基于协同侦测技术的移动主体模型验证策略研究

李海鹰 程 灏 叶为全 庄镇泉

(中国科技大学电子科学与技术系 合肥 230026)

摘 要 移动主体模型可以实现协同侦测网络攻击和区域预警的功能;它利用元组空间(TUPLE-SPACE)构建移动主体服务集群(RMAS-CMAS)网络结构及侦测 ARP 攻击的主体.为了证明该模型逻辑的有效性,验证策略设计了可以分析 ARP 攻击数据包从初始组态到终结组态的动态空间树;利用空间树嵌套演算推理协同侦测系统的组态迁移过程,分析模块的动态移动重组以及消息的并行传递机制.对模型验证策略的研究可以消除在模型设计阶段出现的冗余组态,提高移动系统的设计水平.

关键词 移动主体;元组空间;模型验证;组态迁移

中图法分类号 TP393

Model Checking Strategy of Mobile Agent Based on Technology of Collaborative Detection

LI Hai-Ying CHENG Hao YE Wei-Quan ZHUANG Zhen-Quan

(*Department of Electronic Science and Technology, University of Science and Technology of China, Hefei* 230026)

Abstract The mobile agent model achieves the goal of collaborative detection of network intrusion when attacks occur in a vast region. The architecture of service cluster(RMAS-CMAS) is described as well as mobile agent for detecting ARP attack via the concept of Tuple-Space. To check the effectiveness of the system detection logic, model checking strategy enables us to build dynamic spaces tree from initial configuration to terminative configuration which is used to analyze packets of ARP attack. Transference of collaborative detection system configurations, dynamic recompose of modules and message parallel transfer mechanism are ratiocinated by calculation of nested spaces tree. Study of model checking strategy can eliminate the redundance configurations which exist in the model design and help to improve quality of the design of mobile system.

Keywords mobile agent; tuple-space; model checking; transference of configurations

1 引 言

近年来,网络安全日益成为困扰广大网络用户的问题,传统的入侵检测技术不能满足复杂网络的管理需要.移动主体具有智能性、自治性、协作性、持续性和移动性等优点.用于入侵检测的移动主体模型[1]利用其移动特性,克服了传统入侵检测系统独立运算、协调性差的缺点,可以突破网段的限制,使在不同网段中的多个主体系统能够协同工作,有效地发现网络攻击的特征,更好地保护网络内部信息资源,实现协同侦测与预警的目的.

用于描述抽象模型的移动代码规范,例如 π-calculus 形式语言[2],KLAIM 进程演算语言[3],Mo-

收稿日期:2002-09-13;修改稿收到日期:2004-07-24.本课题得到国家自然基金重点项目(90104030)和中国科学技术大学青年基金资助.
李海鹰,男,1968 年生,博士后,副教授,研究方向为计算机理论、网络安全、软件工程.E-mail:lihy@ustc.edu.cn.程 灏,男,1981 年生,本科生,研究方向为电子信息处理技术.叶为全,男,1971 年生,博士后,研究方向为信息安全、智能信息处理等.庄镇泉,男,1938 年生,教授,博士生导师,研究方向为网络安全、智能信息处理等.

bile UNITY[4]等已经被广泛地研究和应用. 多元组空间语言[5]结合以上规范的优点,能很好地描述侦测系统的移动特性和协同工作机制. 我们利用多元组空间建立了侦测 ARP 攻击的移动主体系统的抽象模型,在此基础上,通过具体实例研究模型的验证方法.

基于多元组空间的移动主体模型验证策略,通过分析元组以及空间的动态生成和销毁来验证主体的移动特性;通过研究元组空间互相嵌套形成的动态空间树结构,跟踪系统组态的迁移,来检验主体的事件驱动机制. 由元组空间描述的主体模型,可以对系统组态进行归类,有效地减少系统所需验证的组态的数量,这有利于对模型中各种变量的可能值进行详细的分析和推理,定义组态之间的转换关系. 模型验证侧重于研究组态的迁移转换,在验证过程中可以不考虑促使相邻组态迁移的规则元组,如此可使验证进一步简化. 模型验证可以分析模型能否有效地达到系统设计目标,并检验模型是否存在冗余组态.

