

基于 Web 操作系统的移动瘦终端多安全策略模型

杨莹^{1,2} 夏剑锋^{1,2} 朱大立²

(中国科学院大学网络空间安全学院 北京 100093)¹ (中国科学院信息工程研究所 北京 100093)²

摘 要 高安全级移动办公对信息系统不断提出更高的安全需求,在此背景下出现了瘦终端(Thin-Client)解决方案。其采用云存储、分布式终端系统和集中管理,为用户提供了更好的安全性。当前的主要技术包括虚拟桌面和 Web 终端,其中前者是主流。近年来,Web 操作系统(Web OS)的发展促使 Web 终端受到业界重视,但 Web OS 还存在机密性和完整性保护不足的问题。基于 Web OS 系统的特点抽象建模,提出了混合机密性模型 BLP 和完整性模型 Biba 的多安全策略模型。首先利用格将机密性标签、完整性标签和范畴集合相结合,解决了 BLP 与 Biba 信息流相反的问题;然后提出可信主体的最小特权原则来进一步约束可信主体的权限,并给予特定可信主体临时权限,以提高灵活性和可用性;最后分析模型的安全性和适用性。

关键词 移动瘦终端, Web 操作系统, 安全模型, 格, 访问控制

中图法分类号 TP309.1 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2018.11.016

Multi-policy Security Model of Mobile Thin Client Based on Web Operating System

YANG Ying^{1,2} XIA Jian-feng^{1,2} ZHU Da-li²

(School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100093, China)¹

(Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China)²

Abstract High-security mobile office has put forward growing security requirements on information systems. In this context, thin-client based solution exists. The solution takes the advantages of cloud storage, distributed terminal system and centralized management, and provides better safeguard for users. Nowadays, the main technologies of thin client are virtual desktop infrastructure (VDI) and Web-client, in which the former is the mainstream, while the latter has received widespread attention with the development of Web-based operating system (Web OS). However, there are some problems, including lower confidentiality and integrity in the existing Web OSes. Based on the abstract modeling of Web OS, this paper proposed a hybrid model by mixing BLP model and Biba model. In order to solve the collision of information flow, a lattice structure was introduced. Since information flow model has no constraints on trusted subjects, the principle of least privilege on trusted subject was promoted. To improve the flexibility and availability, a special trusted subject was authorized to change the security level temporarily. Finally, the security and applicability were analyzed.

Keywords Mobile thin client, Web OS, Security model, Lattice, Access control

1 引言

随着移动智能终端普及率的提高,电子商务、移动支付、移动办公等业务应运而生,同时也暴露出了大量安全问题。传统的智能终端虽然通过一些安全加固手段提高了其安全性,但仍不能满足人们日益增长的安全需求。特别是在移动政务领域,政务信息系统已经由单一的、小规模的系统向多应用、大型、分布式的系统发展。系统复杂度和系统集成中授权管理的难度增大,亟需能够不考虑终端实现平台而进行统一配置,并通过对数据乃至终端资源的集中管理来解决整个系统的安全性。在此背景下,瘦终端解决方案受到了广泛关注。

富终端也称为智能终端,具有智能操作系统,如 Android、iOS 等,具有丰富的应用程序、本地存储和运算处理能力。零终端恰恰相反,不具备操作系统,只提供屏幕显示。瘦终端介于这两者之间,具有 OS、CPU、运算处理等功能,并能够实现数据云存储与集中管理^[1],进而提供更好的安全性。瘦终端相比零终端更灵活,能够提供更多的外设支持,并可通过配置以适应多协议环境。鉴于这些优势,美国政府已计划用瘦终端或零终端替换几乎所有的富终端^[2]。

当前移动瘦终端主要采用虚拟桌面和 Web 终端技术。在访问内容丰富的网站和执行复杂的应用程序时,虚拟桌面严重依赖带宽和使用的传输协议,尤其在使用 3G 等窄带宽

到稿日期:2017-10-22 返修日期:2018-01-24 本文受中国科学院战略性先导专项项目(XDA06010703)资助。

杨莹(1981—),女,博士生,主要研究方向为智能终端安全、操作系统安全,E-mail:yangying@iie.ac.cn(通信作者);夏剑锋(1988—),男,博士生,主要研究方向为数据分析与隐私保护;朱大立(1972—),男,研究员级高级工程师,主要研究方向为智能终端安全、无线管控技术、大数据隐私与保护等。

传送屏幕信息时会产生较大的延迟。另外,还存在服务器端和终端所使用的 OS 不匹配问题,用户必须采用其公司支持的终端平台,因此跨平台性和可用性受限。主流厂商如 VMware、Citrix 和 Microsoft 都致力于研发高性能的传输协议^[3],但目前没有适配所有平台的通用协议。Web OS 是一种新型的操作系统,使用统一标准的 Web 语言开发,类似于浏览器,但能够为系统的软硬件资源提供保护域。基于 Web OS 的瘦终端因为更少与服务器通信,缩短了响应的延迟,进而提供更好的用户体验。当前的 Web OS 采用自主访问控制,面向高安全级移动办公时还须引入强制访问控制模型,以防止未经授权的访问和修改。本文提出了混合 BLP 和 Biba 的多安全策略模型 WLBB(Lattice-based BLP and Biba hybrid model for Web OS),通过格来描述两个模型中的主客体的安全级,并结合 Web OS 的特性重定义模型元素、安全定理和状态转换规则。通过定义特殊可信主体实现两个方向的信息流来提高可用性。Web OS 由于具有良好的跨平台特性和可迁移性,符合未来移动办公的需求,本文提出的基于 Web OS 特征的多安全策略模型为高安全级移动办公的瘦终端解决方案提供了系统安全性增强的措施。

