Journal of Computer Applications
计算机应用,2014,34(2):473 -476
ISSN 1001-9081
CODEN JYIIDU
2014-02-10
http://www.joca.cn

文章编号:1001-9081(2014)02-0473-04
doi:10.11772/j.issn.1001-9081.2014.02.0473

基于污点标记的访问控制模型及其安卓实现

吴泽智[1*],陈性元[1],杨　智[2],杜学绘[2]
(1.信息工程大学 密码工程学院,郑州 450001;　2.信息工程大学 网络空间安全学院,郑州 450001)
(*通信作者电子邮箱 1141208772@qq.com)

摘　要:为保护移动操作系统平台中存储的用户隐私数据,提出一个基于污点标记的访问控制(TBAC)模型,并设计了一个基于污点跟踪的信息流控制框架(TIFC)。为数据添加污点标记,控制力度细化到数据;引入主体能力保证最小特权原则;主体能力独立于数据污染与可信去污防止污点积累。该模型与 BLP 模型相比更加可用、灵活与细粒度。该框架能细粒度地、灵活地、准确地实时跟踪并控制隐私信息的流向,并解决了程序执行中因控制流产生的隐蔽通道问题。

关键词:安卓;隐私安全;访问控制;污点跟踪;隐蔽通道
中图分类号:TP309.2　　**文献标志码**:A

Taint-marking based access control model and its implementation on Android

WU Zezhi[1*], CHEN Xingyuan[1], YANG Zhi[2], DU Xuehui[2]
(1. *College of Cryptogram Engineering, Information Engineering University, Zhengzhou Henan* 450001, *China*;
2. *College of Network Space Security, Information Engineering University, Zhengzhou Henan* 450001, *China*)

Abstract: For protecting the sensitive data on mobile operation system, a Taint-marking Based Access Control (TBAC) model was presented and a Taint-marking Information Flow Control (TIFC) framework was proposed. To improve fine-grained data sharing, labels were designed for each data. To support for least privilege characteristic, capacities were defined to each subject. To avoid accumulating of contamination, decontamination capacities of trust subjects were introduced. Compared with BLP, TBAC is more available, flexible and fine-grained. The results show TIFC is an effective, flexible and accurate framework in tracking and controlling the information flow at runtime, and TIFC solves the problem of covert channel caused by control flow during program execution.

Key words: Android; privacy security; access control; taint tracking; covert channel

0　引言

移动互联是信息时代科技发展的必然趋势。智能终端在人们日常生活已经扮演着不可替代的角色。智能手机上存储着大量用户个人隐私信息,如手机串号、用户标识、电话状态、认证数据、短信、地理位置、认证信息、隐私文件等。然而,此类信息的安全却得不到有效的保证[1-3]。鉴于安卓占领了中国近90%市场及其开源特性,对其进行隐私安全增强十分必要和可能。

安卓体系结构大致可分为四层,从高层到低层分别是应用程序层、应用程序框架层、系统运行库层和 Linux 内核层。安卓为数据安全提供应用程序隔离机制和权限机制,应用程序隔离机制指不同签名的应用程序在安装时,都会被赋予不同的用户标识且运行在不同的系统进程内,任何由应用程序存储的数据不能被其他应用程序访问。权限机制是在应用程序框架层的一个基于能力的访问控制框架。应用程序根据自己需要访问的系统资源或其他应用程序组件,申请对应的权限;但权限机制不能防止混淆代理人攻击和共谋攻击[4-5]。目前,对安卓系统隐私安全增强工作主要有 SEAndroid[6]、Kirin[7]、Apex[8]、Quire[9] 和 TaintDroid[10] 等。SEAndroid 将 SELinux 移植到安卓平台上,强化安卓应用程序对文件的存取控制;但控制力度仅在进程层面而不能面向数据本身,而且安全策略缺乏针对性和灵活性。Kirin、Apex、Quir 主要研究权限机制以增强应用程序对敏感信息的使用权限;但基于权限机制分析难于克服权限机制自身过于粗糙缺点。TaintDroid 实现了安卓平台上的动态实时隐私信息污点跟踪;但其缺乏对信息流的控制机制,而并不能防止用户隐私的泄露,且已有研究都未曾提出针对移动平台的安全模型。

