网络安全策略与措施的语义一致性研究

肖 庆[1],焦 健[2]
(1.广西师范大学 历史文化与旅游学院,广西 桂林 541004;
2. 北京信息科技大学 计算机学院,北京 100192)

摘 要:计算机网络安全中以防火墙和入侵检测为代表的安全措施需要由高层策略转换得出。但在转换过程中由于机械规则的影响,策略与措施间语义的内容可能不一致。文中提出了一种用于计算策略到措施的语义度量方法,针对典型的ponder策略建立其语言结构化操作语义模型,规定高层策略到底层措施的转换规则,根据特定网络环境和事件,构造相关的推理引擎,能够自动实现底层措施到高层策略的语义度量。实验结果表明,该方法可以有效地实现策略和底层措施之间的在语义上存在的差异。

关键词:策略;措施;语义;一致性
中图分类号:TP393.08 **文献标识码**:A **文章编号**:1673-629X(2011)08-0220-03

Research on Semantic Consistency of Network Security Policy and Measure

XIAO Qing[1], JIAO Jian[2]
(1. Dept. of History Culture and Tourism, Guangxi Normal University, Guilin 541004, China;
2. School of Computer Science and Engineering, Beijing Info. Sci. & Techn. Univ., Beijing 100192, China)

Abstract: *In the computer network security, the measures using in firewall and IDS are changed by policy. Because the machine rules are used in the process, the measure is not consistency with the policy. Propose a method to measure semantic between the policy and measure. It makes the semantic model based on ponder with operation semantic, design the rule to transform policy to measure, using these rules to finish engine in order to compute the consistency automatically by the specific network environment and event. The experiment shows that the method can analyse consistency for semantics between policy and measure effectively.*

Key words: policy; measure; semantic; consistency

0 引 言

计算机网络应对攻击都需要相应的网络安全设备,这些设备在网络威胁产生之前或威胁发生之时部署相关计算机网络安全防御措施。网络中的安全防御措施具有严格具体的形式定义,部署到具体网络节点或区域之上的措施数量庞大,人工部署工作极为繁琐。针对这一现状,研究人员提出了使用高层策略描述语言的方式[1],通过屏蔽底层措施的细节,重点关注高层在特定网络环境下对可能产生的攻击事件的处理机制,该机制的表达尽量遵循人的思维意识[2,3],以协助管理人员快速制定网络安全策略。

网络中高层描述策略的产生,其根本目的在于能够转换出部署到具体网络安全设备的措施,因此策略和措施之间存在相应的转换方法。转换方法作为一种机械式计算,其过程中必然存在一定程度语义上的不一致,因而在实际的操作过程中,二者之间的转换可能会造成主观意图与实际结果的差异。

针对语义一致性的分析主要采用语义相似度测量的方法进行[4],其测量的具体技术又可以进一步基于语义树的测量方法[5,6]和基于上下文统计的测量方法[7~9],但这些技术的实质都是基于自然语言的模式。因此形式化的安全策略与措施之间语义转换的研究也基于自然语言展开。

这类研究[10]的主要问题在于自然语言的度量依靠人的主观判断成分较大,对计算机语言中高级语言到底层语言的转义工作涉及较少,自动化程度因此不高。文中针对这一问题,从网络安全防御策略和措施的模型分析入手,以策略和措施的规则为出发点,构建基于操作语义的度量一致性方式,并设计具体的实现机制。

收稿日期:2011-01-16;**修回日期**:2011-04-23
基金项目:国家863信息安全重点专项(2007AA01Z407)
作者简介:肖 庆(1964-),女,广西柳州人,讲师,主要研究方向为计算机网络安全。