2 侦测模型的空间表示

侦测模型以检测 ARP(Address Resolution Protocol)攻击为研究背景,规则元组存活在模型架构中,并促使了移动主体组态迁移;移动主体验证要在具体的模型架构中进行.

在多元组空间中,一个网络在逻辑上可以映射为一个主空间,网络内可以架设 N 台远程移动主体服务器[6](Remote Mobile-Agent-Server,RMAS 元组空间)和一台中心移动主体服务器(Central Mobile-Agent-Server,CMAS 元组空间),在主空间中的网络介质上传输的数据包映射为数值元组. RMAS 可以向 CMAS 申请移动主体. RMAS 接收到 CMAS 发来的模块后,经过安全性验证,移动主体模块就会自动展开,在 RMAS 元组空间中生成执行任务的各个元组以及子空间,对主空间中数据包数值元组按照侦测逻辑进行分析,执行诸如截获、统计本网段数据流量、防御入侵等任务. 不仅移动主体可以移动,而且检测结果也可以作为一个元组空间在网络中移动,分布在各个网段的 RMAS 都会接收到此元组空间,可以协同侦测入侵攻击. 在移动主体模型中,RMAS-CMAS 模式[7]构筑了移动主体的基础平台;移动主体在平台上运作,按照其自身的侦测逻辑执行各种任务.

ARP 攻击是指利用地址解析协议本身的运行机制发动的网络攻击行为,包括进行 ARP 伪装、嗅探数据包、DoS(Denial of Service)攻击等. 由于 ARP 攻击具有一个明显的特征:大部分的 ARP 攻击发出的数据包中包含的 MAC-IP 映射对是伪造的,网络上根本不存在与该映射对相对应的机器. 所以我们针对此特征制定以下的检测规则:ARP 数据包中包含的 MAC-IP 映射对都是有效的,即在局域网上,这台主机是存在的. 如果有 ARP 数据包违反了此规则,则认为局域网上出现了 ARP 攻击. 所以实现此检测规则的移动主体必须对所有 ARP 数据包中出现的 MAC-IP 映射对进行主动验证,并保存历史的验证信息.

图 1 给出了实现此检测规则的移动主体的嵌套空间模型架构,图 2 则为相应的空间树模型. RMAS 元组空间包含于主空间 StartContent 当中,而移动主体在 RMAS 元组空间中展开后,自动生成了 SNMB-MIB 元组空间. SNMB-MIB 元组空间中包含了规则元组以及多个 mactoip_i 元组空间. SNMP-MIB 元组空间中每个 mactoip_i 元组空间对应本网段内一个通过系统验证的 MAC 地址,mactoip_i 元组空间中记录了此 MAC 地址所对应的全部 IP 地址信息.

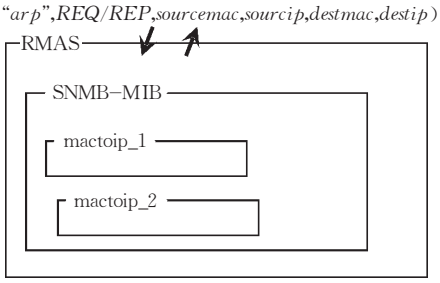

图 1 移动主体的嵌套空间模型架构

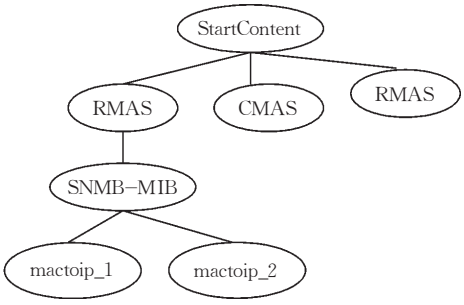

图 2 移动主体空间树模型

3 协同侦测的组态迁移过程

图 3 描述了远程移动代理服务器(RMAS)向中心移动代理服务器(CMAS)[8]申请移动主体以及在接收到移动主体后,主体展开整个过程的组态迁移的过程.