2 研究现状

当前 Web OS 安全方面的研究主要从 Web 应用的安全性^[4-7]、权限机制^[8-9]和应用审核发布^[10-13]等方面进行,还有一些研究针对移动网络的攻击^[14-15]和内置广告的威胁^[16-17]来进行。Zhu 等^[18]提出了一种面向高安全级的解决方案,通过引入改进的 BLP 模型来提高 Web OS 的机密性。

强制访问控制 Bell-LaPadula(BLP)模型^[19]由 Bell 和 LaPadula 于 1973 年首次提出,用于在政府和军事应用中实施访问控制,其策略概括为“不上读,不下写”。BLP 模型的 * 特性对可信主体没有约束,存在利用可信主体实现高安全级到低安全级的信息流。Liu 等^[20]通过细分操作和权限,约束可信主体遵守最小特权原则。陈亮等^[21]实现了对可信主体的约束,这些研究仍未能解决完整性保护的问题。Biba 于 1975 年开发的 Biba 模型^[22]是针对数据完整性保护的,其严格完整性策略与 BLP 模型在形式上对偶,安全策略可概括为“不下读,不上写”。一些研究^[23-24]通过在系统中增加主客体的完整性标签来引入 Biba 模型,但是简单叠加的方法的可用性差^[25]。Biba 直观且易于理解,但是在实际系统中完整性标签很难确定^[26]。BLP 和 Biba 中的可信主体不受限制,因此可信主体的可信和安全验证成为了一个新的问题^[27]。

基于格的访问控制(Lattice Based Access Control, LBAC)模型由 Denning^[28]于 1976 年正式提出,Sandhu^[29]于 1993 年也给出了定义。LBAC 模型主要是基于国防部门的需求,但其理论和概念适用于几乎任何关注信息流向的情况,因此 BLP 和 Biba 也可以看作是信息流的访问控制模型^[29]。对 LBAC 的早期研究是在 20 世纪 70 年代^[28],随后产生了一些演进模型^[30-34],如将单向信息流部分放松来实现信息的选择性,或在完整性应用方面进行改进。Benantar 等^[35]比较了 BLP 和 Biba 模型,并描述了它们组合的可能。Obiedkov 等^[36]认为形式概念分析能够以半自动的方式生成

子格,并讨论了如何将两个解决不同的需求的访问控制模型纳入一个模型。Sandhu^[37]指出,LBAC 可以同时应用于机密性和完整性控制。文献[38-39]提出基于格将 BLP 和 Biba 相结合,通过对 BLP 和 Biba 的模型元素和安全公理进行重写,实现了基于格的 BLP 完整性扩展模型,但是未提出对可信主体的安全性约束以及对灵活性的考虑。

基于以上相关研究,本文通过对 Web OS 的深入分析和抽象建模,提出了基于格的多安全策略模型来满足移动政务中的安全需求。

3 移动 Web 操作系统分析

3.1 平台异构性

开源的 Web OS 有:Firefox OS^[40-41],Chrome OS^[42],Tizen^[43],Ubuntu Touch^[44]等。由于各个平台的商业发展策略不同,应用程序的类型也不同,如 FirefoxOS 支持的 3 类 Web 应用,既有本地安装的,也有安装在服务器端的;Tizen 支持混合类型的应用;而 Chrome 和 Ubuntu 只支持远程安装的 Web 应用。这些 Web 应用的工作方式类似于普通网站,但可通过 Web API 与设备硬件进行功能交互。但是这些平台对于应用可使用的权限都是根据应用的类型来分配的。与 Android 系统的相似之处是,这些平台都本地存储应用的清单文件(manifest),并且根据其进行应用安装时和运行时的访问控制。

3.2 安全性分析

在访问控制策略方面,这些平台都基于 Linux 内核,因此文件系统和系统敏感资源的访问控制都基于 LinuxDAC 模型,并且都采用了应用沙箱机制。但是,这些系统都具有一些特别的访问控制策略,且存在不同程度的安全风险。

Firefox OS 应用通过 Web API 调用访问系统资源时,由系统框架层根据应用程序的类型和访问控制列表来检查访问请求。这种访问控制不足以控制特权提升,且可能导致信息泄露。

Tizen 提供了一种简化的强制访问控制内核(Simplified Mandatory Access Control Kernel,SMACK)^[45]作为其强制访问控制机制,它在安装时给每个进程(主体)和资源(客体)一个 10 个字符的 SMACK 标签,将其作为扩展属性。一旦应用程序在安装期间被授予某些权限,这些权限就将成为相应的 SMACK 规则。出于其商业策略,Tizen 采取混合的框架来支持更多的应用类型,如支持 Android 应用,但其缺点是会导致未经授权的访问和管理混淆。

Chrome OS 同样根据 manifest 中声明的权限实现访问控制,但开发人员可以添加更严格的运行时检查。Chrome 将应用程序的本地代码和远程内容隔离,视它们为不同来源,并应用同源策略^[46]。默认情况下,单个 Web API 必须由应用程序显式请求才能激活,其安全性取决于开发人员对每个资源请求的源检查。此外,即使正确执行的检查也可能被绕过。

Ubuntu 提供了应用程序的本地代码和远程代码之间的隔离,并强制实施同源策略。Ubuntu 提供了 3 种 API:Ubuntu 平台 API、W3C API 和 Cordova API,分别对应不同类型的

