多域环境下工作流访问控制时序策略组合研究

唐 卓 刘国华 李肯立
(湖南大学计算机与通信学院计算机系 长沙 410082)

摘 要 多域环境下工作流访问控制策略往往表现为异构策略的时序组合,其基本需求是使访问主体在一定的时间段或者时间周期内具有对客体的访问权限。XACML在描述策略组合时,并没有体现异构策略组合时态约束。根据GTRBAC提出的时态约束种类,定义了相关时态策略并进行了图解说明;并对XACML进行了扩展,引入了相应的时态约束元素。最后,通过实例说明了扩展后的XACML能方便地描述异构的时态策略组合。

关键词 时态约束,策略组合,XACML,工作流

Research on Workflow Access Control Temporal Policy Combine in Multi-domains

TANG Zhuo LIU Guo-hua LI Ken-li
(Dept. of Computer, Institute of Computer and Technology, Hunan University, Changsha 410082, China)

Abstract In multi-domains environment, workflow access control policy is consisted of heterogeneous temporal policies in difference autonomic domains, and its requirement is special subjects can access special objects in perodic time or duration time. While XACML specifies policy combine, it does not contains temporal constraint. Based on the kinds of temporal constraint proposed by GTRBAC, this paper defined temporal constraints policies and illustrated by figures. It is extended from XACML by introducing correspond temporal constriant elements. Finally, this paper illustrated that the extended XACML can describe heterogeneous temporal policy combine conveniently through a example.

Keywords Temporal constraint, Policy combine, XACML, Workflow

1 引言

工作流的安全问题一直是工作流领域专家和学者研究的热点之一,而工作流访问控制是工作流安全的基本问题,也是实现一个工作流的必要条件。访问控制[1]就是通过某种途径显式地准许或限制访问能力及范围,从而限制对关键资源的访问,防止非法用户的侵入或者合法用户的不慎操作造成破坏。

随着应用需求的不断增加,越来越多的用户和企业希望获取和使用Internet上海量资源和服务,以实现在多个软硬件系统以及不同信息源之间操作。然而,这些信息源可能分布在异构环境的多个自治域中,给工作流的安全带来了新的挑战。一个工作流由多个子任务组成,子任务可能涉及多个不同的自治域环境,而不同的自治域可能采用不同的计算模式,其安全策略实现机制也不一样。即使是同一计算模式下不同的自治域,其安全策略的数据格式、存储语义、数据语义等也往往是异构的。在多域环境中,为了保证工作流任务的安全执行,工作流访问策略是这些异构策略的时序组合,其基本需求是实现一定访问主体在一定的时间段或者时间周期内对一定客体的访问权限。

很多策略访问控制语言允许一个策略包含很多子策略,而且对于一个请求,策略产生的最终效果是由多个子策略的效果按照一定的规则组合而成的,包括XACML[3],XACL[4],EPAL[5],SPL[6]和防火墙策略语言。其中,XACML提供最灵活的方式,而且应用最为广泛。采用XACML语言描述策略组合时,虽然能用条件元素来描述时态条件,但使用非常繁琐,而且用户操作不友好且不能描述异构策略组合任意一种时态约束。

为了解决以上几个问题,本文对GTRBAC提出的几种时态约束扩展了XACML策略语言,以简单、直观地描述策略组合时态约束。本文第2节介绍相关工作;第3节引入时态约束元素,扩展XACML;第4节进行了实例分析;最后进行总结并展望将来继续进行的工作。

2 相关工作

近年来,工作流访问控制模型成为国内外学者研究的焦点,并且取得重大的突破。他们提出了许多的工作流访问控制模型,大体上可分为扩展的基于角色的访问控制模型、基于任务的访问控制模型、基于角色和任务的访问控制模型、基于团队的访问控制模型、基于规则的访问控制模型、基于状态的访问控制模型、面向服务的访问控制模型7种类型。最为典型的是扩展的基于角色的访问控制模型。

到稿日期:2010-02-05 返修日期:2010-05-20 本文受国家自然科学基金项目(90715029,60603053),中央高校基本科研业务费专项资金(53 1107040053)资助。