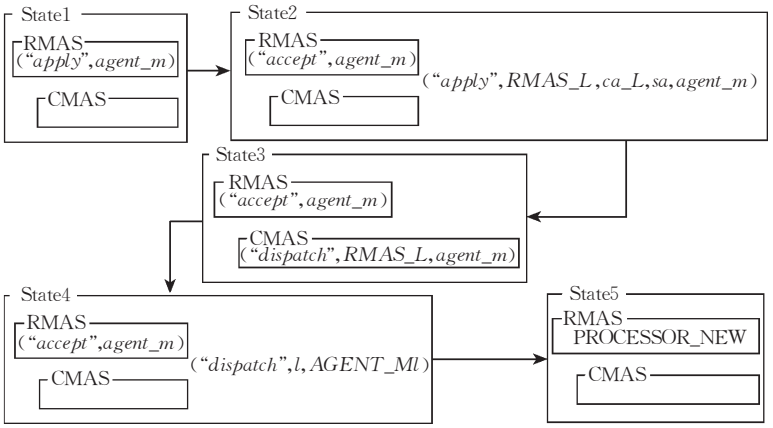

图 3　移动主体展开过程的组态迁移

$\forall C((("apply",agent\_m)),\mathrm{CMAS})\in C$
$\rightarrow(("apply",RMAS\_L,ca\_l,sa,agent\_m),$
$(("accept",agent\_m)),\mathrm{CMAS})\in C$
$\rightarrow((("accept",agent\_m)),$
$(("dispatch",RMAS\_L,agent\_m)))\in C$
$\rightarrow(("dispatch",l,AGENT\_M1),$
$(("accept",agent\_m)),\mathrm{CMAS})\in C$
$\rightarrow((PROCESSOR\_NEW),\mathrm{CMAS})\in C.$

上面的推理子式等价于移动主体的组态迁移图，推理子式中每一步推导都对应着模型每一次组态的迁移，推理式可以很好地验证模型组态的迁移. 验证过程中，我们假设所有组态的集合为 C，**由元组以及空间组成的任何一个组态都属于组态集合** C. RMAS **向** CMAS **申请特定的移动主体，当** RMAS **发出请求后，整体模型由初始** State1 **组态迁移到** State2 **组态，**apply **数值元组包括了该** RMAS **和** CMAS **的验证密钥以及申请的移动主体标识序号.** CMAS **接收到请求后，经过验证，则模型进入** State3 **组态.** State4 **组态代表了** CMAS **收到请求后发出了移动主体，该移动主体由** CMAS **和该** RMAS **验证密钥共同加密后的移动主体代码** $AGENT\_Ml$ **构成. 当模型转入** State5 **终结组态，**RMAS **收到了移动主体，并自动展开生成了动态元组空间的集合** PROCESSOR _NEW.

当某个网段中的 RMAS **在检测** ARP **数据包时发现了** ARP **攻击的痕迹，该移动主体会自动地在网络上广播** $("arpattack",mac,ip)$ **数值元组，**mac，ip **对应了可疑的** MAC-IP **映射对. 在网络上的其它网段的** RMAS **以及** CMAS **接收到警告信息后，会相应地采取防御措施. 下面的子式验证了整个消息并行传递过程，其对应的组态迁移如图** 4 **所示.**

$\forall C((("arpattack",mac,ip)),\mathrm{CMAS},\mathrm{RMAS})\in C$
$\rightarrow(("arpattack",mac,ip),(("arpattack",mac,ip)),$
$\mathrm{CMAS},\mathrm{RMAS})\in C$
$\rightarrow((("arpattack",mac,ip)),(("arpattack",mac,ip)),$
$(("arpattack",mac,ip)))\in C.$

