第 35 卷 第 2 期 计 算 机 工 程 2009 年 1 月
Vol.35 No.2 Computer Engineering January 2009
·安全技术· 文章编号：1000—3428(2009)02—0148—03 文献标识码：A 中图分类号：TP309

可信移动平台软件安全载入策略模型研究

李 建[1]，刘吉强[2]，周 正[3]，沈昌祥[4]，张 俊[3]
(1. 解放军信息工程大学电子技术学院，郑州 450002；2. 北京交通大学信息安全体系结构研究中心，北京 100044；
3. 海军工程大学电气与信息工程学院，武汉 430033；4. 海军计算技术研究所，北京 100841)

摘 要：针对手机卧底等木马软件通过软件下载的途径安装到用户手机，使手机用户的隐私受到了巨大的威胁的实际。通过分析目前软件下载方案中存在的安全问题及产生的根源，提出移动终端软件载入的控制策略，建立了策略模型，采用形式化的描述与分析，并从可信移动平台技术的角度，设计软件载入策略的实现方案，对模型和方案进行安全性分析，结果证明，该方案能有效地防范手机卧底等恶意软件的侵入。

关键词：移动平台；可信计算；安全分析

Study of Policy Model of Software Secure Loading for Trusted Mobile Platform

LI Jian[1], LIU Ji-qiang[2], ZHOU Zheng[3], SHEN Chang-xiang[4], ZHANG Jun[3]
(1. Institute of Electronic Technology, PLA Information Engineering University, Zhengzhou 450002; 2. Research Center of Information Secure Architecture, Beijing Jiaotong University, Beijing 100044; 3. College of Electrical and Information Engineering, Naval University of Engineering, Wuhan 430033; 4. Naval Institute of Computing Technology, Beijing 100841)

【Abstract】 Aiming at the fact that Xwodi, a kind of Trojan software, is fit in the users handsets by downloading software and threatens the privacy of user deadly. With analyzing security fault and cause in the solution of current software download. This paper puts forward the control policy for mobile equipment for downloading software, sets up politic model, carries out formalized description and analysis, designs implementing scheme of software loading policy from point of view of trusted mobile platform and makes security analysis for the model. Result indicates that the scheme can prevent Xwodi from being intruded effectively.

【Key words】 mobile platform; trusted computing; security analysis

1 概述

随着移动终端功能的不断增多，它已从只安装设备制造商提供软件的封闭平台，成为了可以从任何软件源安装各种软件的开放平台[1]。人们可以从网上下载各种应用软件、操作系统、驱动程序、无线电程序、中间件以及其他辅助软件。通过下载软件，人们可以给现有系统打补丁，改变系统设置参数和升级系统，大大节省了移动终端的维护费用。但是安全问题如影随行。由于HTTP和FTP等公共下载协议和机制本身存在的漏洞以及缺乏较为完善的检测手段，使得各种木马、病毒程序大行其道。如今年的手机卧底软件，又称Xwodi,就是国外间谍软件Flexispy的一个变种，它是在手机用户不知情的情况下，通过网络下载到手机等移动设备。当该软件运行时，可将机主的通信记录(语音、短信、通话人、通话时间等信息)以及存储的各种个人机密信息(如银行账号、密码等重要资料)发到指定的监视网站上，然后，可下载到监视手机。监视手机还可以通过拨通被监视手机，打开机内麦克风甚至打开摄影/摄像头对机主进行音频和视频监听和监视，使用户的隐私和通信安全受到了极大的威胁，不仅破坏了社会的和谐与稳定，而且还威胁到了国家安全。为此，研究人员针对手机软件下载提出了一些安全方案，如目的地保护[2]、安全措施[3]、平台软件的完整性和安全引导[4]、各种软件下载的公共需求[5]、软件下载[6]等方案，这些方案虽然在下载前进行了双方身份验证和下载代码完整性保护，但前提是移动终端和用户必须无条件地信任服务器来的下载软件，即假定下载的软件没有木马、病毒，从而没有对下载软件进行安全检测，而且软件的下载、安装以及运行方式也没有体现机主的意愿，目前还没有有效的改进方法来增强软件下载的安全。因此，本文拟从软件安全载入控制策略模型原理、安全载入实现方案、安全性分析和总结等方面对手机软件安全载入问题进行研究和探讨。