系统资源。但是对这 3 类 API 的管控不够严格,如将 Cordova API 公开给所有 Web 源代码,也就是允许不可信的远程 Web 代码访问摄像头、麦克风等敏感资源。

这些 Web OS 平台与其他移动操作系统一样,面临的攻击不仅来自互联网,还可能来自系统内部。作为终端系统的访问控制模型,本文重点关注对系统内部安全威胁的控制,这类攻击包括旨在执行未经授权的特权代码的攻击、修改特权代码二进制文件或提升自己的应用程序的权限,以及相同类型应用之间的信息泄漏。

在面向高安全级移动办公的瘦终端应用背景下,Web 应用具有云端安装、云存储以及集中管理的优点,因此本文从 Web 应用的特点出发,对通用 Web OS 架构进行抽象建模,并利用强制访问控制模型,改进其现有的访问控制策略。

4 WLB 模型设计

WLB 模型的主要目标是在通用 Web OS 上实现机密性和完整性的保护。在高安全级别系统中,还需要在每个用户之间进行隔离,且对于不同的数据项和文件系统有不同的级别,这些级别应被标记以区分彼此之间的完整性。

4.1 BLP 与 Biba 信息流

BLP 中的强制访问控制是出于机密性考虑的,Biba 基于完整性的考虑提出了类似的访问控制。BLP 中的读意味着从客体到主体的信息流,也就是信息由客体流向主体,要求主体安全级支配客体安全级;写意味着从主体到客体的信息流,也就是信息由主体流向客体,要求客体安全级支配主体当前安全级。以由 Top Secret (TS), Secret (S), Classified (C) 和 Unclassified (U) 组成的安全级集合为例,支配关系和信息流走向如图 1 所示。

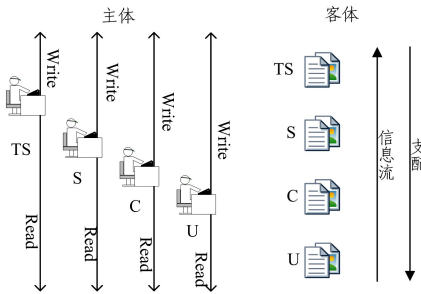


图 1 BLP 模型中的信息流
Fig. 1 Information flow in BLP model

Biba 通过防止低完整级客体中存储的信息流向更高级的客体或完整级不可比的客体来保护系统的完整性。例如,完整级为 Crucial (C)、Important (I) 和 Unknown (U) 时,信息流的流向如图 2 所示。从图 1 和图 2 可以看出,机密性策略允许信息流向上流动,而完整性策略允许信息流向下流动,但是它们的支配关系是在同一个方向。尽管 BLP 模型和 Biba 模型的表现形式不同,但本质上都可以看作是安全标记(格)的信息流模型^[13],它们遵循的是一种单向的信息流动策略,因此可以将这两个格叠加起来形成一个统一的格以保护系统的机密性和完整性。

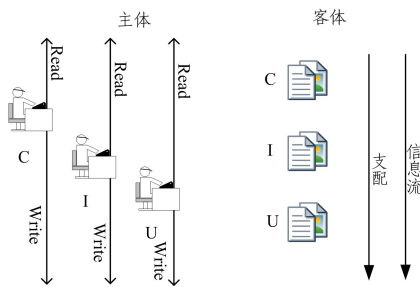


图 2 Biba 模型中的信息流
Fig. 2 Information flow in Biba model

4.2 Web OS 抽象建模

移动设备的资源可分为硬件、软件和数据。操作系统作为设备资源的管理者,通过管理各种操作过程来实现对设备的管理。任一操作过程都有如下 3 个要素:操作、操作者(操作的执行者)和操作对象。通常,操作者即主体(记为 s_i),一般是活动的进程;操作对象一般是数据、文件等,也可能是另一个进程,操作对象称为客体(记为 o_j)。将所有主体的集合记为 S ,所有操作的集合记为 A ,所有客体的集合记为 O ,则操作过程是定义在 $S \times A \times O$ 上的关系。

主体集合 $S = \{s_1, s_2, \dots, s_n\}$, s_i 表示第 i 个主体。在 Web OS 中,活动主体通常是执行程序的进程,由另一进程或在用户登录时由系统创建。在 LBAC 类模型中,可信主体是不受 * 规则约束的主体^[25],用 S_T 表示。基于上文对 Web OS 的分析,将移动瘦终端的应用程序分为两类:本地应用和 Web 应用,因为采用云存储架构,本地应用仅有系统级应用,而 Web 应用根据其存储情况分为本地和远程,并且具有不同的安全级和权限。因此,主体集合 $S = \{S_w, S_l, S_c\}$,分别代表远程代码或它们相应的操作、Web 应用的本地代码或它们相应的操作、系统应用或系统服务。

客体集合 $O = \{o_1, o_2, \dots, o_m\}$,所有文件、目录、特殊文件、共享内存、消息、信号量、管道和进程可以作为客体。其安全级等于创建它的进程的安全级。因此,通过进程的执行产生客体之间的信息流,从而实现安全类之间的信息流。相应地,将存储空间划分为 $\{O_u, O_p, O_s, O_v\}$,客体安全级对应系统存储空间的不同分区,从而实现客体域间的隔离。其中, O_u 代表一般用户空间域, O_p 代表受信任用户空间域, O_s 代表系统空间域, O_v 代表病毒保护域。

访问模式集合 $A = \{e, r, a, w\}$,代表系统的基本操作类型: r 只读(读出数据,但不做其他操作)、 a 添加(不读,只在客体数据尾添加,即只写)、 w 读写、 e 执行。