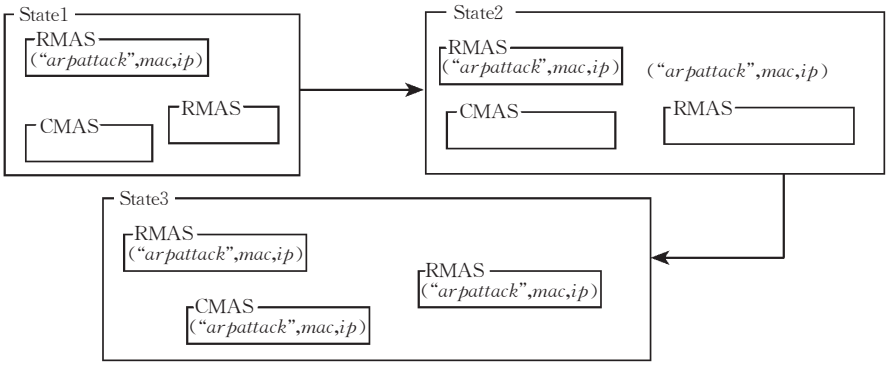

图 4　主体模型消息并行传递组态迁移图

4　模型验证策略实例分析

整个模型是基于多元组空间的、嵌套的空间树结构，这个空间树随着时间的变化会动态地发生进化，也就是组态会随着信息数据的到来进行迁移. 在本模型中，通过对截取的 ARP **数据包进行全面的审查**[9]，**判断是否有异常情况. 每一种情况的检验都**

会使模型由初始组态向某个终结组态移动.

4.1 ARP 攻击检测流程

ARP 攻击被抽象为若干个系统组态,代表 ARP 攻击的终结组态的出现,表明了网络上有 ARP 攻击.在初始组态下,模型开始检查 ARP 数据包,对所有可疑的 MAC-IP 映射对进行主动验证.检验信息以及检验结果将会促使模型组态迁移.如果到达某个终结组态,模型断定对应的 ARP 攻击的特征被成功匹配,模型会自动发出警报;否则模型将继续检查数据包.对模型进行验证时,要考虑到所有可能出现的组态情况.

式(1)证明移动主体可以在本网段内监听 ARP 数据包,并从中获取 MAC-IP 映射对,以供系统进一步分析.

$$\forall C, type \in (REQ, REP), mac, ip, mac1, ip1((\text{“}arp\text{”}, type, mac, ip, mac1, ip1)) \in C \rightarrow ((((\text{“}macip\text{”}, mac, ip, unchecked, 1), (\text{“}macip\text{”}, mac1, ip1, unchecked, 1)))) \in C \quad (1)$$

移动主体搜集到 MAC-IP 映射对(mac, ip),该映射对与移动主体已经获得的映射对信息相结合,可以具体分为下面 4 种情况.这 4 种情况囊括了全部可能性.

分类 1. 新映射对的 MAC,IP 地址皆未出现于任何 $mactoip$ 子元组空间中.

$$Type1 = \forall i \in (1..macindex), k \in (1..mactoip\_i.ipindex) (mac \text{ !=} mactoip\_i.mac) \wedge (ip \text{ !=} mactoip\_i.ip\_k).$$

分类 2. 新映射对的 MAC 地址存在于某个 $mactoip\_i$ 元组空间中,而该 $mactoip\_i$ 元组空间中尚未有该 IP 映射对信息.

$$Type2 = \exists i \in (1..macindex), \forall k \in (1..mactoip\_i.ipindex) (mac = mactoip\_i.mac) \wedge (ip \text{ !=} mactoip\_i.ip\_k).$$

分类 3. 新映射对的 IP 地址已经存在于某个 $mactoip\_i$ 元组空间中,而该 $mactoip\_i$ 元组空间中的该 IP 映射对信息对应的 MAC 地址与 MAC-IP 映射对中的 MAC 地址不相同.

$$Type3 = \exists i \in (1..macindex), k \in (1..mactoip\_i.ipindex) (mac \text{ !=} mactoip\_i.mac) \wedge (ip = mactoip\_i.ip\_k).$$

分类 4. 新映射对,已经存在于某个 $mactoip\_i$ 元组空间.

$$Type4 = \exists i \in (1..macindex), k \in (1..mactoip\_i.ipindex) (mac = mactoip\_i.mac) \wedge (ip = mactoip\_i.ip\_k).$$