2 软件安全载入控制策略模型原理

可信移动平台软件安全载入控制策略模型基本思想是为了使软件安全载入：

(1)必须建立软件载入控制策略模型。即确定什么类型的软件可以载入，什么类型的软件不能载入。

(2)判断载入软件是否正确，代码有无被非授权修改。

(3)软件载入的内容是否包含有不安全的因素(比如恶意代码)。

基金项目：国家“863”计划基金资助项目(2006AA01Z440)
作者简介：李 建(1962－)，男，博士研究生，主研方向：信息安全，计算机网络安全；刘吉强，博士；周 正，博士研究生；沈昌祥，中国工程院院士、博士生导师；张 俊，博士研究生
收稿日期：2008-05-15 **E-mail：**pauljli@sina.com

(4)是安全状态的保护，即将通过检测后的软件进行加密和完整性保护后进行存储。基本流程如图 1 所示。

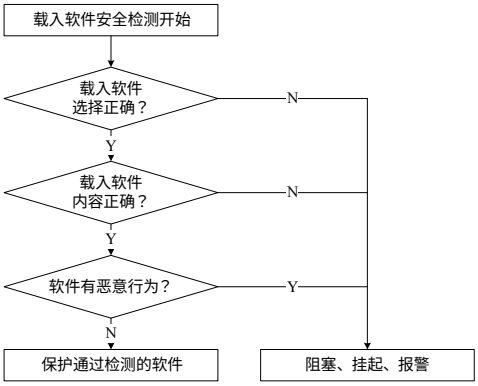

图 1　载入软件检测流程

其具体的流程可以分为载入软件选择、载入软件验证、运行动态阻塞和安全状态保护等部分。

2.1　载入软件选择规则

定义1 所有的代码构成的集合为 $E=\{e_1,e_2,\cdots,e_n\}$，其中，$\forall e_i$，$1\le i\le n$ 为任意一个待载入的软件代码。取 d_i，$1\le i\le n$ 为 e_i 的唯一标识，所有的标识构成的集合为 $D=\{d_1,d_2,\cdots,d_n\}$。取函数 $f_d:E\to D$，使得每一个 e_i 都有一个唯一的标识 d_i。

定义2 取 $t_r,1\le r\le m$ 为 $e_i\in E$ 的类型，所有的类型构成的集合为 $T=\{t_1,t_2,\cdots,t_m\}$，$m\le n$。存在一个类型划分函数 $f_t:E\to T$，使得 $\forall e_i\in E$，$\exists t_r\in T$ 与 e_i 相对应，表示为 $f_t(e_i)=t_r$。取与 $d_j,1\le j\le n$ 以及 $t_k,1\le k\le m$ 相关的 l_i 作为 E 中元素的选择表述，这些选择表述又构成一个选择表述集合 $L=\{l_1,l_2,\cdots,l_r\}$。在构造选择表述集合 L 的过程中存在函数 $f_l:D\times T\to L,\forall l\in L,\exists e\in E$，使得 $l=f_l(f_d(e)\times f_t(e))$。

这里定义类型划分函数 f_t 与选择表述函数 f_l 的目的是通过具体标识与类型的组合，可以灵活地把 E 中的元素设定到合理的域中，比如可以设定符合载入条件如白名单、信任网站等。目的是确保要下载安装的对象符合机主以及移动终端安全需要。针对下载安装的选择构建规则如下：

规则 1　$\forall e\in E$，$Select(e)\ \to\ \exists l\in L$　s.t.　$l=f_l(f_d(e)\times f_t(e))$。

这里的 $Select(e)$ 表示可以选择 e，其条件就是要符合某个选择表述 l 的要求。规则 1 的作用可以表述为：在规则 1 的约束下，体现了机主以及移动终端的安全需要的 L 可以保证 $Select(e)$ 符合机主以及移动终端安全需要，而不符合 L 的下载资源将不会与移动终端系统发生任何联系，更不会产生任何影响。