为解决移动平台数据隐私安全问题,借鉴已有安全模型的设计思想[11-12]与已有安卓安全研究工作的方法,提出一个基于污点的访问控制模型。模型的基本思想是:主客体能力决定信息流向;控制力度细化到数据;主体能力独立于数据污染;分析污点传播以关闭隐蔽通道;可信去污防止污点积累。依据此模型设计了一个并设计了一个基于污点跟踪的信息流控制框架(Taint-marking based Information Flow Control, TIFC)。该框架能细粒度地、灵活地、准确地实时跟踪应用程

收稿日期:2013-07-02;**修回日期**:2013-10-24。
基金项目:国家973计划项目(2011CB311801);国家863计划项目(2012AA012704);河南省科技创新人才计划项目(114200510001)。
作者简介:吴泽智(1990-),男,湖南长沙人,硕士研究生,主要研究方向:信息安全;　陈性元(1963-),男,安徽无为人,教授,博士生导师,博士,主要研究方向:信息安全;　杨智(1975-),男,河南开封人,副教授,博士,主要研究方向:信息安全;　杜学绘(1968-),女,河南新乡人,教授,博士生导师,博士,主要研究方向:空间信息网络、信息安全。

序所使用隐私信息并控制隐私信息的流向,试图解决程序执行中产生隐蔽通道问题;并通过分析指令污点传播,试图解决程序执行中产生隐蔽通道问题。

1 基于污点标记的访问控制模型半形式化描述

1.1 系统定义

1) 主体集 $S = \{S_1, S_2, \cdots, S_n \mid (M,B)\}$:主体指主动行为发出者,包括应用程序或进程。

2) 客体集 $O = \{O_1, O_2, \cdots, O_n \mid (M,B)\}$:客体指行为的承受者,包括主体、文件、数据、资源等。

3) 颜色集 $C = \{color_1, color_2, \cdots, color_n\}$:$color_i$ 表示污点基本种类。如 $color_1$ 表示黄色,$color_2$ 表示绿色。在秘密域可表达秘密信息范畴,在完整域可表达信息恶意来源。

4) 能力集 $B = C \times (+, -)$:$color_i^+$ 表示主体或客体能被 $color_i$ 污染,$color_{i-}$ 表示主体能除去客体 $color_i$ 污点。

5) 污点集 $T = \{taint_1, taint_2, \cdots, taint_n\}$,其中 $\{taint_i \mid \forall i(1 \leqslant i \leqslant n), color_i \in C\}$:$taint_i$ 表示一个污点,其可能由任意不同数量 $color_i$ 组成。

6) 数据元集 $M = \{m_1, m_2, \cdots, m_n\}$:数据元 m_i 表示主体所使用的数据。为详细刻画主体污染状态,主体不同数据 m_i 可标记不同污点。

7) 污点-能力向量集 $F = \{f \mid f = (f_t(m), f_b(S,O))\}$:数据污点映射函数 f_t 表示从数据 m 中提取污点;能力映射函数 f_b 表示提取主客体能力。

8) 访问权限集 $A = \{r, w, c\}$:r表示主体读客体,w表示主体写客体,c 表示主体清除污点所含颜色。

9) 决定集 $D = \{accept, deny\}$:由允许(accept) 或拒绝(deny) 组成。

1.2 规则描述

1.2.1 访问控制规则

规则 1 $D(S, m_s, r, O, m_o) = accept \leftrightarrow \forall color_i \in f_t(m_o), color_i^+ \in f_b(S)$

表示主体能读客体当且仅当主体所含客体污点集中所有污点颜色能被污染。比如,系统某文件污点信息中包含红色与绿色,某进程能读取该文件,则红色和绿色属于进程颜色集,且该进程必须具备被红色和绿色感染能力。

规则 2 $D(S, m_s, w, O, m_o) = accept \leftrightarrow \forall color_i \in f_t(m_s), color_i^+ \in f_b(O)$