移动主体从本网段中所有正常 ARP 数据包中搜集到的 MAC-IP 映射对信息可能为分类 1～4,也可能为分类 2,3 的结合(分类 1 或 4 与其它分类都没有交集),而且正常的映射对可以通过主动验证,正常的 MAC-IP 映射对可以由下式描述.

$$Normal = (\text{“}macip\text{”}, mac, ip, existed, 1) \wedge (Type1 \vee Type2 \vee Type3 \vee Type4).$$

移动主体对于正常的映射对会按照其所属分类做出相应的动作,对分类 1 生成 $mactoip\_i$ 空间;对分类 2 则更新对应的 $mactoip\_i$ 空间;对分类 3,如果老映射对无效则空操作(NULL),如果老映射对仍旧有效则发出 IP 冲突警报(由于人为配置失误而出现的 IP 冲突不属于 ARP 攻击,对应的映射对是正常的);对分类 4,主体不进行额外处理.

$$Normal\_reaction = (mactoip\_maccount\_new) \vee (\text{“}macindex\text{”}, i, mac, ipcount\_new) \vee (\text{“}ipconflict\text{”}, ip) \vee \text{NULL}.$$

从异常 ARP 数据包中搜集到的 MAC-IP 映射对信息则可能为分类 1～3 任一种(不可能为分类 4,如果攻击者伪造的 MAC-IP 映射对对应某台实际存在的主机,则此映射对是无法起到攻击作用),也可能为分类 2,3 的结合,而且异常的映射对无法通过验证,异常的 MAC-IP 映射对可以由下式描述.

$$Abnormal = (\text{“}macip\text{”}, mac, ip, unexisted, 1) \wedge (Type1 \vee Type2 \vee Type3).$$

当发现包含异常映射对的 ARP 数据包时,移动主体认为局域网上出现 ARP 攻击,会立即广播发送出警报.

$$Abnormal\_reaction = (\text{“}arpattack\text{”}, mac, ip).$$

以上过程可以通过图 5 给出的移动主体检测 ARP 攻击的具体实现机制流程直观给出.为了证明侦测逻辑的有效性需要验证式(2)和式(3).

$$\forall CNormal \in C \rightarrow Normal\_reaction \in C \quad (2)$$

$$\forall CAbnormal \in C \rightarrow Abnormal\_reaction \in C \quad (3)$$

4.2 侦测逻辑的有效性验证

对于分类 1,2 的 ARP 映射对,移动主体都必须主动地发送针对该映射对的 ARP Request 数据包,对此 MAC-IP 映射对进行验证并等待验证结果:

$$\forall C, ((((\text{“}macip\text{”}, mac, ip, unchecked, 1) \wedge (Type1 \vee Type2)))) \in C \rightarrow ((((\text{“}macip\text{”}, mac, ip, unchecked, 0)))) \in C \rightarrow ((\text{“}arp\text{”}, REQ, hostmac, hostip, mac, ip), (((\text{“}macip\text{”}, mac, ip, checking, CONST)))) \in C \quad (4)$$