1　度量原理

网络安全策略的特点是对网络中的安全规则实现抽象描述,最终以安全措施的形式实施,措施一般具体指面向网络安全设备的规则(如防火墙、IDS)。策略和措施的不一致性可以用图 1 实现形象的说明。假定左侧椭圆为策略(policy)描述的内容范围,右侧椭圆描述由该策略转换生成的措施(measure),二者一般情况会产生相交(即 A、B 和 C 区),其中 A 区表示策略和措施语义含义一致的地方,该部分内容的转换没有问题发生;而 B 区则表示转化措施与策略相比语义缺失的地方,即 B 区中策略在转换生成的措施中没有相应的结果;C 区表示措施与策略相比语义冗余的地方,即转换后产生了多余的措施。

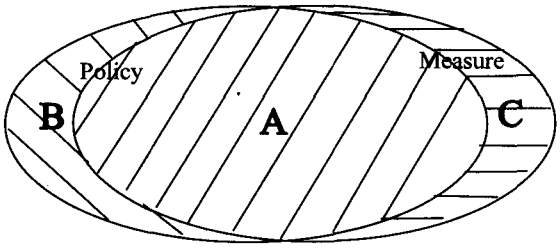

图 1　策略和措施转换不一致性

网络中的策略表述抽象,一般可以包括如下几个部分。在策略中的视图描述网络的场景,其中的网络拓扑和网络状态可统一表示为语境。策略中的上下文可表示为网络中一定语境下发生、改变网络安全状态的攻击事件,简称为事件(event),并且某些事件可以进一步推导出新的攻击事件,这些事件是校验策略到措施转换一致性的必要条件。

在这种情况下,语义度量机制的主要原理为:通过从策略中提取出来的语境和事件,同时引入转换后得到的措施进入推理引擎。安全措施会结合语境处理相关的事件发生,若语义转换过程中出现缺失,在推理过程中,会出现有关事件无法得到处理的情况,即推理引擎停机后会有事件尚未处理,证明转换过程会发生语义缺失;相反,若推理结束后,仍然有未被使用的措施,则证明转换过程具有语义冗余。

2　语义度量模型

为构造语义度量的模型,首先实现对策略和措施的预处理,即实现语境、事件和措施等形式化描述。而后实现推理引擎机制。

2.1　策略和措施的预处理

按照第一节的解决思路,首先需要构造语境、事件和措施的语义描述,在此选用以类 ponder[11] 语言的高层策略描述为研究对象,主要内容包括:构造语境的初始集合 σ,视图中的多节点构成域,域之间的连接情况表示为 T,节点的代表区域的初始状况为 S。

T 可以使用谓词的表达形式:

Area:hostA,hostB,hostC…

hostA:hostB　Link1 表示二者通过 link1 连接

Area 表示具体的网络区域,本研究对网络中的区域按照域、子网、主机、进程等顺序划分。

S 的谓词形式可以表示为:Area:Status。

Status 表示网络当前的状态,分为稳态(normal)和非稳态(unnormal),其中稳态表示网络的正常运行,非稳态表示网络在遭受到攻击的状态。

策略中的上下文产生一系列的事件,表示为<area1, area2, attack>, 构成集合 C。措施中的防御规则,以基本单元 action:<area, event, measure>的形式组成集合 Y。为方便起见,对于集合 C 和 Y 中的元素设立访问标志位,用以记录元素的被访问情况。

2.2　一致性推理系统

语义一致性的推理引擎的主要工作是实现措施和策略的形式化推导,引擎的推理规则按照形式化操作语义[12]的格式,主要包括以下几条:

$\langle \text{skip}, \sigma \rangle \rightarrow \sigma$:表示在输入为空的情况下,状态不变。

$\langle \text{action}, \sigma \rangle \rightarrow \langle \sigma' \rangle$: 表示在措施发生的情况下,状态发生变化。

$\langle \text{event}, \sigma \rangle \rightarrow \langle \sigma' \rangle$:表示在事件发生后,网络中状态发生的变化。