机密性标记集合 $C = \{C_1, C_2, \dots, C_q\}$, $C_1 > C_2 > \dots > C_q$ 。
完整性标记集合 $I = \{I_1, I_2, \dots, I_p\}$, $I_1 < I_2 < \dots < I_p$ 。
扩展属性标记集合 $K = \{K_1, K_2, \dots, K_r\}$,用来指定用户所属部门以及部门之间的从属关系。

安全级集合 $L = C \times I \times K = \{L_1, L_2, \dots, L_n\}$,对于主体 s_i ,其安全级 L_{s_i} 包含了机密性标记、完整性标记和扩展属性。

特权操作集合 $S_t = \{u_1, u_2, u_3, \dots, u_n\}$,其中 u_i 表示某个系统特权操作。

特权映射函数 $RA(set)$,主体在被创建时都被授予一个

安全级,根据该安全级将主体集合映射到不同的权限组, $RA(S_i) = \{U_1, U_2, \dots, U_m\}$, U_k 是具有某类特权的特权用户。

访问矩阵 M , M_{ij} 表示主体 s_i 对客体 o_j 具有的访问类型。

4.3 安全模型定义

定义 WLBB 模型为: $\langle O, S, L, \oplus, \rightarrow \rangle$, 其中 O, S 分别是客体和主体的有限集, L 是安全类的有限集。类运算符 $\oplus$ 是一个满足结合律和交换律的二进制运算符, 对于任意两个操作数的类, 由 $\oplus$ 指定它们之间任意二进制函数产生的结果操作数所属的类。流向关系 $\rightarrow$ 指定了两个安全类之间的信息流动。这个模型被认为是安全的, 当且仅当任何操作的执行产生的信息流的状态与 $\rightarrow$ 关系预定义的流策略一致。

WLBB 模型的安全策略 $\langle L, \oplus, \rightarrow \rangle$ 可以简单表述为: 模型是安全的, 当且仅当一个操作序列的执行不会产生违反 $\rightarrow$ 关系所规定的信息流。基于以下假设, 安全策略形成了一个有限格。

- (1) 安全标记集合 L 是有限的;
- (2) “能够流向”关系 $\rightarrow$ 在 L 上是偏序的;
- (3) 根据 $\rightarrow$, L 具有下界;
- (4) $\oplus$ 操作定义了最小上界。

WLBB 安全标记 L 满足这 4 个条件, 那么 L 形成一个格。 L 扩展了 Sandhu 和 Denning 定义的混合格, 既结合了机密性和完整性, 又可根据实际系统定义特殊安全因子, 因而具有更好的可用性。

4.4 访问控制规则

利用 BLP 和 Biba 的核心思想扩充 DAC, 用 MAC 实施信息流控制。在实际系统中, DAC 和 MAC 通常同时使用, 其中 MAC 仅在满足 DAC (如访问矩阵 M) 的检查之后才执行。以往对信息流模型描述^[47-49] 难于理解, 因此本文采用更接近于状态机模型的形式化表达。

规则 1 (自主安全规则) $s_i \in S, o_j \in O, s_i$ 能够以 $\underline{x}$ 方式访问 o_j , 当且仅当 $\underline{x} \in M_{ij}$ 。

规则 2 (读规则) $s_i \in S, o_j \in O, s_i$ 能够读 o_j , 当且仅当 $L(s_i) \geq L(o_j) \Leftrightarrow o_j \rightarrow s_i$ 。

规则 3 (自由写规则) $s_i \in S, o_j \in O, s_i$ 能够写 o_j , 当且仅当 $L(s_i) \leq L(o_j) \Leftrightarrow s_i \rightarrow o_j$ 。

规则 4 (严格写规则) $s_i \in S, o_j \in O, s_i$ 能够写 o_j , 当且仅当 $L(s_i) = L(o_j) \Leftrightarrow s_i \rightarrow o_j$ 。

规则 5 (域间隔离) 对于所有的主体和客体, 当前访问状态 $(s_i, o_j, \underline{x})$ 是合法的, 则需要满足:

$$o_j \in O_u \text{ 且 } s_i \in S_l, \text{ 那么 } x \in \{a, w, r, e\} \quad (1)$$

$$o_j \in O_u \text{ 且 } s_i \in S_w, \text{ 那么 } x = e \quad (2)$$

$$o_j \in O_u \cup O_s \text{ 且 } s_i \in S_T, \text{ 那么 } x \in \{a, w, r, e\} \quad (3)$$

$$o_j \in O_s \text{ 且 } s_i \in S_w \cup S_l, \text{ 那么 } x = e \quad (4)$$

$$o_j \in O_v, \text{ 如果 } s_i = U_n, n \text{ 为特定值, 那么 } x \in \{a, w\} \quad (5)$$

$$o_j \in O_s, \text{ 如果 } s_i = U_m, m \text{ 为特定值, 那么 } x \in \{a, w\} \quad (6)$$

规则 1 给出了自主访问控制首先需要满足的要求, 规则 2—规则 4 给出了强制访问控制需要满足的基本要求。规则 5 对不同类型的主体所能访问的客体域进行了划分, 实现主体与客体的隔离 (如用户空间和系统空间的隔离), 使得用户

的操作无法影响内核的安全。对主体类型的划分, 与 Web 操作系统中存在的类型相对应, 以实现系统中不同类型应用的隔离。WLBB 写策略用于防止向下写以防止信息流向流动, 但只适用于非可信主体进行, 还需对可信主体进行进一步约束, 因此提出可信主体最小权限规则。