表示主体能写客体当且仅客体所含主体数据集中所有污点颜色能被污染。比如,系统某进程向文件中写含红色污点的信息,则红色属于该文件颜色集,且该文件必须具备被红色感染能力。

规则 3 $D(S, c, O, m_o, color_i) = accept \leftrightarrow color_i \in f_t(m_o) \wedge color_{i-} \in f_b(S)$

表示主体能除去客体感染的颜色当且仅当该颜色属于客体污点,且主体具有对该颜色的去污能力。比如,某文件包含红色污点,具备删除红色能力的进程可以将红色污点从客体数据属性中除去。

1.2.2 污点传播规则

规则 4 $D(S, m_s, r, O, m_o) = accept \rightarrow f_t(m_s) = f_t(m_o) \cup f_t(m_s)$

表示主体从客体中读数据存入 m 后,数据 m 污点将更新为客体污点与数据 m 污点并集。比如,某进程数据污点包含绿色,某文件污点包含红色与黄色,当读动作发生后,进程数据污点更新为绿色、红色与黄色。

规则 5 $D(S, m_s, w, O, m_o) = accept \rightarrow f_t(m_o) = f_t(m_o) \cup f_t(m_s)$

表示主体将数据 m 写入客体后,客体污点将更新为客体污点与数据 m 污点并集。比如,某进程数据污点包含绿色,某文件污点包含红色与黄色,当写动作发生后,文件污点更新为绿色、红色与黄色。

规则 6 $D(S, c, O, m_o, color_i) = accept \rightarrow f_t(m_o) = f_t(m_o) - color_i$

表示主体删除客体污点某种颜色后,该颜色从污点中除去。比如,某文件污点包含红色与黄色,当删除黄色动作发生后,文件污点更新为红色。

规则 7 $(S(m_1) \rightarrow S(m_2)) \rightarrow f_t(m_2) = f_t(m_1) \cup f_t(m_2)$

表示数据污点在进程内部传染。比如,某进程内数据 m_1 污点包含绿色,m_2 包含红色,该数据 m_1 拷贝到数据 m_2 时,数据 m_2 污点更新为绿色与红色。

1.3 模型对比

常见的计算机安全模型包括 Biba、RBAC、BLP 和 GTPM (Generalized Taint Propagation Model)[11]。Biba 模型主要完整性保护,但其完整性等级难于确定,基本不能构造一个可用系统。基于污点标记的访问控制(Taint-marking Based Access Control, TBAC)模型通过主客体拒绝污染能很好支持完整性保护。RBAC 模型能有效支持最小特权原则,但基于传统访问控制的模型不能控制对信息的传播和间接污染。BLP 模型基于格模型能控制信息流向,但对安全等级划分过于生硬,可用性较差。TBAC 模型引入主体能力能有效支持最小特权原则和职责分离原则,并通过控制污点传播以控制信息在整个系统的流向,甚至发现系统中存在的隐蔽通道。此外,TBAC 引入可信主体和可信去污概念,保证模型可用性。与 GTPM 相比,TBAC 提供更细粒度基于数据的信息流控制机制。

2 TIFC 设计

2.1 系统框架

如图 1 所示:1) 调用敏感 API,如地理位置提供者,将其获得数据标记污点;2) 调用本地方法,借助解释器状态,将污点传入并返回;3) 数据在虚拟机内执行过程中进行复制或运算等处理,污点随之传播;4) 发生进程间通信时,依据策略判定是否允许,如果允许,将污点按规定格式写入通信数据结构中;5) 进行文件读写时,依据策略判定是否允许,写文件时,将文件标记为污点,读文件时,将读取数据标记为污点;6) 数据离开系统时,依据策略判定是否允许。

2.2 关键技术

2.2.1 污点存储

污点存储在程序变量、文件、解释器状态、进程通信数据结构中。对于程序运行时的变量,为与 Dalvik 寄存器规范一致,使用 32 位来存储一个污点。对于文件,则通过修改文件数据结构,将污点信息保存在附加属性中。对于解释器状态和进程间通信污点保存在运行时相应数据结构中。