下载到移动终端的 e 的实际内容有没有被破坏或篡改，则需要接下来的载入验证规则来保证。

2.2　载入软件验证规则

定义3 在规则1的约束下选择的代码构成的集合记作 E_{Select}，显然 $E_{\text{Select}}\subseteq E$。$\forall e_i\in E$，$1\le i\le n$，取 c_i 表示 e_i 所独有的唯一特征，这些特征将构成一个特征集合 $C=\{c_1,c_2,\cdots,c_n\}$。定义特征函数 $f_c:E\to C$，使得 $\forall e\in E$，$\exists c\in C$，且 $f_c(e)=c$。

定义 3 中的特征集合与特征函数显然存在，签名、完整性校验值等都可看作特征函数的具体应用。定义特征函数就是构建出一种能够保证已经被选择下载且待载入目标 e 的完整性的规则。

规则 2　$\forall e_r\in E_{\text{Select}}$，$Import(e_r)\ \to\ f_c(e_r)=c_r$。

E_{Select} 表示在规则 1 的约束下已经选择(下载到移动终端)的代码(包括组件、安装包等)，$Import(e_r)$ 表示可以载入(安装)代码 e_r，前提是通过特征函数 f_c 能够得出期望的特征值 c_r。

2.3　动态阻塞规则

鉴于卧底代码未知，目前杀毒、扫描、沙箱等技术也都难以保证检查的完备性，因此要实行实体行为动态阻塞策略。

定义 4　$\forall e_i\in E_{\text{Select}}$，对应一个期望的操作清单 OPL_i，表示一系列的对哪些客体进行哪些操作的一个集合，记为：$OPL_i=\{(a_{i,1},o_{i,1}),(a_{i,2},o_{i,2}),\cdots,(a_{i,k},o_{i,l})\}$，当然 e_i 在实际的运行过程中又对应一系列的实际操作的一个集合，记为：$TO_i=\{(a_{i,1},o_{i,1}),(a_{i,2},o_{i,2}),\cdots,(a_{i,m},o_{i,n})\}$。

规则 3 对于 $\forall e_i\in E_{\text{Select}}$ 的实际过程操作：

(1) $\forall(a_{i,r},o_{i,s})\in TO_i\wedge(a_{i,r},o_{i,s})\notin OPL_i$　then　Deny

(2) $\forall(a_{i,r},o_{i,s})\in TO_i\wedge(a_{i,r},o_{i,s})\in OPL_i$　then　Accept

规则 3 在代码运行过程中发现并禁止不符合期望的操作，不但能够清除攻击和感染源而且能对潜在的攻击进行预警。由于它不考虑具体恶意代码的特征，因此避免了大量的特征码计算比较的工作量以及特征库的存储空间。

2.4　安全状态保护规则

规则 1~规则 3 实现了软件载入选择、载入软件验证以及载入软件不符合期望的操作的阻隔，保证了移动终端的安全性不会因为软件载入而受到损坏，那么这种安全状态在接下来的其他条件下如何继续保证呢？为此本文引入完整性检测函数、备份函数和恢复函数[7]。

定义 5 对 $\forall e\in E$，在任一时刻 k 有唯一特征码记 $c_{e,k}$，在 0 时刻的特征码为 $c_{e,0}$，E_k，E_0 分别是任一时刻 k 和 0 时刻系统程序的集合，取 $ST=\{UNMODIFIED,\ MODIFIED,\ NOTFOUND\}$，取 $g:e\to ST$，$\forall e\in E$，则

$$g(e)=\begin{cases}UNMODIFIED,\text{if } e\in E_0\cap E_k\wedge c_{e,k}=c_{e,0}\\ MODIFIED,\text{if } e\in E_0\cap E_k\wedge c_{e,k}\ne c_{e,0}\\ NOTFOUND,\text{if } e\in E_k-E_0\end{cases}$$