唐 卓(1980—),男,博士,讲师,主要研究方向为分布式系统安全,E-mail:190838506@qq.com;刘国华(1983—),男,硕士生,主要研究方向为分布式系统安全;李肯立(1971—),男,博士,教授,博士生导师,主要研究方向为并行与分布计算。

Sandhu 在 1996 年提出了 RBAC 模型族[7]。RBAC 模型使权限与角色相关，用户通过扮演角色来获取相应的权限。2000 年开始，美国国家标准和技术局对于基于角色的访问控制模型(RBAC)作进一步的规范，并提交到国际标准化组织，由此引发了 RBAC 从概念模型到商业实现的快速发展。2003 年，J. Wainer 等人将 RBAC 模型进行扩展，提出了 W-RBAC 模型，使其适用于工作流系统。2007 年，J. Wainer 等人在 W-RBAC 模型的基础上，提出了一个适用于工作流系统的带转授权限的模型[8]，但是这些模型没有完整考虑各种工作流时序约束。James B. D 等人于 2005 年提出的 GTRBAC 模型把角色分为 3 种状态：不可用、可用和激活。根据角色的 3 种状态，文献 [9] 提出了 3 类时态约束：周期性约束、持续性约束和激活约束。GTRBAC 模型完整地考虑了时态约束，但没有考虑工作流特有属性时，而且没有从整体上考虑时态约束。

在工作流访问控制模型发展的同时，策略语言的发展也取得了长足发展。在这些众多的策略描述语言中，应用最为典型的是 XACML。可扩展的访问控制标注语言(eXtensible Access Control Markup Language，XACML)是由 OASIS(Organization for the Advancement of Structured Information Standards)于 2003 年 2 月制定和发布的可扩展标记语言 XML 规范，用于表示 Internet 上的信息访问策略，是应用最为典型的访问策略组合描述语言。XACML 由规则、策略和策略集 3 个元素组成。若一个请求想对某个资源进行特定动作，只有当它满足策略主体、条件以及相关属性时，策略才允许请求对资源执行相关动作。XACML 条件元素在一定程度上可描述策略时态约束，但操作繁琐、不直观，因此，需对 XACML 语言进行改进，从而直观、简易地体现时态安全约束。

针对以上问题，本文的贡献有：

1) 总结 GTRBAC 模型提出的各种时态，从工作流角度定义相对应的时态安全策略；

2) 根据定义的时态安全策略，在 XACML 中引入相对应的时态约束元素，以有效表示策略组合时序约束。

3 多域环境下工作流策略组合时态约束

3.1 时态约束策略

由于持续性约束表述和激活约束表述有相同形式[9]，因此，在语法和语义上，两者也相似。所以，将上面 3 种约束形式总结为两类：周期性时态约束和持续性时态约束。从时态约束出发，定义相对应的策略，即周期性时态策略和持续性时态策略。下面详细说明这两类策略。

3.1.1 周期性时态策略

在 GTRBAC 中，周期性约束被用来精确表述时间间隔，在这段时间间隔内，角色可用或者不可用，用户-角色指派和权限-角色指派可用或不可用。周期性约束的一般表达式为 $(I,P,pr:E)$。图 1 举例说明了周期性约束。

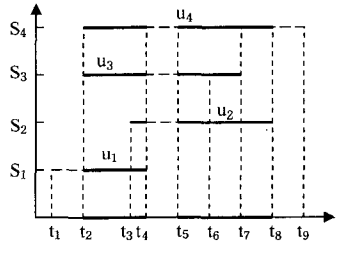

图 1 用户-角色指派周期性约束

从图 1 中可以看出，在时间轴上，两根粗线代表在 (t_2,t_4) 和 (t_5,t_8) 间隔内，角色 r 可用。在时间轴上面的粗线指示在以上时间间隔内，用户可指定该角色。虚线代表用户-角色指派是可用的。但是在某些时间间隔内，由于角色不可用，因此用户-角色指派实际上是不起作用的。例如：对于用户 u_2 在会话 s_2 的情况，在 (t_3,t_8) 时间间隔内，用户-角色指派可用。但仅仅能在 (t_3,t_4) 和 (t_5,t_8) 时间间隔内，用户 u_2 能指派给角色 r。可以看出，如用户 u_2 在会话 s_2 中，利用一个访问控制策略指派一个角色 r，这个访问控制策略实际起作用的时间间隔为 (t_3,t_4) 和 (t_5,t_8)，尽管这个访问控制策略在任何时刻都可用。图 1 对应的周期性时态策略如图 2 所示。