2.2.2　指令污点传播

通过研究 Dalvik 指令格式和类型,将可能产生信息流指令分为 16 大类,如表 1 所示。其中 vx、vy、vz 是寄存器, fy、fz 是字段 ID,T( )表示污点值。

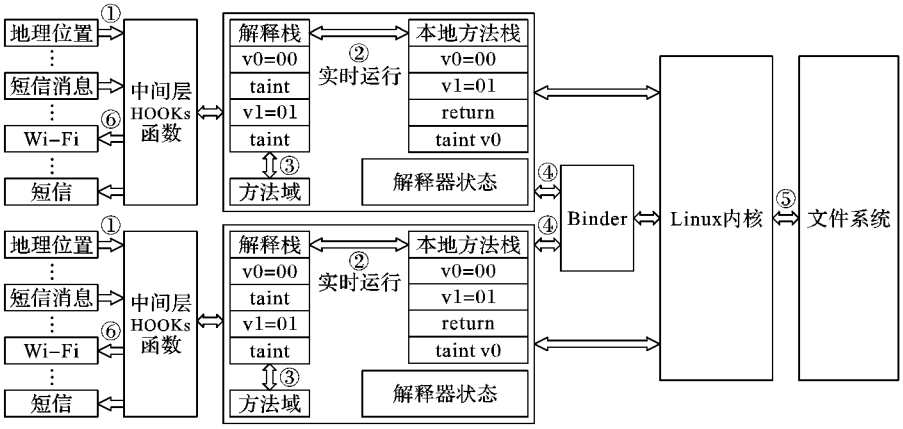

图 1　系统框架

表 1　指令污点传播分析

序号	指令类型	指令含义	污点传播逻辑	污点传播描述
1	Move vx,vy	移动 vy 的内容到 vx	T(vy)→T(vx)	将 T(vy)复制到 T(vx)
2	Return vx	返回在 vx 的值	T(vx) →T(∑)	将 T(vx)返回
3	Const vx,lit32	将 lit32 值存入 vx	T(vx)→0	清空污点
4	Throw vx	将出错信息返回 vx	T(vx)→T(E)	设置出错污点
5	Iput vx,vy, fz	根据 fz 将 vx 值存入实例 vy 的 int 型字段	T(vx)∣T(vy)→T(fz)	将 T(vx) 与 T(vy)存入实例 int 字段
6	Iget vx,vy, fz	根据 fz 读取实例 vy 的 int 型字段到 vx	T(fz)∣T(vy)→T(vx)	将 T(vy) 与实例 int 字段相与存入 T(vx)
7	Sput vx, fy	根据 fy 将 vx 存入 int 型字段	T(vx)→T(fy)	将 T(vx)复制到 T(fy)
8	Sget vx, fy	根据 fy 读取 int 型字段到 vx	T(fy)→T(vx)	将 T(fy)复制到 T(vx)
9	Aput vx, vy, vz	将 vx 值存入位于 vy 的数组引用且索引位置为 vz	T(vx)→T(vy)	将 T(vx)复制数组污点
10	Aget vz,vy,vz	从位于 vy 的数组引用获取索引位置为 vz 的 int 型值存入 vx	T(vy)→T(vx)	将数组污点复制到 T(vx)
11	And vx,vy,vz	将 vy∣vz 并存入 vx	T(vy)∣T(vz)→T(vx)	将 T(vy)与 T(vz)相与并存入 T(vx)
12	Add vx,vy,vz	计算 vy + vz 并存入 vx	T(vy)∣T(vz)→T(vx)	将 T(vy)与 T(vz)相与并存入 T(vx)
13	If-lt vx,vy,0080	如果 vx < vy,跳转到目标 0080	T(vx)∣T(vy)→T(vy) ∪T(vx)	将 T(vx)与 T(vy)相与并更新各自污点
14	Int-to-long vx,vy	将 vy 中 int 值转换 long 并保存到 vx,vx + 1	T(vy)→T(vx)	将 T(vy)复制到 T(vx)
15	Neg vx,vy	计算 vx = - vy 并保存在 vx	T(vy)→T(vx)	将 T(vy)复制到 T(vx)
16	Cmpl vx, vy, vz	比较 vy 和 vz 的值并在 vz 存入 int 型返回值	T(vy)∣T(vz)→T(vz)∪T(vy) ∪ T(vz)	将 T(vy)与 T(vz)相与更新各自污点并存入 T(vz)