其中，称 g 为 E 的完整性检测函数。

这里的完整性检测函数 g 与定义 3 中的特征函数 f_c 的意义是不同的，f_c 是为了保证代码从服务器下载到移动终端并且在安装之前没有遭到修改或者破坏，而 g 是为了保护移动终端上的代码的完整性，因此，这里所提的特征的计算方式也与定义 3 中的不同。

定义 6 对 $\forall\ e\in E$，$content(e)$ 表示 e 中包含的信息，如果以 E 为定义域的函数，b 和 h 函数具有如下性质：

(1) b 的输出是另一个客体；

(2) $\forall\ e_1,e_2\in E,b(e_1)\ne b(e_2)$　iff　$e_1\ne e_2$；

(3) $M=\{content(e)|\forall e\in E\}$，$N=\{content(b(e))|\forall e\in E\}$，$\exists\ h:N\to M$　s.t.　$\forall\ e\in E$，$h(content(b(e)))=content(e)$。

则称 b 为 E 的备份函数，h 为 $b(E)$ 的恢复函数。显然，对 $\forall E$ 总是可以构造出 b 和 h。

定义 7 对 $\forall e_k\in E_k$，取 $w:E_K\to E_0$，s.t.　$\forall e_k\in E_k$，

$$w(e_k)=\begin{cases} e_0, \text{iff } g(e_k)=UNMODIFIED \\ h(b(e_0))=e_0, \text{iff } g(e_k)=MODIFIED \\ 0, \ \text{iff} \ \ g(e_k)=MODIFIED \wedge h(b(e_0))\neq e_0 \\ 0, \text{iff } g(e_k)=NOTFOUND \end{cases}$$

其中，称 w 为 E 的动态审查恢复函数。

在实际的代码将要载入执行时可以添加审查控制，并且以 $Go-on$ 表示不加任何干预， $Block$ 表示阻塞挂起将要执行的操作，可以得到下面的规则：

规则 4 当 $\forall e_k \in E_k$ 要载入执行时会出现以下 2 种情况：

(1) $Go-on \rightarrow w(e_k)=e_0$ ；

(2) $Block \rightarrow w(e_k)=0$ 。

规则 4 表示如果可执行程序没有被修改或者即使被修改但已经被恢复，那么程序的运行不会受到干预；如果程序被修改并且无法恢复，或者程序未知，则该程序的载入执行会被阻塞挂起，还可以进一步发出系统告警并且做出审计日志。

以上定义和规则分别从软件如何选择下载、选择下载的软件是否可信、载入运行的软件具体行为是否可信以及如何保护和恢复这种安全状态进行了分析和阐述，这 4 个方面构成了一个完整封闭的流程，对移动终端平台软件的更新实施了全方位的控制和保护。

3 安全载入实现方案

可信计算组织(TCG)的主要成员：NTT DoCoMo, IBM, Intel为移动无线设备定义了一个综合的端-端安全体系结构——可信移动平台[6]，根据软件安全载入模型要求，利用可信移动平台设计了如图 2 所示的下载软件安全载入方案。可信第三方TTP为证书机构，它产生了公私钥对，私钥用于对下载服务器证书进行签名。公钥用于验证证书，存储在可信移动终端的可信平台模块(TPM)中，TPM是一个内含密码运算函数和可信存储器的封闭的片上系统，它可以有效地阻止病毒、木马程序的攻击，保护内部数据的安全。证书还包含了下载服务器ID(SID)，SID也存储在TPM中，进行软件下载时，它与证书中的SID进行比较，以确定该可信移动终端就是要下载软件的平台，下载服务器证书使可信移动设备相信下载的软件来自合法的下载源。即SID与证书完成了软件下载双方的身份认证。由于下载的内容有时需要保密，则还要使用TPM中的SMS4 算法和对称密钥对下载的软件(或其他重要信息)进行加密，以防信息的非授权泄露。由AES算法使用可信移动设备的身份证明密钥AIK对下载双方共享对称密钥进行加密。证书的私钥对下载的软件进行签名，以保护下载软件的完整性。软件包中的时戳用于防止针对可信移动终端的DoS攻击。