对于分类 3 映射对,移动主体须对该 IP 对应的

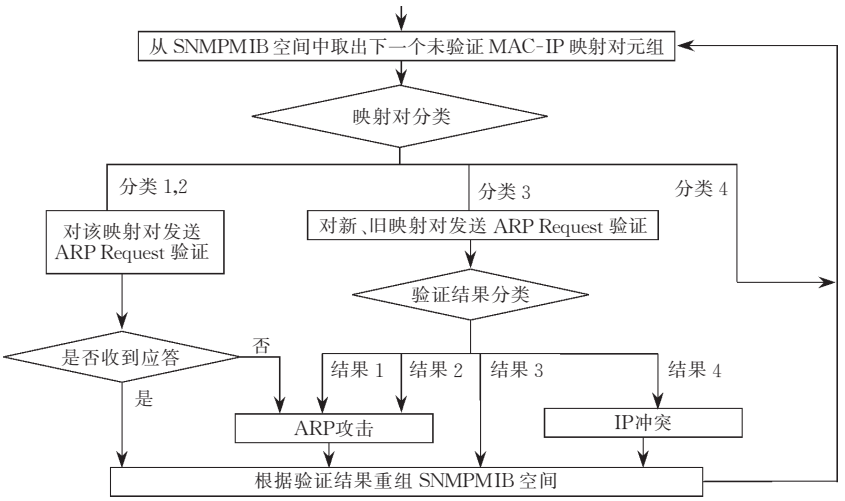

图 5　侦测主体检测 ARP 攻击的实现机制

新旧两个映射对都进行验证：

$$\forall C,((((\text{“}macip\text{”},mac,ip,unchecked,1)\wedge Type3)))\in C \rightarrow((((\text{“}macip\text{”},mac,ip,unchecked,0),(\text{“}macip\text{”},mactoip\_i,mac,ip,unchecked,0))))\in C \rightarrow((\text{“}arp\text{”},REQ,hostmac,hostip,mac,ip),(\text{“}arp\text{”},REQ,hostmac,hostip,mactoip\_i,mac,ip),(((\text{“}macip\text{”},mac,ip,checking,CONST),(\text{“}macip\text{”},mactoip\_i,mac,ip,checking,CONST),((\text{“}ipindex\text{”},k,ip\_k,checking,mac,checking)))))\in C \quad (5)$$

对于分类 4 的 ARP 映射对，由于已经过确认，该映射对已经存在了（也即（“$macip$”，mac，ip，$existed$，1）不用验证就可获得），所以不需再次验证，如式（6）：

$$\forall C,((((\text{“}macip\text{”},mac,ip,unchecked,1)\wedge Type4)))\in C \rightarrow(\text{NULL})\in C \quad (6)$$

移动主体发出 ARP Request 数据包主动查询之后，至多在 CONST 个周期之后就可以获得验证结果. 正常的 MAC-IP 映射对可以通过验证，而异常的 MAC-IP 映射对无法通过验证. 如果在 $CONST$ 个周期内接收到发出的 Request 的回应 Reply 数据包，则此映射对通过验证，生成（“$macip$”，mac，ip，$existed$，1）（见式（7）），否则超时，模型自动生成（“$macip$”，mac，ip，$unexisted$，1）（见式（8））.

$$\forall C,i((((\text{“}macip\text{”},mac,ip,checking,i)\wedge(i>0)),(\text{“}arp\text{”},REP,mac,ip,hostmac,hostip))\in C \rightarrow((((\text{“}macip\text{”},mac,ip,existed,1))))\in C \quad (7)$$

$$\forall C((((\text{“}macip\text{”},mac,ip,checking,0))))\in C \rightarrow((((\text{“}macip\text{”},mac,ip,unexisted,1))))\in C \quad (8)$$

移动主体刚加载时，移动主体还未搜集到任何 MAC-IP 映射对，在 SNMP-MIB 元组空间中没有任何的 $mactoip$ 元组空间. 移动主体会为每一个经过验证的 MAC 地址生成一个 $mactoip\_i$ 元组空间. 移动主体可能在以下两种情况生成 $mactoip\_i$ 元组空间.

情况 1.　属于分类 1 的映射对经过验证后，移动主体会为此 MAC 地址建立新的 $mactoip$ 元组空间（见式（9））. 这种情况出现于：当移动主体正常加载之后，在该网段中，另一台主机接入网络，且主机配置与网络上其它主机没有冲突.

$$\forall C((((\text{“}macip\text{”},mac,ip,existed,1)\wedge Type1)))\in C \rightarrow((((\text{“}macip\text{”},mac,ip,existed,0))))\in C \rightarrow((((\text{“}macindex\text{”},maccount\_new),(mactoip\_maccount\_new))))\in C \quad maccount\_new=maccount+1 \quad (9)$$