规则 6 (可信主体最小权限) 对于特权操作 $S_i = u_1 \cup u_2 \cup u_3 \cup \dots \cup u_n$, 由角色映射函数 RA 将它们映射到不同的角色中, 并把这些“角色”赋予系统中的指定用户, 用 $U_1, U_2, \dots, U_m$ 表示, 即 $RA(u_i) = U_i$ 。这些特权用户共同完成系统的特权操作, 每个特权用户 U_i 只有完成其工作所需的最小特权, 而不能独自控制整个系统, 即:

$$\begin{aligned} \exists S_i = u_1 \cup u_2 \cup u_3 \cup \dots \cup u_n \Rightarrow RA(S_i) = \{U_1, U_2, \dots, U_n\} \\ \forall U_k \rightarrow P(U_k) \subset S_i \Leftrightarrow P(U_k) = \min(\sum u_j \mid 1 \leq j \leq n), 1 \leq i \leq m \end{aligned}$$

Sandhu 的 LBAC 模型中信息只能沿一个方向流动, 而在实际系统中存在两个方向的场景, 如共享对象。本文定义了特殊的可信主体 α 作为机密性审查员或完整性审查员, 它在特定条件下改变客体的机密性或完整性等级。

规则 7 令 α 为机密性审查员, $\alpha \in S_T, \exists s_i \in S_T, \alpha$ 改变客体 o_j 的安全级后, s_i 可以 $\underline{x}$ 方式访问 o_j , 这一操作记作 $\rho(\alpha, s_i, o_j, \underline{x})$, 有:

$$\rho(\alpha, s_i, o_j, \underline{x}) = \begin{cases} f_o(o_j) = f_s(s_i), M = M_{ij} \cup r; \\ \text{iff } [f_s(s_i) < f_o(o_j)] \text{ or } [i(o_j) < i(s_i)] \\ f_o(o_j) = f_s(s_i), M = M_{ij} \cup w; \\ \text{iff } [f_s(s_i) > f_o(o_j)] \text{ or } [i(o_j) > i(s_i)] \end{cases}$$

其中, 机密级函数 $f = (f_s, f_c, f_o)$, f_s 表示主体最大机密级函数, f_c 表示主体当前机密级函数, f_o 表示客体机密级函数。 $i(S)$ 和 $i(O)$ 分别表示主体和客体的完整性级别函数。

规则 8 α 为完整性审查员, $\alpha \in S_T, \exists s_i \in S_T, \alpha$ 改变客体 o_j 的完整级后, s_i 可以 $\underline{x}$ 方式访问 o_j , 这一操作记作 $\varphi(\alpha, s_i, o_j, \underline{x})$, 有:

$$\varphi(\alpha, s_i, o_j, \underline{x}) = \begin{cases} i(o_j) = i(s_i), M = M_{ij} \cup r; \\ \text{iff } [f_s(s_i) < f_o(o_j)] \text{ or } [i(o_j) < i(s_i)] \\ i(o_j) = i(s_i), M = M_{ij} \cup w; \\ \text{iff } [f_s(s_i) > f_o(o_j)] \text{ or } [i(o_j) > i(s_i)] \end{cases}$$

以完整性检查为例, α 通过给主体一个临时操作权限来改变客体的机密性和完整性级别。如图 3 所示, 具有高机密级高完整级的主体 S 请求对低机密级低完整级的客体 O 进行读访问, 根据规则 2 不允许该访问。这里通过提升 O 的副本 O' 的完整级, 使 S 在缓冲器中能够读取 O 的内容。这种方式提高了系统的可用性, 且操作仅限于特殊可信主体, 该访问实际上是访问该客体的一个实例, 不影响客体本身的完整性。

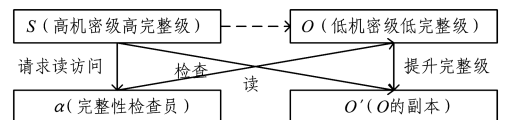


图 3 完整性检查

Fig. 3 Integrity check

4.5 模型分析

面向移动瘦终端操作系统的模型,以机密性为首要考虑因素,因此 WLBB 格的描述以构造与 BLP 格等价的方式实现。当在实际应用中只考虑机密性和完整性标记时,类别集 K 被视为一个扩展的安全因素, WLBB 可以简化为 Sandhu 的方法,令 $L=F\times I, F_H, F_L, I_H, I_L$ 分别为集合 F 和集合 I 的最小上界和最大下界,格中主体与客体的访问方式如表 1 所列。

表 1 L' 主体和客体的访问控制

Table 1 Access control between subjects and objects in L'

M	$F_L I_L$	$F_L I_H$	$F_H I_L$	$F_H I_H$
$F_L I_L$	rw	r	w	$\emptyset$
$F_L I_H$	w	rw	w	w
$F_H I_L$	r	r	rw	r
$F_H I_H$	$\emptyset$	r	w	rw