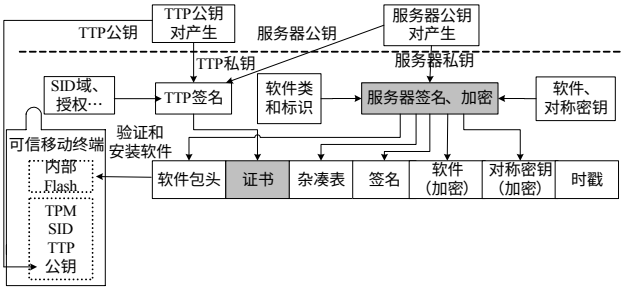

图 2 下载软件安全载入可信移动设备

4 安全性分析

(1)TTP 公私钥对的安全问题，其困难程度相当于大整数分解问题 FAC。显然，已知公钥，要推出私钥，在计算上是不可能的。

(2)该模型首先判别软件下载网站是不是可信网站，即下载网站有无 TTP 颁发的数字证书，若该网站服务器能够提供有效的数字证书，则表明该网站是合法的软件下载网站。否则，拒绝访问该网站，这样通过拒绝访问不合法的网站，避免了可信移动终端盲目下载软件的情况。

(3)通过将下载软件进行加密和完整性保护，保证了下载软件不被非授权的访问和篡改。再加上时戳，还能有效地防止信息在传输途中的某个系统重复将数据包发往用户可信移动终端，造成 DoS 攻击。

(4)通过对下载软件进行恶意代码检测，先进行正常的行为模式的检测，可以区分出下载软件的行为模式，再将非正常行为模式进行特殊行为检测，如有在非授权的情况下打开机内麦克风、打开摄影/摄像头和将短信记录、通信录、个人机密资料向外发送的行为，将作为攻击软件进行挂起、阻塞和报警。

5 结束语

本文针对当前手机软件下载存在严重安全威胁的现实，建立了可信移动平台软件安全载入策略模型，通过规定移动终端能载入什么软件，不能载入什么软件来保证软件来源的可信；通过检查载入的软件是否被篡改来保证载入软件本身的可信；通过检测载入的代码是否安全来保证载入软件行为的可信；通过对载入的安全代码实施保护和恢复来保证安全状态的可信和保持。这种模型不仅为当前移动终端软件下载和执行中出现的安全问题提供了解决方案，而且能够对将来的智能移动终端可能存在的恶意代码等安全问题的解决提供支持。

参考文献

[1] Pisko E, Rannenberg K, Roβnagel H. Trusted Computing in Mobile Platforms Players, Usage Scenarios, and Interests[J]. Datenschutz and Datensicherheit, 2005, 9(29): 526-530.

[2] 谢俊杰, 孟利民. 软件无线电的软件下载与安全策略[J]. 计算机与数字工程, 2006, 34(5): 24-26, 40.

[3] Cook P G. Wireless Software Download Security[EB/OL]. (2006-06-14). http://www.sdrforum.org/uploads/pub_17683004_ i_ 0069_v0_00_wireless_securit y_06_14_04.pdf.

[4] Gehrmann C, Ståhl P. Mobile Platform Security[EB/OL]. (2006-02-16). http://www.ericsson.com/ericsson/corpinfo/publica-tionns/review/2006_ 02/03.shtml.

[5] Hoffmeyer J, Park I, Majmundar M. Radio Software Download for Commercial Wireless Reconfigurable Devices[J]. IEEE Radio Communications, 2004, 42(3): 26-32.

[6] Aissi S, Maruyama H, Miura F, et al Trusted Mobile Platform Protocol Specification Document[EB/OL]. (2004-04-05). http:// www.trusted-mobile.org/TMP_Protocol_rev1_00.pdf.

[7] 陈泽茂, 沈昌祥. 基于操作系统安全的计算机病毒防御策略[J]. 武汉理工大学学报, 2004, 26(9): 75-77.