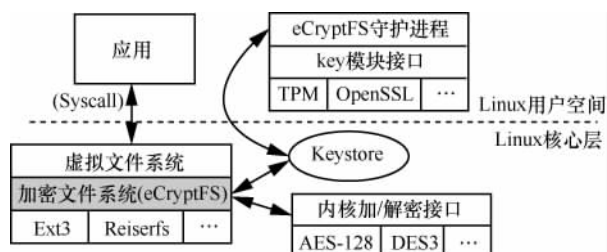


图5 安全存储系统结构

毕后,再转给下层物理文件系统;读请求(包括打开文件)的流程则相反。

Keystore 和用户 eCryptfs-Daemon 进程负责协同密钥管理,当 eCryptfs 层读取文件时,通过下层文件系统读取该文件的头部元数据,交予 Keystore 模块进行加密后的 EFEK 的解密。依据 RFC2440-OpenPGP 规范要求,允许许多对象或角色共享加密文件,头部元数据中可以有一系列 EFEK。OpenPGP 格式被 eCryptfs 用于存放加密文件,由 ecryptfs\_auth\_tok 结构表示,EFEK 和相应的公钥算法/口令的描述构成一个鉴别标识符<sup>[4]</sup>。通过信任链已经登记的鉴别标识符,采用证书区别不同对象或角色的加密区域,从而保证不同对象或角色间不能查看和获取加密文件。

## 4 结束语

较之安卓原生态系统存在的信息泄露、系统篡改、通信骚扰、漏洞利用等问题,安卓加固方案通过对安卓系统内核进行安全增强与加固是智能终端安全防护的核心内容,采用基于证书链验证机制方案能够有效解决系统的完整性和应用可信任性问题,为用户提供终端安全服务,并为各类移动互联网业务安全性提升奠定基础,同时为我国智能终端定制开发、安全手机研发等领域提

供一种安全加固方案参考。

## 参考文献:

- [1] IDC. 全球智能手机发展预测报告 2015-2019[R]. [S.l.:s.n.], 2015.  
IDC. Worldwide business use smartphone forecast 2015-2019[R]. [S.l.:s.n.], 2015.
- [2] 李兴新. 移动互联网时代的智能终端安全[M]. 北京: 人民邮电出版社, 2016.  
Li X X. Intelligent terminal security in mobile internet [M]. Beijing: Posts & Telecom Press, 2016.
- [3] 傅慧明. 一种基于双向证书信任链的密钥管理方案[J]. 计算机安全, 2012, 32(2):8-12.  
FU H M. A key management scheme based on bidirectional certificate chain [J]. Computer Security, 2012, 32(2): 8-12.
- [4] IETF. OpenPGP message format: RFC 2440[S]. 1998.

## [作者简介]



江家仁(1981-),男,移动互联网系统与应用安全国家工程实验室、中国电信股份有限公司上海研究院高级工程师,主要从事移动互联网安全技术及安全产品攻防技术方面的研究工作。

姜臻(1984-),男,中国电信股份有限公司上海分公司总工程师室综合设施技术主管,主要从事通信基础设施及网络、信息安全技术方面的研究工作。

王渭清(1980-),男,中国电信集团公司工程师,主要研究方向为信息安全管理、大数据安全。