3　示例分析和系统测试

3.1　示例分析

如图 2 所示,安卓系统安全需求可描述为:允许飞信读取通讯录和通过短信接口发送短信,但禁止通过短信接口发送包含联系人信息和读取地理位置信息;允许 QQ 读取地理位置信息和通过网络接口发送聊天信息,但禁止通过网络接口发送包含地理位置数据和读取联系人信息;允许飞信和 QQ 间通信,但禁止通信内容包含联系人信息和地理位置信息。

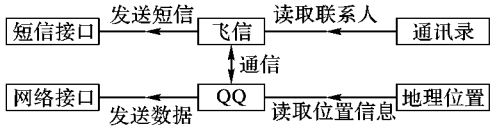

图 2　安卓应用系统

针对如上安全需求,BLP 过于刚性约束,无法表达飞信可发送短信,但禁止发送包含敏感信息的短信。RBAC 无法表达允许飞信和 QQ 间通信,但禁止通信内容包含联系人信息和地理位置信息。TBAC 能有效描述此安全需求:飞信程序标记为具备联系人感染能力;QQ 程序标记为具备地理位置感染能力;通读录标记为通讯录敏感;地理位置提供者标记为地理位置敏感;短信接口和网络接口标记为空,可发送任何未被污染数据。飞信具备联系人感染能力,能读取联系人信息,以支持基本短信发送功能。当通过短信发送所读取联系人信息时,由于发送数据已发生污染,发送失败。QQ 不具备通讯录感染能力,故不能直接读取联系人信息。当飞信向 QQ 发送联系人信息时,数据已污染且 QQ 不具备该感染能力,通信失败。飞信与 QQ 程序读取敏感信息,污点保存在所读数据上,仍然可发送未被污染信息,可保证系统持续运行和可用

性。

3.2 系统性能测试

TIFC 在模拟器上运行测试(Ubuntu 10.04, Android 4.1.1),由于模拟器与真机实验条件差异,并不能提供真实的地理位置信息、短信、蓝牙和网络等环境,同时模拟器较真机效率较低。但模拟器可以通过 DDMS(Dalvik Debug Monitor Service)提供更加充分的调试命令和虚拟出必要的测试环境。TIFC 对系统性能主要表现在系统调用时间上。通过 logcat 分析系统调用完成时间差,并与原系统进行对比,结果如表2所示。

表2 系统调用完成时间差对比

系统调用 API	完成时间差/ms		延迟率/%
	原系统	TIFC 系统	
获取地理位置	62	69	11.2
发送短信信息	72	86	19.4
拍摄图片	555	621	12.4

4 结语

随着移动互联网络的发展,更多更强大的功能将出现在移动终端上,甚至,政府、军队、企业的业务都向移动终端上拓展。安卓作为当前最流行的移动终端平台,针对其安全研究将会是一项长期而艰巨的任务。

本文针对现有的访问控制模型在保护移动平台数据安全都有一定局限性。借鉴了软件测试中的用于跟踪和分析输入数据在程序内部流向的污点传播机制,并从吸取传统访问控制模型中的思想,提出一个基于污点的访问控制模型。TBAC 相比现有访问控制模型更加可用、灵活与细粒度。TBAC 试图通过污点传播分析来解决程序执行过程中产生隐蔽通道问题,还设计了一个基于污点标记与跟踪的隐私信息控制框架。TIFC 通过分析安卓平台上所有污染源与污染离开点、研究污点在程序执行中的传播方式与途径、控制关键点的信息流向,能细粒度地、灵活地、准确地实时跟踪应用程序所使用隐私信息并控制隐私信息的流向。下一步将对该模型进行扩展,以满足不同安全需求,并对模型进行形式化验证。

参考文献:

[1] ZHOU Y, JIANG X. Dissecting Android malware: characterization and evolution[C]// IEEE Symposium on Security and Privacy. Piscataway: IEEE Press, 2012: 95 - 109.