由于系统中的信息流包含显式的信息流和隐式的信息流,显式信息流是在安全策略的规定下产生的所有信息流;相反地,隐式信息流是间接的信息流,可能导致信息泄露,例如低安全级用户通过外部观测来推断高安全级用户的行为(进而可泄露信息)。对于信息流模型,系统是安全的当且仅当信息流在安全策略的规定下能够保持系统的安全状态。结合 BLP 模型的状态转换规则, WLBB 重新定义了只读、只写、读写等状态转换规则。而强制访问控制策略的实施可能存在隐蔽通道。为解决隐蔽信道或隐式信息流问题,以只读规则(T_1)为例, WLBB 在状态转换规则 $T(s_i, o_j, \underline{x})$ 中增加了对隐式的安全信息流的判断: $T_1(s_i, o_j, r) = \text{true} \Leftrightarrow o_j \rightarrow s_i$, 即由其引起的状态转换导致系统状态是安全的,需要满足:

$$T_1(s_i, o_j, r) = \begin{cases} (? , v), & \text{interdom}(s_i, o_j) = \text{false} \\ \text{yes}, & [L(s_i) < \triangleright L(o_j)] \& [L(s_i) \geq L(\text{parent}(o_j))] \\ \text{yes}, & [(r \in M_{ij}) \& (L(s_i) \geq L(o_j))] \text{ or } (s_i \in S_T) \\ \text{no}, & \text{else} \end{cases}$$

其中, $\text{interdom}(s_i, o_j)$ 用于检查主体和客体是否满足域间隔离规则。当主体和客体的安全级不可比时,如果存在主体到客体父结点的信息流,则仍可能通过其父结点,产生对该客体隐式的信息流。因此,在状态转换规则中增加对这类信息流的判断,可以解决隐蔽通道问题。

5 验证

Isabelle/HOL^[50] 是一种支持高阶逻辑 (Higher Order Logic, HOL) 的交互式定理证明器,支持形式化数学公式的验证,并提供了证明工具完成对数学公式的逻辑演算。若要验证模型的正确性和一致性,需要证明系统的初始状态是安全状态,并且系统任一状态迁移后的状态仍是安全状态,而系统状态是安全的就认为该状态满足模型策略的规定。操作系统安全模型的证明可以简化为在操作 p 完成后的系统状态满足安全策略^[51]。本文利用 Isabelle 2016.1-x64 的规范化证明工具,在 Win10 环境下,采用更适用于复杂的命题的半自动证明方法,对 WLBB 的正确性进行验证。

首先,定义模型的基本元素、请求类型、安全标记等,例如使用 `typedcl` 定义主体和客体,使用 `datatype` 定义请求类型和访问模式,用 `record` 和 `Constdefs` 定义安全级 L 及其关系。其次,定义系统安全状态、系统初始状态和规则。系统初始状态对主客体的安全级、层次结构、访问矩阵等进行赋值,代码如下:

1. `types fs="Subject⇒SecurityLevel" // security level on subject`
2. `Lmin="Object⇒SecurityLevel"`
3. `Lmax="Object⇒SecurityLevel"`
4. `Hierarchy="(att×string,att,Object) env"`
5. `record States=Subjects::"Subject set"`
6. `Objects::"Object set"`
7. `CAT::"AccessTriple set"`
8. `AM::"AccessTriple set"`
9. `f_s::fs`
10. `L_min::Lmin`
11. `L_max::Lmax`
12. `Hier::Hierarchy`

然后,依次对规则 1—规则 3 采用自动化验证的方法验证其逻辑一致性。

最后,应用半自动化验证方法,对规则 4—规则 6 进行半自动化验证,显式地指明从哪些已知条件、根据什么规则进行推导能够得到需要的结论。若仍不成功,则需要重新检查定义部分的正确性。验证方法如算法 1 所示。

算法 1 Verifyprocess

Input: 初始状态: 一个系统状态序列, `acc_req`: 主体访问请求

output: 当前系统状态, 系统是否保持安全状态

Method: `induction(initial state)`: 检查系统初始状态

`auto(sub, obj, acc_req)`: 自动分析过程

`semi-auto(sub, obj, acc_req)`: 半自动分析过程

Subroutine: `auto(sub, obj, acc_req)`

`semi-auto(sub, obj, acc_req)`

Parameters:

初始状态序列, 包括请求主体、安全级、被请求客体、当前主体集合、当前客体集合、访问矩阵、层次等;

`sub_i`: 发出访问请求的主体

`acc_req`: 主体请求的访问模式

`obj`: 访问客体

Method:

Step1 应用 `induction(state_0)`, 确定初始状态是否是安全的;

`yes`: 返回 `true`;

`no`: 跳转至 step 2;

Step2 重新定义系统安全状态;

for theorem 1 to 6

应用 `auto(sub, obj, acc_req)`, 确定访问请求是否满足规则;

`yes`: 验证下一个规则;

`no`: 转向 `semi-auto process`;

Step3 Assume cons: 检查一致性, 如果都满足, 则返回 `true`, 跳出循环。

结束语 本文首先分析了开源 Web 操作系统的安全问题, 这些系统具有不同的访问控制策略和应用类型。随后, 本文面向基于 Web OS 的移动瘦终端, 研究了机密性模型 BLP

和完整性模型 Biba,利用这些模型在模型设计阶段提高了 Web OS 的安全性。这两个模型在形式上是对偶的,这使得将它们组合起来成为可能。本文采用了基于格的方法来组合这两个模型,因为在数学上,这两个模型可以被看作基于格的信息流模型。Biba 严格的完整性策略没有给出自主访问控制策略,而 Biba 模型的基本操作只有修改、查看和调用,对于特定系统来说难以提供操作指导,因此本文在这些方面做出了改进。最后,Sandhu 的 LBAC 模型未能考虑可信主体,且只允许信息单向流动,但在实际系统中,存在信息共享等需要信息的双向流动。为了提高模型的可用性和灵活性,本文定义了一个特殊的信任主体 α ,它可以在某些条件下改变客体的机密性和完整性等级。

基于格的方法是我们认识和探索计算机安全的一个重要方法,但它并没有提供信息流策略的完整解决方案。例如,存在并发性问题,即客体必须被保护以免被相同级别的进程并发写入,因此对并发修改时的保护将是我们未来的工作。类似于 BLP 模型,WLBB 中的安全类遵循平静原则,这意味着它们一旦分配就不能改变,在未来工作中将研究动态安全策略问题。

参 考 文 献

[1] Wiki. Thin client[OL].[2016-06-21].https://en.wikipedia.org/wiki/Thin_client.