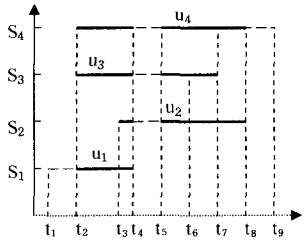

图 2 周期时态策略

3.1.2 持续性时态约束

持续性约束说明角色可用或者指派可用的持续时间。当一个事件发生时，持续时间约束仅仅在指定的持续时间内验证该事件的有效性。持续约束的一般表述式为：$([(I,P)|D],Dx,pr:E)$[9]。根据该表述式，分为 3 种类型的持续约束：

$(I,P,Dx,pr:E)$，$(D,Dx,pr:E)$ 和 $(Dx,pr:E)$

图 3 说明 3 种持续性约束。

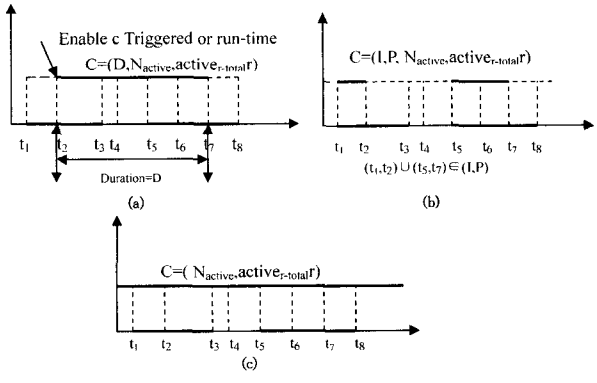

图 3 持续性时态约束

图 3(a)约束 $c=(D,N_{active},Active_{r\text{-}total}r)$ 说明角色 r 在持续时间 D 内可激活，但对于角色 r 最大总共激活持续时间为 N_{active}。在图 3(a)中，时间轴上粗线表明角色 r 可用，即角色 r 仅在时间段 (t_1,t_3) 和 (t_5,t_8) 可用。在时间轴上的粗线表时角色 r 仅在此时间段 (t_2,t_7) 可激活。因此从图中可以看出，角色 r 仅在 (t_2,t_3) 和 (t_5,t_7) 上实际起作用。由此可以看出，选取的访问控制策略最多也只在 (t_2,t_3) 和 (t_5,t_7) 时间间隔内实际起作用，但应考虑对于一个角色的总共激活持续时间 $Duration(t)$ 不超过 N_{active}：$Duration(t)\leqslant N_{active}$。因此，以图 3 中(a)为例，对于策略而言，它实际起作用的时间分成 3 种情况：

1) 当角色 r 的可激活时间剩余总时间 $Re(t)=N_{active}$ 时，策略实际可用时间段为 (t_2,t_3) 和 (t_5,t_7)，该持续时间约束策略图如图 4 所示。

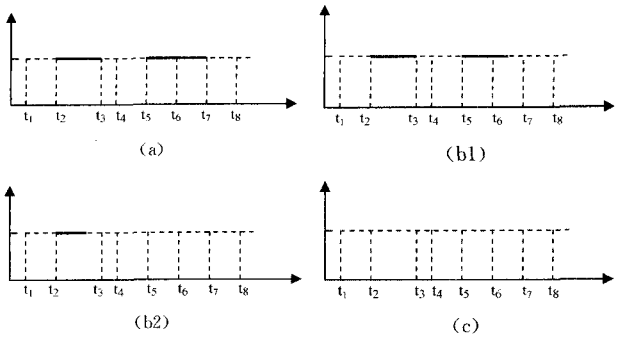

图 4

2)当角色 r 的可激活时间剩余总时间 $0<Re(t)<N_{active}$ 时,策略实际可用时间段则应包含在(t_2,t_3)和(t_5,t_7)内,相应的持续约束策略图有两种,分别如图 4(b1)和图 4(b2)所示。

