



一种安全的智能机顶盒实现方案

胡冰松,黄小桑

(中国电信股份有限公司上海研究院 中国电信 IPTV 实验室 上海 200122)

摘要:基于 Android 的智能机顶盒设备由于系统开放、跨平台性好而受到业界认可,但软件的开放性带来了终端软件的安全问题。本文从智能机顶盒芯片层面提出了一种解决智能机顶盒设备终端安全性问题的方案,利用 OTP 数据、安全引导等功能,建立起智能机顶盒系统软件安全链,以保证终端软件系统的安全性,并通过使用基于 CPU 的终端身份验证,将系统可信域扩展到用户侧设备,确保了业务运行稳定可靠。

关键词:智能电视终端;OTP;安全引导;软件安全;Android

doi: 10.3969/j.issn.1000-0801.2013.04.007

An Implement Scheme for Secure STB

Hu Bingsong, Huang Xiaosang

(IPTV Lab of China Telecom Corporation, Shanghai Research Institute of China Telecom Co., Ltd., Shanghai 200012, China)

Abstract: Android set-top box(STB) is well developed of its open and cross platform and the rich application. But security is one of the key issues of open systems. A software security scheme based on CPU for Android STB was proposed. By using OTP data and secure booting, the secure chain was set up to ensure safety of the software system, and the CPU based terminal authentication extends the secure domain to the CPE, provided the stability of the services.

Key words: smart TV terminal, OTP, secure booting, software security, Android

1 引言

智能机顶盒功能丰富、业务开发方便,已经成为传统运营商以及新兴 OTT(over the top)运营商的首选设备。目前这类设备基本采用 Android 操作系统。Android 智能机顶盒终端软件系统的开放性在引发终端变革的同时也带来了软件安全隐患,非法刷机、安装非法应用软件、更改系统安全相关设置及终端配置等操作,使得业务安全性受到威胁。因此,智能机顶盒终端设备亟需在安全方面多加考虑,以满足开放环境下业务与终端的安全性。本文就上述问题展开探讨,提出了一种适合电信运营的终端软件安全方案,该方案从芯片层面为智能机顶盒设备提供软件安全保

障,对于提高基于智能机顶盒的业务运营能力具有重要意义。

2 智能机顶盒终端安全方案

智能机顶盒作为用户侧设备,其安全性直接关乎业务运营与用户应用安全。由于采用 Android 智能操作系统,如果不对软件进行有效管理,被非法程序(如木马等)入侵后,用户的业务数据(用户名、密码、平台地址身份信息等)面临高风险,用户与运营商都可能因此面临巨额损失。为了保护用户与运营商,需要从软件保护、终端认证、应用安装 3 个方面保证机顶盒终端安全。对于应用安装来说,可以对软件安装进行控制,只允许安装来自运营商应用商城的软件,由运营商对发布的应用进行审核,以确保安全。但



应用安装的安全性取决于终端系统软件的安全性,可以通过采用基于芯片的安全机制确保终端系统的安全以及对终端进行合法性验证,使业务系统的安全域覆盖包括平台与终端的完整范围。

2.1 基于 Android 的智能机顶盒软件系统

智能机顶盒的软件系统包含引导区、恢复区、内核区、系统数据区、用户数据区 5 个部分,如图 1 所示。



图 1 智能机顶盒软件分区

其中,引导区的功能是对系统基本硬件(如存储器等)进行初始化,使得后续执行的软件具备基本的运行环境。引导程序完成系统初始化后,根据系统的状态执行恢复区程序或内核程序。恢复程序的主要作用是软件升级维护。当系统需要升级时,恢复程序被引导程序载入内存并执行,完成系统升级;当系统需要恢复默认出厂状态时,也是由恢复程序根据操作维护指令完成恢复出厂状态。当引导状态为正常启动时,引导程序将内核载入内存,并将控制权交给内核,由内核完成正常引导,包括加载 RAM disk 与 flash 文件系统、启动 Android 系统等。系统数据区主要包括 Android 系统软件以及 Android 核心应用;用户数据区用于存放用户选装软件以及用户软件所需的运行数据。