[2] LA POLLA M, MARTINELLI F, SGANDURRA D. A survey on security for mobile devices[J]. IEEE Communications Surveys & Tutorials, 2012, 15(1): 446 - 471.

[3] VIDAS T, VOTIPKA D, CHRISTIN N. All your droid are belong to us: a survey of current Android attacks[C]// Proceedings of the 5th USENIX Conference on Offensive Technologies. Berkeley: USENIX Association, 2011: 10 - 19.

[4] MARFORIO C, FRANCILLON A, CAPKUN S, *et al.* Application collusion attack on the permission-based security model and its implications for modern smartphone systems [R]. Zürich: Eidgenössische Technische Hochschule Zürich, Department of Computer Science, 2011.

[5] ENCK W, OCTEAU D, MCDANIEL P, *et al.* A study of Android application security[C]// Proceedings of the 20th USENIX Security Symposium. Berkeley: USENIX Association, 2011: 101 - 113.

[6] SMALLEY S, CRAIG R. Security Enhanced (SE) Android: bring flexible MAC to Android[C]// Proceedings of the 2013 Network & Distributed System Security. San Diego: Internet Society, 2013: 75 - 84.

[7] ENCK W, ONGTANG M, MCDANIEL P. On lightweight mobile phone application certification[C]// Proceedings of the 16th ACM Conference on Computer and Communications Security. New York: ACM, 2009: 235 - 245.

[8] NAUMAN M, KHAN S, ZHANG X. Apex: extending Android permission model and enforcement with user-defined runtime constraints [C]// Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security. New York: ACM Press, 2010: 328 - 332.

[9] DIETZ M, SHEKHAR S, PISETSKY Y, *et al.* Quire: lightweight provenance for smart phone operating systems[C]// Proceedings of the 20th USENIX Security Symposium. Berkeley: USENIX Association, 2011: 371 - 387.

[10] ENCK W, GILBERT P, CHUN B G, *et al.* TaintDroid: an information-flow tracking system for realtime privacy monitoring on smartphones[C]// Proceedings of the 9th USENIX Conference on Operating Systems Design and Implementation. Berkeley: USENIX Association, 2010: 1 - 6.

[11] YANG Z, YIN L, DUAN M, *et al.* Generalized taint propagation model for access control in operation systems[J]. Journal of Software, 2012, 23(6): 1602 - 1619. (杨智, 殷丽华, 段洣毅, 等. 基于广义污点传播模型的操作系统访问控制[J]. 软件学报, 2012, 23(6): 1602 - 1619.)

[12] LI F H, SU M, SHI G Z, *et al.* Research status and development trends of access control mode[J]. Journal of Electronics, 2012, 40(4): 805 - 813. (李凤华, 苏锑, 史国振, 等. 访问控制模型研究进展及发展趋势[J]. 电子学报, 2012, 40(4): 805 - 813.)

(上接第455页)

[8] HE W, LIU X, NGUYEN H, *et al.* PDA: Privacy-preserving data aggregation in wireless sensor networks[C]// Proceedings of the 26th IEEE Conference on Computer Communications (INFOCOM). Piscataway: IEEE, 2007, 2045 - 2053.

[9] DAS M L. Two-factor user authentication in wireless sensor networks[J]. IEEE Transactions on Wireless Communications, 2009, 8(3): 1086 - 1090.

[10] TIWARI H, ASAWA K. A secure and efficient cryptographic hash function based on NewFORK-256 [J]. Egyptian Informatics Journal, 2012, 13(3): 199 - 208.

[11] KHAN M K, ALGHATHBAR K. Cryptanalysis and security improvements of two-factor user authentication in wireless sensor networks[J]. Sensors, 2010, 10(3): 2450 - 2459.

[12] DYANG D H, LEE M K. Improvement of Das's two-factor authentication protocol in wireless sensor networks [J/OL]. (2009-12-20)[2013-06-20]. http://eprint.iacr.org/2009/631.pdf.

[13] CHEN T H, SHIH W K. A robust mutual authentication protocol for wireless sensor networks[J]. ETRI Journal, 2010, 32(5): 704 - 712.