例如: $< x, y, \text{worm} > < x, \text{unnormal} > < x, y > < y, \text{normal} > \rightarrow < y, \text{unnormal} >$,表述区域 x 和 y 之间联通,y 正常,x 为非正常情况下,由 x 到 y 发起蠕虫攻击,区域 y 进入非正常状态。

$\dfrac{\text{eval}(\text{area}, \sigma) = \text{true}}{\langle \text{if area then action}, \sigma \rangle \rightarrow \langle \sigma' \rangle}$: 若网络中指定区域措施需要的状态出现,则措施被触发。

$\dfrac{\text{eval}(\text{area}, \sigma) = \text{false}}{\langle \text{ship}, \sigma \rangle}$: 若网络中指定区域措施需要的状态未出现,则跳过。

利用推理机停机和推导结果判断二者的不一致性,其算法流程如下:

```
Begin
    初始化 σ、C 和 Y
    While ( C 不空)或(一致性推理引擎停机) DO
    抽取 C 中的事件,和 σ 产生匹配推理,
    若成功改变则和 Y 匹配,从 C 中删除该事件,否则停机
    新产生的状态和 Y 一起实现匹配,
    若匹配成功,则修改 Y 访问记录
    否则返回 C 中,
End
判断结果:若 Y 中有元素访问记录为空,则存在转换冗余
```

若 C 有元素不为空并且 Y 全部被访问，则转换缺失
输出不一致的结果。
End

推理机输入的元素主要是语境 σ、事件集合 C 和防御规则集合 Y。在整个推理机的工作过程中，推理机不断从集合 C 中取出元素和语境进行推理匹配，产生的结果会以状态的形式触发集合 Y 中规则发生，规则的触发意味着措施属于和策略语义一致的转换结果，其它情况则分别视为转换中造成的缺失和冗余。

3 实验验证

网络安全策略与措施的语义度量实验以一定的具体网络为环境，针对该网络环境预先制定相应的网络安全策略，制定不同的转换方法产生具体的措施。而后依照模型对不同的转换结果实施语义度量，评价不同方法的转换效果。

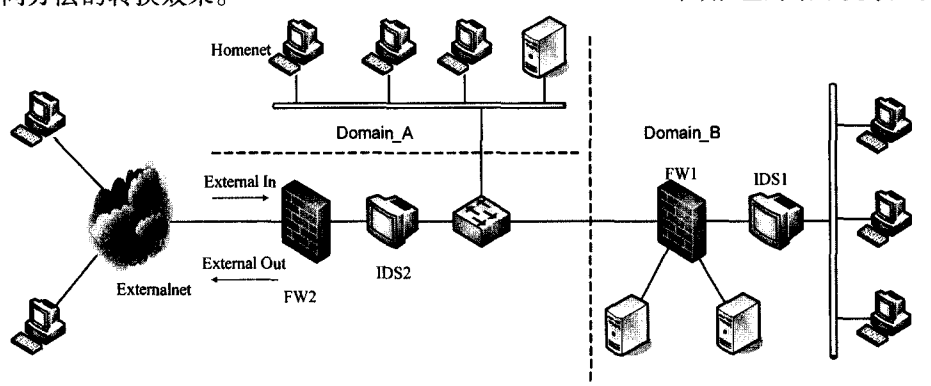

图 2 网络拓扑结构图

如图 2 所示，该图描述了一个典型 DMZ 局域网络安全体系结构，攻击活动从外网(Externalnet)发起，经过由 Domain_A 和 Domain_B 组成的防御区，进入内部网络 Homenet。针对这种网络体系，安全规划者可以制定如下的策略，用于实现对蠕虫扩散而造成的拒绝服务攻击的防御部署。内容如下：

Policy
{context severity INCIDENT worm authorityexploit servicedenial
Policy prohibit_source externalnet all homenet severity}