图 4(b1)表示策略在(t_2,t_3)整个时间间隔可用,但只在(t_5,t_7)部分时间间隔可用。

图 4(b2)表示策略中(t_2,t_3)部分时间间隔可用,在(t_5,t_7)整个时间间隔都不可用。

3)当角色 r 的可激活剩余总时间 $Re(t)\leqslant 0$ 时,说明策略实际可用时间段为 0,相应的持续约束策略图如图 4(c)所示。

图 4(c)表示策略实际可用时间已经用完。

利用相应的方法也可以画出其它相应的持续约束策略图,由于篇幅限制就不再一一画出。

3.2 扩展 XACML 语言

在上一小节,我们讨论了 GTRBAC 模型中周期性约束和持续性约束,相应定义了周期性时态策略和持续性时态策略,并且用图形举例说明了部分的情况。在这一小节中,我们将根据前面定义的周期性时态策略和持续性时态策略,提取相应特征,扩展 XACML,从而直观且简单地描述具有相应时态约束的策略。

在 GTRBAC 模型中,时态表达式的一般形式为:([begin,end],P)。[begin,end]代表一个时间间隔,begin 代表下限,end 代表上限。文献[9]用日历来表示 begin 和 end。日历由时、天、周、月、年 4 个基本单位组成。P 是一个周期表达式:$P=\sum_{i=1}^{n}Oi.Ci\triangleright x.Cd$。XACML 中描述策略 P 时采用 4 个元素:目标、规则组合算法、规则和义务。其中规则有目标、效果和条件。当一个请求匹配规则中有相应条件时,该策略才能产生相对应的效果。为了保持与 XACML 语言的兼容性,只扩展条件标签来描述策略中的时态约束。接下来分别介绍如何扩展 XACML 来描述周期性时态约束和持续性时态约束。

3.2.1 周期性时态策略

从以上讨论可知,周期性时态策略在时态上仅依赖于时间间隔的上限与下限,所以只需在 XACML 中增加如下标签:〈Role〉,〈Perodic_constraint〉,〈Begin〉与〈Begin_value〉和〈End〉与〈End_value〉。其中〈Perodic_constraint〉代表周期性时态约束策略元素开始标签,相对应结束标签为〈/Perodic_constraint〉,以区别持续性时态约束元素。〈Begin〉与〈End〉相对应为周期时态约束策略实际可用时间间隔下限元素和时间间隔上限元素开始标签,结束标签为〈/Begin〉与〈/End〉。一般形式如下:

```
〈Condition〉
  〈Apply〉
    〈Role 属性〉
      〈Perodic_constraint〉
        〈Begin 属性〉
            〈Begin_value 属性〉
                /——下限值——/
            〈/Begin_value〉
        〈/Begin〉
        〈End 属性〉
            〈End_value 属性〉
            /——上限值——/
        〈/End_value〉
        〈/End〉
        …
      〈/Perodic_constraint〉
    〈Role〉
  〈/Apply〉
〈/Condition〉
```

以上定义的标签可出现,也可以不出现。在〈Perodic_constraint〉标签对内,可以出现 $N(N\geqslant 0)$对〈Begin〉与〈End〉标签,〈Begin〉标签与〈End〉标签必须成对出现。

(1) 元素〈Role〉

该元素代表一个角色,有一个标识属性:role_ID。有〈Perodic_constraint〉和〈Duration_constraint〉两个子元素。

(2) 元素〈Perodic_constraint〉

〈Perodic_constraint〉标签代表周期性时态元素,在一个〈Role〉元素中,最多出现 $N(0\leqslant N\leqslant 1)$对这样的标记。当该元素出现零次时,代表该策略没有周期性时态约束。元素〈Perodic_constraint〉没有属性,有〈Begin〉和〈End〉两个子元素。

(3) 元素〈Begin〉

〈Begin〉标签代表周期性约束时间间隔下限,在一个策略中,可出现 $N(N\geqslant 0)$次。该标签有一个属性 begin_ID,为了区别其它下限标签。该标签有一个子元素〈Begin_value〉。

(4) 元素〈Begin_value〉

〈Begin_value〉 标签中内容为周期性时态约束下限值。该标签有一个属性 dataType,表示求该值类型。在该子元素内,值沿用 GTRBAC 中日历表示形式。