一般来说,系统软件的升级过程由终端用户下载包含内核区域系统数据区的系统镜像 image,启动恢复程序将内核区与系统数据区进行重新烧写。

由于 Android 系统的开放性,会有爱好者针对不同的硬件平台开发不同功能的 image 供用户选择升级。但这种情况往往会被不怀好意者利用,使得终端用户或运营商遭受损失。

另外,终端核心数据(如用户业务认证信息、平台数据信息)如果存放在 flash 区域,则可以通过软件方便地获取或修改,这些数据的泄露会使运营商面临终端失控,使合法用户的业务被非法使用,业务安全性无法得到保障。

因此,对于智能机顶盒终端,首先要确保终端软件系统的安全,杜绝软件非法升级,并保护终端核心数据不被

泄露。

2.2 用于智能机顶盒的安全芯片架构

从上述系统结构来看,如果要确保系统不被恶意修改,必须具备更底层的安全机制,从根本上保证软件的合法升级、数据被适当使用。CPU 是智能终端设备的核心芯片,如果 CPU 具备安全机制将是终端软件合法性的有力保障。

另外,从安全学的角度看,软件与任何其他采用数字技术的文档一样,可以通过数字签名验证签发者的合法性。

安全芯片正是从上述两个基本出发点解决终端系统的安全性问题。安全芯片通过芯片内部的安全模块验证外部数据(内存芯片中的程序)的合法性,只有确认内存中的程序合法之后,才会将系统控制权交给外部程序,从而开始智能终端的软件执行过程。

安全芯片的架构如图 2 所示。安全芯片除普通 SOC 芯片具备的各种寄存器、片内外设以外,还有一个称为安全域的特殊部分,该部分由安全算法模块与片内安全数据组成。其中,安全算法模块实现各种加密算法与散列算法,如 RSA、AES、SHA、HMAC 等,并可以对芯片外部存储器的数据进行签名验证,以确认将要启动的程序是否合法,只有外部存储器中的程序通过签名验证、证明合法后才会被执行。

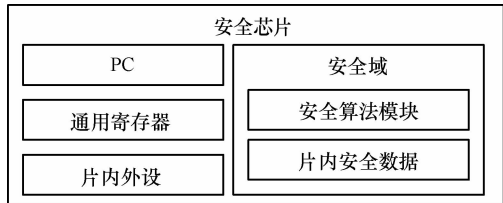


图 2 安全芯片架构

片内安全数据一般是 OTP(一次性写入)数据,这些数据具有可读属性,只有那些可读属性为真的数据才能被外部存储器中的程序读取,而不可读数据只能被安全算法作为参数使用,外部程序无法读取这些数据本身,只能将需要加/解密的数据传递给安全域,得到以 OTP 数据作为参数的加/解密结果。因此,只要确保这些 OTP 数据的唯一性,即可确保每一片芯片的唯一性,通过与业务平台的配合实现高等级的终端安全机制。

2.3 安全智能机顶盒的软件架构

安全智能机顶盒终端软件基本架构如图 3 所示。

终端软件系统分为安全域与普通域两个基本部分。用

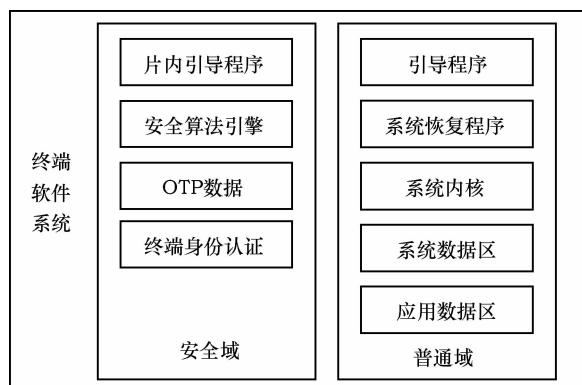


图3 安全智能机顶盒软件架构

户可接触位于普通域中的代码与数据,存储介质是 flash 与 RAM。安全域是用户以及普通域的代码不能直接接触的部分,部分核心数据对于普通域是不可见的,安全域位于 CPU 片内。