从定义的规则上看，第一条上下文描述了对服务出现的三种攻击：蠕虫、非授权访问和拒绝服务攻击。针对这三种攻击方式通过禁止攻击源的方法完成对内网的保护。

由网络安全策略可以提取出相应的网络事件 C，表示如下：

(Extend, Domain_A , worm)
(Domain_A, Domain_A, authorityexploit)
(Domain_A, Domain_B, worm)
(Domain_A, Domain_B, servicedenial)

三条事件分别表示蠕虫通过扩散的方式，进入内部网络，而后利用非授权访问提升自身的权限，并对 Domain_B 中的网络发动拒绝服务攻击。

根据这条策略，使用自动化策略转换机制可以获取部署在 IDS 上的措施。在转换机制上，分别使用 lex/yacc 编译器和 XSB 推理引擎两种方式完成这种转换(见表 1)。

表 1 措施集合

措施集合 1	措施集合 2
IDS 2	IDS 2
worm prohibition	worm prohibition
IDS 1	authority exploit prohibition
worm prohibition	IDS 1
authority exploit prohibition	worm prohibition
service denial prohibition	service denial prohibition
exit	exit

按照第二节中方法，可以构造语境网络的 σ 和措施集合 Y。上述内容作为输入进入一致性推理引擎之中，推理的结果见表 2。

从推理的结果上看，IDS1 和 IDS2 部署了针对蠕虫、非授权访问和拒绝服务攻击。当攻击从外部发生的时候，攻击首先从 external 进入 Domain_A，对于控制防火墙的 IDS2 而言，需要防止外部网的多种攻击。但对于控制 FW1 的 IDS1 而言，其攻击源并没有直接来自于 external。而只能产生在 Domain_A 中，因此其产生的防御措施虽然可以防止同样的攻击发生，但与最初的策略相比既存在缺失(Domain_A 中的拒绝服务攻击事件)，又有语义冗余部分(针对 Domain_B 中的权限访问措施)。因此，从转换结果上来看，转换结果 2 要好于转换结果 1，具有较好的语义一致性。

表 2 推理结果表

转换结果	1	2
C	(a1, a1, ser_den)	Φ
Y	(a2, auth, prob)	Action Access_full

4 结束语

计算机网络的规模需要快速高效地部署大量安全措施以应对网络攻击的发生，如何替代手工操作，将高层抽象的管理策略自动转换成为措施一直是网络安全研究的重点。而这种机械式转换中产生的语义不一致性是研究必须面对的问题。

文中对网络安全策略到措施的转换中存在的语义差异进行了分析，以类 ponder 语言为例，使用操作语

(下转第 227 页)

$$\begin{bmatrix} 0.034 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{bmatrix} = [0.0101 \quad 1 \quad 0 \quad 0 \quad 0]$$

目标层 A 的加权平均判决值为:

$$V_A = [0.0101 \quad 1.0 \quad 0 \quad 0 \quad 0] \bullet \begin{bmatrix} 90 \\ 70 \\ 50 \\ 30 \\ 10 \end{bmatrix} = 70.9$$

从模糊综合评判结果判断,航天测控系统的总体容灾能力等级“较强”,但是结合准则层的综合评判结果分析,航天测控系统在灾难恢复管理、灾难恢复规划及灾难恢复技术措施三方面都还有需要提高之处。特别是,航天测控系统担负保障航天任务安全可靠的重任,其容灾能力要求更为严格,应该从各方面着手加强,争取将其容灾能力提高至“强”等级水平。

3　结束语

通过层次分析和模糊评判相结合的方法对航天测控系统容灾能力进行评估,综合考虑了定量计算和定性评价两个方面,能够为建设航天测控容灾系统提供合理、有效的参考依据。在以后的工作中,将进一步对评价指标体系进行优化,并根据评估结果针对容灾建设中存在的不足之处进行改进,建设完善的航天测控容灾系统。

参考文献:

[1] 夏南银. 航天测控系统[M]. 北京: 国防工业出版社, 2002.

[2] 张卫民. 航天飞控软件的二维容错体系结构设计[J]. 计算机工程,2008,34(5):265-267.