(5) 元素〈End〉

〈End〉标签代表周期性约束时间间隔上限,在一个策略中,出现一个〈Begin〉标签,就必须出现相对应的〈End〉标签。该标签有一个属性 end_ID,为了区别其它上限标签,值应等于相应的 Begin_ID 值。该标签有一个子元素〈End_value〉。

(6) 元素〈End_value〉

〈End_value〉 标签中内容为周期性时态约束上限值。该标签有一个属性 dataType,表求该值类型。在上限标签内,如果策略实际可用时间从下限标签值开始后一直可用,那么在上限标签内,值采用∞来表示。

3.2.2 持续性时态策略

在前面的讨论中我们提到,持续时态约束在语法和语义上与激活约束相近,因此,持续时态约束常伴随角色激活事件。文献对持续时态约束进行了详细的分类,具体分类如图 5 所示。

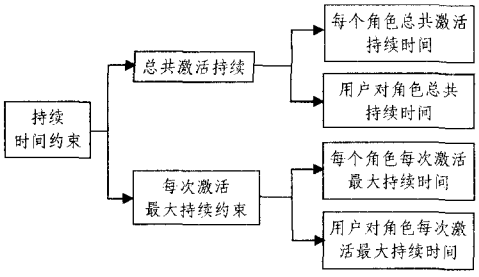

图 5　持续时态约束分类

在前面的讨论中，持续约束表达一般形式为：([(*I*,*P*)|*D*],*Dx*,*pr*:*E*)，相应地分成(*I*,*P*,*Dx*,*pr*:*E*)，(*D*,*Dx*,*pr*:*E*)和(*Dx*,*pr*:*E*) 3 种形式。结合持续约束分类图，推出持续约束策略依赖于策略实际可用时间与可激活总时间间隔 R_{total_r} 或者每次激活最大持续时间 R_{max_r}，因些扩展 XACML 语言描述持续时态约束的一般形式如下：

```
〈Condition〉
        〈Apply〉
          〈Role 属性〉
           〈Duration_constraint 〉
             〈Duration_begin 属性〉
               〈Duration_beginvalue 〉
/——持续约束策略实际起作用时间间隔下限——/
                    〈/Duration_beginvalue〉
                  〈/Duration_begin〉
                  〈Duration_end 属性〉
                    〈Duration_endvalue 〉
/——持续约束策略实际起作用时间间隔上限——/
                     〈/Duration_endvalue〉
                  〈/Duration_end〉
                 〈Duration_total 〉
                   〈total_per_role 〉
                     〈total_per_role_value 〉
/——每个角色总共可激活时间——/
                     〈/total_per_role_value〉
                   〈/total_per_role〉
                 〈total_per_user_role 属性〉
          〈total_per_user_role_value 〉
          /——特定用户对角色总共可激活时间——/
          〈/total_per_user_role_value〉
        〈/total_per_user_role〉
      〈/Duration_total〉
        〈Duration_max 〉
          〈max_per_role 〉
              〈max_per_role_value 〉
          /——对于角色每次激活，最大时间间隔——/
          〈/max_per_role_value〉
          〈/max_per_role〉
          〈max_per_user_role 属性〉
              〈max_per_user_role_value 〉
/——对于特定用户每次激活角色最大时间间隔——/
            〈/max_per_user_role_value〉
          〈/max_per_user_role〉
        〈/Duration_max 〉
      〈/Duration_constraint 〉
    〈/Role〉
  〈/Apply〉
〈/Condition〉
```

在上述标签的应用过程中，必须遵守一定的规则，比如有些标签必须成对出现等。由于有些元素的使用方式与周期性约束元素相似，因此详细介绍几个与周期时态策略差异大的元素：

1) 元素〈total_per_user_role〉

元素〈total_per_user_total〉说明特定用户对角色总共可激活时间类，可出现多次。其有一个属性：user_ID，代表用户标识，有一个子元素〈total_per_user_role_value〉。