- CPU 利用安全域的片内引导程序对普通域代码进行基本的合法性验证,通常采用数字签名方法或代码加密方法实现。
- 安全算法引擎提供各类加密与散列算法,供普通域代码调用。
- OTP 数据域存放用户身份数据与加密算法密钥。
- 终端身份认证计算并输出终端身份认证所需的认证数据。
- 普通域中的引导程序是终端在启动过程中 CPU 执行的第一段片外代码,引导程序可根据不同的启动状态执行系统恢复程序或系统内核。
- 系统恢复程序可对系统内核、系统数据区、应用数据区进行升级、初始化等管理。
- 系统内核执行后将系统引导到终端的正常功能状态,在该状态下用户可通过终端正常使用业务功能。
- 系统数据区是终端最小的应用软件与数据存放区,终端只能通过软件升级与恢复对系统数据区进行修改。
- 应用数据区是用户选择安装程序与数据的存放区域,终端可在运行时对该区域进行修改操作。

2.4 中国电信智能机顶盒的安全流程

智能机顶盒通过采用安全芯片并使用特定的系统安全流程,实现终端软件系统的安全性,并保护业务系统的核心业务数据,从而确保用户与运营商的信息与设备安全。

中国电信的智能机顶盒安全方案主要包括安全启动

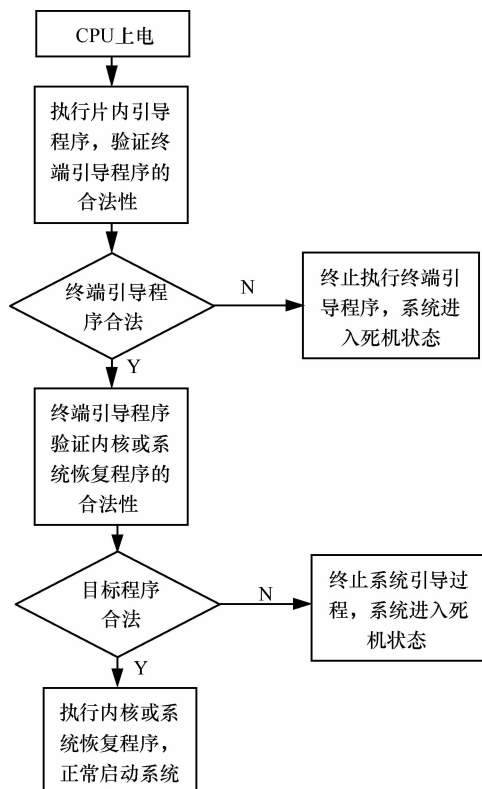


图4 终端软件安全引导过程

与终端验证两部分。安全引导过程如图4所示。

CPU 对终端引导程序的验证以及后续引导过程中的验证过程均采用安全、有效的验证算法,如基于 SHA256+RSA2048 的数字签名验证、基于 AES128 的代码加密方法。用于验证的密钥存放在 OTP 区域或以 OTP 区域数据为密钥进行加密后存放在 flash 中。图4中涉及的签名验证均采用全覆盖签名验证方式。

当内核被引导后,内核需要以文件系统或其他方式加载系统数据区中的数据。内核在加载系统数据区之前以及系统正常运行之后,都会对系统数据区采用随机抽样的片区数据验证方式进行合法性验证。