[3] 厉　剑,廉国斌, 黄　栋. 数据容灾系统与 CDP 技术[J]. 计算机技术与发展,2009,19(1):168-171.

[4] Lyu M R. Handbook of Software Reliability Engineering[M]. New York: McGraw-Hill,1996.

[5] Saaty T L. The Analytic Hierarchy Process[M]. New York: Hill,1980.

[6] 王莲芬,许树柏. 层次分析法引论[M]. 北京:中国人民大学出版社,1989.

[7] Bard J F, Sousk S F. A Tradeoff Analysis for Rough Cargo Handlers Using the AHP:an Example of Group Decision Making[C]//Proceedings of the 2005 Winter Simulation Conference. [s. l.]:[s. n.],2005.

[8] 刘　宁, 高飞燕. 基于 AHP-FCE 的供应商选择问题研究与应用[J]. 计算机技术与发展,2009,19(11):11-15.

[9] 黄　松, 夏洪亚, 谈利群. 基于模糊综合的信息安全风险评估[J]. 计算机技术与发展,2010, 20(1):189-192.

[10] 胡宝清. 模糊理论基础[M]. 武汉:武汉大学出版社,2004.

[11] 陈敏刚,董　军,张丽亮. AHP 和模糊综合评判在灾难恢复能力评估中的应用[J]. 计算机工程,2006,32(18):135-137.

[12] 陈希祥,邱　静,刘冠军. 基于层次分析法与模糊综合评判的测试设备选择方法研究[J]. 兵工学报, 2010,31(1):68-73.

(上接第 222 页)

义的分析机制构建了用于度量一致性的模型和推理引擎算法。结果表明,利用该方法可以有效地实现网络中策略到措施转换一致性的验证,为分析网络安全系统转换效率提供了一种有效方法。需要指出的是,语义的一致性比较具有较强的主观性,策略转换后措施的可行性仍需在网络中实际运行予以验证,如何将运行结果引入到一致性的语义分析中有待进一步研究。

参考文献:

[1] Stern D F. On the Buzzword “Security Policy”[C]//Proceedings of the Symposium on Security and Privacy. Piscataway, NJ, USA:IEEE,1991:219-230.

[2] Damianou N, Bandara K A, Sloman M, et al. A Survey of Policy Specification Approaches [D]. London, UK: Imperial College,2002.

[3] Verma D. Simplifying Network Administration Using Policy Based, Management[J]. IEEE Network, 2002,16(2): 20-26.

[4] 魏凯斌,冉延平, 余　牛. 语义相似度的计算方法研究与分析[J]. 计算机技术与发展,2010,20(7):102-105.

[5] Cilibrasi R L. The Google Similarity Distance[J]. IEEE Transactions on Knowledge and Data Engineering, 2007, 19(3):370-383.

[6] 董振东. 语义关系的表达和知识系统的建造[J]. 语言文字应用,1998(3):79-85.

[7] 李　峰,李　芳. 中文词语语义相似度计算-基于知网 2000[J]. 中文信息学报,2007(3):99-105.

[8] 杨　哲. 基于启发式规则的本体概念语义相似度匹配[J]. 计算机应用,2007,27(12):2919-2921.

[9] 张明宝,马　静. 一种基于知网的中文词义消歧算法[J]. 计算机技术与发展,2009,19(2):9-11.

[10] Hao Senshen, Jiao Jian, Xia Chunhe, et al. Semantic similarity analysis model for CND policy and measure [C]//Proceedings of 2010 International Conference on Educational and Information Technology (ICEIT'10). Chongqing, China: [s. n.],2010,340-343.

[11] 夏春和,魏玉娣,李肖坚,等. 计算机网络防御策略描述语言研究[J]. 计算机研究与发展,2009,46(1):89-99.

[12] 陆汝钤. 计算机语言的形式语义[M]. 北京:科学出版社, 1972:186-187.