2) 元素〈max_per_user_role〉

该元素对应用户激活角色每次最大可持续时间类。其有一个属性：user_ID，代表用户标识，有一个子元素：〈max_per_user_role_value〉。

4　实例分析

本节通过网上购物实例来说明扩展后的 XACML 描述访问控制策略时序约束。网上购物包括 4 个流程任务：T1，网上选择商品；T2，进入网上银行查看自己银行余额；T3，如果余额充足，则进行订货，把货款存入支付宝，如果余额不足，则取消订货；T4，收到货物，上网确认，支付货款。为了网上银行账户的安全，T2 定义了两个角色：R1-银行存折账号，用户-角色指派时间 20:00pm—08:00am；R2-银行卡账号，用户-角色指派时间 8:00am—20:00pm。用户采取一个访问控制策略选取角色 R1 查看自己银行余额，按照以上定义的时态约束策略，该策略是周期性时态策略。接下来利用扩展后的 XACML 描述该策略，由于篇幅限制，只给出其时态约束部分，剩下的可依此类推。

```
〈Condition〉
  〈Apply FunctionId=
"urn:oasis:name:tc:xacml:1.0:
function:data-between"〉
      〈Role role_ID="1"〉
        〈Perodic_constraint〉
          〈Begin begin_ID="100112"〉
            〈Begin_value" dataType="data"〉
                20:00 am
            〈/Begin_value〉
          〈/Begin〉
          〈End end_ID="100112"〉
              〈End_value dataType="data"〉
                08:00 am
              〈/End_value〉
          〈/End〉
        〈/Perodic_constraint〉
      〈/Rolc〉
    〈/Apply〉
〈/Condition〉
```

当各个工作流子任务访问控制策略都确定后，XACML 利用策略组合算法对这些策略进行组合，产生一个整体策略，以保证工作流安全执行。从以上实例可以看出，扩展后的 XACML 直观地体现了策略时态约束。

结束语　多域环境下工作流访问控制策略组合是工作流领域的研究热点之一。目前已产生了不少的研究成果，提出了许多策略组合描述语言。其中，由于 XML 能得到各种浏览器的支持及其平台无关性，基于 XML 的策略描述语言发展最为迅速，其中 XACML 语言已成为许多应用策略描述语

言的事实标准。本文在 XACML 基础上，通过引入时态约束来弥补 XACML 在描述异构策略组合时不能有效描述时态约束的不足。XACML 在描述策略组合时，没有考虑策略之间的安全属性，也无法描述策略组合后的安全属性，如何在 XACML 中引入策略的安全等级将是下一步需要解决的问题。

参 考 文 献

[1] 邓集波，洪帆. 基于任务的访问控制模型[J]. 软件学报，2003，14(1)：76-82

[2] Gong L，Qian X. Computational Issues in Secure Interoperation [J]. IEEE Transactions on Software Engineering，1996，22(1)：43-52

[3] Xacml T C. OASIS eXtensible Access Control Markup Language (XACML) [DB/OL]. http://www. oasis-open. org/committees/xacml/

[4] Hada S，Kudo M. XML access control language：Provisional authorization for XML documents [DB/OL]. http:// www. trl. ibm. com /projects /xml / xacl /xacl-spec. html

[5] Ashley P，Hada S，Karjoth G，et al. The enterprise privacy authorization language(EPAL) [DB/OL]. http://www. w3. org/2003/p3p-ws/pp/ibm3. html

[6] Ribeiro C，Z' lšquete A，Ferreira P，et al. SPL：An access control language for security policies with complex constraints [C]// NDSS '01：Network and Distributed System Security Symposium. 2001

[7] Bharadwaj V G，Baras J S. Towards automated negotiation of access control policies [C]// Proceedings of IEEE 4th International Workshop on Policies for Distributed Systems and Networks. Washington DC，USA：IEEE Computer Society Press，2003：111-119

[8] Wainer J，Kumar A，Barthelmess P. DW-RBAC：A Formal Security Model of Delegation and Revocation in Workflow Systems [J]. Information Systems，2007，22(3)：365-384

[9] James B D，Bertino E，Latif U，et al. A Generalized Temporal Role-Based Access Control Model [J]. IEEE Transaction on Knowledge and Data Engineering，2005：4-22

[10] 唐卓，赵林，李肯立，等. 一种基于风险的多域互操作动态访问控制模型[J]. 计算机研究与发展，2009，43(6)：948-955

[11] Li Ninghui，Wang Qihua，Qardaji W，et al. Access Control Policy Combining：Theory Meets Practice[C]// Proceedings of the 14th ACM symposium on Access control models and technologies. June 2009