[2] Thin and Zero Clients Meet Military Security Environmental Requirements[OL]. [2014-10-30]. <http://eecatalog.com/military/2014/10/30/thin-and-zero-clients-meet-military-security-environmental-requirements>.

[3] BERRYMAN A,CALYAM P,HONIGFORD M,et al. VDBench:A Benchmarking Toolkit for Thin-Client Based Virtual Desktop Environments[C]//IEEE Second International Conference on Cloud Computing Technology and Science. IEEE,2010:480-487.

[4] GEORGIEV M,JANA S,SHMATIKOV V. Rethinking Security of Web-Based System Applications[C]//International Conference on World Wide Web. International World Wide Web Conferences Steering Committee,2015:366-376.

[5] DEFREEZ D,SHASTRY B,CHEN H,et al. A first look at Firefox OS security[C]//Proceedings of the Third Workshop on Mobile Security Technologies(IEEE MoST). 2014.

[6] BAE S G,CHO H,LIM I,et al. SAFEWAPI: web API misuse detector for web applications[C]//The ACM Sigsoft International Symposium. ACM,2014:507-517.

[7] CHEN B,MING W S,HUANG Y L. An Anomaly Detection Module for Firefox OS[C]//IEEE Eighth International Conference on Software Security and Reliability-Companion. IEEE,2014:176-184.

[8] PIEKARSKA M,SHASTRY B,BORGAONKAR R. What Does the Fox Say? On the Security Architecture of Firefox OS[C]//Ninth International Conference on Availability, Reliability and Security. IEEE Computer Society,2014:172-177.

[9] HUANG L S,MOSHCHUK A,WANG H J,et al. Clickjacking:

attacks and defenses[C]//Usenix Conference on Security Symposium. USENIX Association,2012:22.

[10] WEST W,PULIMOOD S M. Analysis of privacy and security in HTML5 web storage[J]. Journal of Computing Sciences in Colleges,2011,27(3):80-87.

[11] HEIDERICH M,SCHWENK J,FROSCH T,et al. mXSS attacks: attacking well-secured web-applications by using inner HTML mutations[M]. ACM,2013:777-788.

[12] BOJINOV H,BURSZTEIN E,DAN B. XCS:cross channel scripting and its impact on web applications[C]//ACM Conference on Computer and Communications Security(CCS 2009). Chicago, Illinois, USA, DBLP, 2009:420-431.

[13] DANISEVSKIS J,PIEKARSKA M,SEIFERT J P. Dark Side of the Shader: Mobile GPU-Aided Malware Delivery[M]//Information Security and Cryptology(ICISC 2013). Springer International Publishing,2013:483-495.

[14] MULLINER C,GOLDE N,SEIFERT J P. Sms of death: From analyzing to attacking mobile phones on a large scale[C]//Proceedings of the 20th USENIX Conference on Security. 2011:24.

[15] MULLINER C,VIGNA G. Vulnerability analysis of mms user agents[C]//Proceedings of the 22nd Annual Computer Security Applications Conference. 2006:77-88.

[16] AKHAWA D,LI F,HE W,et al. Data-Confined HTML5 Applications[M]//Computer Security -ESORICS 2013. Springer Berlin Heidelberg,2013:736-754.

[17] AKHAWA D,SAXENA P,AND SONG D. Privilege separation in HTML5 applications[C]//Usenix Conference on Security Symposium,USENIX Association. 2012:23-23.

[18] ZHU D,YANG Y,JIN H,et al. Application of Modified BLP Model on Mobile Web Operating System[C]//2016 IEEE Trustcom/BigDataSE/ISPA. 2017:1818-1824.

[19] BELL D E. Secure computer systems:a refinement of the mathematical model[M]. NTIS,1974.

[20] LIU W Q,QIN S H,LIU H F. Design of a Modified BLP Security Model and Its Application to SecLinux[J]. Journal of Software,2002,13(4):567-573. (in Chinese)
刘文清,卿斯汉,刘海峰. 一个修改 BLP 安全模型的设计及在 SecLinux 上的应用[J]. 软件学报,2002,13(4):567-573.

[21] XU L,TAN H. Formal Description and Automated Verification of improved BLP Model [J]. Computer Engineering,2013,39(12):130-135. (in Chinese)
徐亮,谭煌. BLP 改进模型的形式化描述及自动化验证[J]. 计算机工程,2013,39(12):130-135.

[22] BIBA K J. Integrity Considerations for Secure Computer Systems[R]. MITRE Technical Report,1975.

[23] LIU Y M,DONG Q K,LI X P. Study on enhancing integrity for BLP model[J]. Journal on Communications,2010,31(2):100-106. (in Chinese)
刘彦明,董庆宽,李小平. BLP 模型的完整性增强研究[J]. 通信学报,2010,31(2):100-106.

[24] ZHANG J,ZHOU Z,LI J,et al. Confidentiality and integrity dynamic union model based on MLS policy[J]. Computer Engineering and Applications,2008,44(12):19-21. (in Chinese)
张俊,周正,李建,等. 基于 MLS 策略的机密性和完整性动态统一模型[J]. 计算机工程与应用,2008,44(12):19-21.