在系统软件升级时,系统恢复程序对将要用于系统升级或恢复的所有数据采用与引导程序相同的合法性验证方法进行验证。

从图4可以看出,智能终端从终端上电开始逐步对终端软件的各个部分进行合法性验证,整个过程构成了一个完整的安全链,极大地提升了终端软件的安全性。

在确保终端软件安全的情况下,为了验证终端本身的合法性,中国电信的安全终端还引入了如图5所示的终端

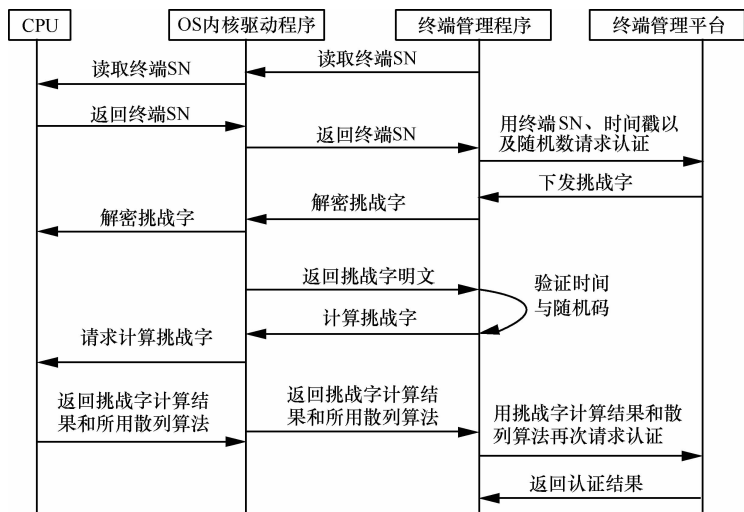


图5 终端身份验证流程

身份验证机制。

图5中终端管理程序与内核驱动程序均运行在终端软件系统的普通域,实现平台的身份认证协议。在身份认证过程中,终端在内核提供安全域访问的驱动程序,并提供应用调用API。内核驱动程序将终端管理程序API的相应请求发送到CPU安全域,由其返回对应的结果。图5中的SN为终端序列号,具备唯一性,存放在OTP区域,外部程序可读,而其他加密密钥均不可读。

通过采用可靠的终端启动安全链,配合终端身份验证机制,基本阻断了非法软件以及非法终端的接入途径,实现了可信终端。

中国电信智能机顶盒的安全流程除了安全启动流程外,还引入了基于芯片的终端身份验证机制,通过终端身份验证机制实现了对终端合法性的确认,使得业务的可控安全范围从业务平台扩展到了用户侧,终端成为可信设

备,极大地扩展了安全范围,有力地保证了业务的安全性。目前该方案已经进行了严格的实验室测试,其软件安全性取决于相关算法安全性以及密钥管理安全性,是一种较高级别的安全机制。该方案已经在中国电信股份有限公司上海分公司进行了试点。

3 结束语

本方案采用高安全级别的芯片安全机制以及OTP数据存储方法,对芯片安全模块进行了身份验证扩展,极大地提升了智能机顶盒的安全性,为后续中国电信智能机顶盒的推广应用提供了有力保障。

[作者简介]



胡冰松,男,中国电信股份有限公司上海研究院高级工程师、中国电信IPTV实验室成员,主要研究方向为手机、机顶盒、操作系统等终端相关基础技术。



黄小桑,男,硕士,中国电信股份有限公司上海研究院研发工程师,主要从事以IPTV业务为主的多媒体业务系统方面的相关技术及产品研发工作。

(收稿日期:2013-04-03)



· 简讯 ·

工业和信息化部出台 《“宽带中国 2013 专项行动”实施方案》

为全面贯彻落实党的十八大和《国民经济和社会发展的第十二个五年规划纲要》精神,加快下一代信息基础设施建设,2013年,工业和信息化部在“宽带普及提速工程”的基础上,启动实施“宽带中国 2013 专项行动”。3月7日,工业和信息化部发布了《“宽带中国 2013 专项行动”实施方

案》,明确了专项行动的主要目标、重点工作和进度安排。专项行动具体包括“城市宽带提速计划”、“农村宽带普及计划”、“农村校通宽带计划”、“应用创新推广计划”、“宽带体验提升计划”、“宽带产品研发计划”等6项行动计划,并将大力贯彻落实光纤到户两项国家标准,建立全国宽带网速监测分析机制,开展宽带城市评定等工作,促进我国宽带发展水平再上新台阶。

(来源:工业和信息化部通信发展司)