[12] Cheng chen，Rohatgi P，Wagner G M，et al. Fuzzy Multi-Level Security：An Experiment on Quantified Risk-Adaptive Access Control[C]// IEEE Symposium on Security and Privacy. 2007：222-230

[13] 许峰，赖海光，等. 面向服务的角色访问控制技术研究[J]. 计算机学报，2005，28(4)：686-693

[14] 黄建，卿斯汉. 带时间特性的角色访问控制[J]. 软件学报，2003，14(11)：1944-1954

[15] Dewri R，Poolsappasit N，Ray P，et al. Optimal Security Hardening Using Multi-Objective Optimization on Attack Tree Models of Networks[C]// Proceedings of the 14th ACM Conference on Computer and Communications Security(CCS'07). New York，USA：ACM Press，2007：204-213

(上接第 90 页)

表 3　信息增益排名前五的特征

Rank	Feature
1	Number of suspicious external domains
2	Number of page redirection steps
3	Number of requests with incomplete headers
4	Whether external domains with 2 segments exist
5	Number of requested html files

表 4　不同样本分布下 C4.5 分类模型的性能

Malicious Webpage percentage	TP	FP	Precision	Accuracy
50%	96.6%	0.6%	99.4%	98%
20%	95.7%	0.4%	98.4%	98.8%
10%	92.2%	0.3%	97.2%	98.9%
All Sources	89.7%	0.3%	85.7%	99.5%

结束语　当前检测挂马网页的主要手段有网页代码特征匹配与高交互虚拟蜜罐技术。前者难以对抗代码加密与混淆变形技术，后者资源消耗较大，难以在客户端直接部署。针对这些不足，本文提出一种轻量级的、基于访问网页的 HTTP 会话统计特征的挂马网页检测方法，它无需对网页 HTML 代码、数据载荷进行特征匹配。基于低维特征与有监督的 C4.5 决策树学习，训练了能有效检测挂马网页的分类模型。实验证明，我们能达到 89.7%的检测率与 0.3%的误检率。下一步工作是进一步发掘更多挂马网页的特征，研究在线学习算法，以适应不断更新的挂马网页特征。

参 考 文 献

[1] 2009 年上半年中国大陆地区互联网安全报告[EB/OL]. See http://it. rising. com. cn/new2008/News/NewsInfo/2009-07-21/1248160663d53890. shtml

[2] Provos N，McNamee D，Mavrommatis P，et al. The ghost in the browser analysis of Web-based malware[C]// Proceedings of the First Workshop on Hot Topics in Understanding Botnets. Cambridge，MA，2007

[3] Hou Yung-Tsung，Chang Yimeng，Chen Tsuhan，et al. Malicious Web content detection by machine learning[J]. Expert Systems with Applications，2010，37(1)：55-60

[4] Seifert C，Komisarczuk P，Welch I. Identification of Malicious Web Pages with Static Heuristics[C]// IEEE Australasian Telecommunication Networks and Applications Conference. Adelaide，2008：91-96

[5] Moshchuk A，Bragin T，Deville D，et al. SpyProxy：Execution-based Detection of Malicious Web Content[C]// Proc. of the USENIX Security Symposium. Boston，MA，Aug. 2007：27-42

[6] Provos N，Mavrommatis P，Rajab M A，et al. All Your iFRAMEs Point to Us[C]// Proc. of the USENIX Security Symposium. San Jose，CA，July 2008：1-15

[7] Zhuge Jianwei，Thorsten H，Song Chengyu，et al. Studying Malicious Websites and the Underground Economy on the Chinese Web[C]// Proceedings of 2008 Workshop on the Economics of Information Security(WEIS'08). June 2008

[8] Top 1，000，000 Sites[EB/OL]. http://www. alexa. com/topsites，September 2009

[9] Seifert C，Steenson R. Capture-honeypot client [EB/OL]. https://www. client-honeynet. org/capture. html，2006

[10] Witten I H，Frank E. Data Mining：Practical Machine Learning Tools and Techniques (2nd ed) [M]. San Francisco：Elsevier Inc.，2005