[25] LIU B,CHEN S H,DENG J S. Survey of Bell-LaPadula model [J]. Application Research of Computers,2013,30(3):656-660. (in Chinese)
刘波,陈曙晖,邓劲生. Bell-LaPadula 模型研究综述[J]. 计算机应用研究,2013,30(3):656-660.

[26] KARGER P A,AUSTEL V R,TOLL D C. A new mandatory security policy combining secrecy and integrity[R]. IBM Research Report,2000.

[27] YUAN C Y,XU J F,ZHU C G. A Trusted recovery Model for Assurance of Integrity Policy Validity[J]. Journal of Computer Research and Development,2014,51(2):360-372. (in Chinese)
袁春阳,许俊峰,朱春鸽. 一种可确保完整性策略有效性的可信恢复模型[J]. 计算机研究与发展,2014,51(2):360-372.

[28] DENNING D E. A lattice model of secure information flow[J]. Communications of the ACM,1976,19(5):236-243.

[29] SANDHU R S. Lattice-based access control models[J]. Computer,1993,26(11):9-19.

[30] BELL D E. Secure computer systems: A network interpretation [C]// Third Annual Computer Security Application Conference (ACSAC). 1987:32-39.

[31] LEE T M P. Using Mandatory Integrity to Enforce “Commercial” Security[C]// IEEE Conference on Security and Privacy (IEEE S&P). IEEE Computer Society,1988:140-146.

[32] SCHOCKLEY W R. Implementing the Clark-Wilson integrity policy using current technology[C]// NIST National Computer Security Conference. 1988:29-37.

[33] LIPNER S B. Security and Source Code Access : Issues and Realities[C]// IEEE Conference on Security and Privacy (IEEE S&P 2000). 2000:124-125.

[34] GUERRA M,SANTOS N,MIRANDA J,et al. Access Control Systems:Security,Identity Management and Trust Models[M]. Springer Publishing Company,Incorporated. 2010.

[35] BOURDIER T,CIRSTEA H,MOREAU P E. Analysis of lattice-based access control policies using rewriting systems and tom [C]//Luxembourg Day on Security & Reliability. 2009:1-8.

[36] OBIEDKOV S,KOURIE D G,ELOFF J H P. On Lattices in Access Control Models. Conceptual Structures: Inspiration and Application[C]// International Conference on Conceptual Structures (Proceedings ICCS 2006). 2006.

[37] SANDHU R. Role hierarchies and constraints for lattice-based access controls[C]// European Symposium on Research in Computer Security: Computer Security. Springer-Verlag,1996,1146: 65-79.

[38] MA X Q,HUANG Y. Trusted computing model based on lattice [J]. Journal on Communications,2010,31(8A):105-110. (in Chinese)
马新强,黄羿. 基于格的可信计算模型[J]. 通信学报,2010,31(8A):105-110.

[39] SHEN Y,SHEN C X. BLP Integrity Expansion Model on Lattice [J]. Journal of Beijing University of Technology,2013,39(3):402-406. (in Chinese)
沈琰,沈昌祥. 基于格的 BLP 完整性扩展模型[J]. 北京工业大学学报,2013,39(3):402-406.

[40] Mozilla. Firefox OS 架构 [OL]. [2016-12-02]. https://developer.mozilla.org/zh-CN/Firefox_OS/Platform/Architecture.

[41] Mozilla. Firefox OS security overview [OL]. [2016-12-02]. https://developer.mozilla.org/en-US/Firefox_OS/Security/Security_model.

[42] Google. Chrome OS [OL]. [2016-04-16]. https://en.wikipedia.org/wiki/Chrome_OS.

[43] Wiki. Tizen [OL]. [2017-03-10]. <https://zh.wikipedia.org/zh-cn/Tizen>.

[44] Ubuntu. Ubuntu Touch [OL]. [2017-03-10]. <https://developer.ubuntu.com/en/phone/devices/porting-new-device/>.

[45] Wiki. TizenSecurity [OL]. [2017-03-11]. https://wiki.tizen.org/wiki/Security#All_3_X_security_pages.

[46] Google. Permissions in Chrome apps and extensions [OL]. [2017-03-11]. https://developer.chrome.com/apps/declare_permissions.

[47] WANG C. Access control model based on indirect information flows restrains [J]. Computer Engineering and Design,2012,33(7):2521-2525. (in Chinese)
王超. 基于间接信息流约束的访问控制模型[J]. 计算机工程与设计,2012,33(7):2521-2525.

[48] WANG Y,LI J,HE J H. A selinux strategy analysis model based on information flow[J]. Computer Applications and Software,2011,28(4):284-288. (in Chinese)
王燕,李佳,何建波. 基于信息流的 SELinux 策略分析模型[J]. 计算机应用与软件,2011,28(4):284-288.

[49] LIU Y H,SHEN C X. An Information Security Function and Application Model [J]. Journal of Computer-aided Design & Computer Graphics,2005,17(12):2734-2738. (in Chinese)
刘益和,沈昌祥. 一个信息安全函数及应用模型[J]. 计算机辅助设计与图形学学报,2005,17(12):2734-2738.

[50] TOBIAS N,WENZEL M,PAULSON L C. Isabelle/HOL:a proof assistant for higher-order logic [M]. Springer-Verlag, 2013.

[51] CHEN K,HE Y P. Application of Isabelle in analyzing secure operating system state-machine models[J]. Computer Engineering and Design,2008,29(3):580-582. (in Chinese)
陈坤,贺也平. Isabelle 在分析安全操作系统状态机模型中的应用[J]. 计算机工程与设计,2008,29(3):580-582.