情况 2.　属于分类 3 的新的映射对经过验证后，移动主体会为此 MAC 地址建立一个新的 $mactoip\_i$ 元组空间. 这种情况出现于：当移动主体加载之后，在本网段内主机 A 接入网络，而且使用主机 B 之前使用的一个 IP 地址，而主机 B 在这之前刚好不再使用此 IP 地址，或主机 B 断开网络连接：

$$\forall C,((((\text{“}macip\text{”},mac,ip,existed,1)\wedge(\text{“}macip\text{”},mactoip\_i,mac,ip,unexisted,1)\wedge Type3\wedge(\text{“}macindex\text{”},maccount)\wedge((\text{“}ipindex\text{”},k,ip\_k,checking,mac,checking)))))\in C \rightarrow((((\text{“}macip\text{”},mac,ip,existed,0),((\text{“}macindex\text{”},i,mactoip\_i,mac,ipcount\_new)))))\in C \rightarrow((((\text{“}macindex\text{”},maccount\_new),(mactoip\_maccount\_new,mactoip\_i)))\in C \quad maccount\_new=maccount+1,\ ipcount\_new=ipcount-1 \quad (10)$$

或者是某台主机接入网络，而其配置 IP 与网络上另

外一台主机的 IP 相同,即出现了 IP 冲突,移动主体可以检测出 IP 冲突:

$$\forall C,((((\text{“}macip\text{”},mac,ip,existed,1)\wedge(\text{“}macip\text{”},mactoip\_i.mac,ip,existed,1)\wedge Type3\wedge(\text{“}macindex\text{”},maccount)\wedge((\text{“}ipindex\text{”},k,ip\_k,checking,mac,checking)))))\in C\rightarrow((((\text{“}macip\text{”},mac,ip,existed,0),((\text{“}ipindex\text{”},k,ip\_k,existed,mac,existed)))))\in C\rightarrow((\text{“}ipconflict\text{”},ip),((\text{“}macindex\text{”},maccount\_new),mactoip\_maccount\_new)))\in C$$

$$maccount\_new=maccount+1 \tag{11}$$

上面式(10),(11)分别是分类 1 和分类 3 的 MAC-IP 映射对经过验证的情况,证明了移动主体可以生成 *mactoip* 元组空间. 移动主体不仅可以生成 *mactoip* 元组空间,而且在某个 MAC 地址失效之后(该 *mactoip_i* 元组空间中不包含任何 MAC-IP 映射对的信息),会自动地删除该 *mactoip_i* 元组空间(见式(12)). 这种情况出现于当某台主机断开网络连接,且该主机配置与其它主机没有冲突.

$$\forall C,((((\text{“}macindex\text{”},maccount),((\text{“}macindex\text{”},i,mactoip\_i.mac,0)))))\in C\rightarrow((((\text{“}macindex\text{”},macindex),(\text{“}macipdelete\text{”},delete))))\in C\rightarrow((((\text{“}macindex\text{”},maccount\_new))))\in C$$

$$maccount\_new=maccount-1 \tag{12}$$

移动主体获得映射对验证结果之后,就可以在各个判别规则元组和 *mactoip* 元组空间协助下进一步判别是否出现了 ARP 攻击的痕迹. 属于分类 1~4 的映射对,只要经过验证,这几种映射对都可以认为是正常的,本网段未出现 ARP 攻击. 下面补充属于分类 2 经过验证的映射对的逻辑推理过程:

$$\forall C,((((\text{“}macip\text{”},mac,ip,existed,1)\wedge Type2))))\in C\rightarrow(((((\text{“}macindex\text{”},i,mactoip\_i,mac,ipcount\_new),(\text{“}ipindex\text{”},ipcount\_new,ip,existed)))))\in C$$

$$ipcount\_new=ipcount+1 \tag{13}$$

式(6),(9)~(13)证明了移动主体能够识别正常的 MAC-IP 映射,综合以上各式,式(2)得证. 下面验证式(3).

$$\forall C((((\text{“}macip\text{”},mac,ip,unexisted,1)\wedge(Type1\wedge Type2))))\in C\rightarrow((((\text{“}macip\text{”},mac,ip,unexisted,0))))\in C\rightarrow((((\text{“}arpattack\text{”},mac,ip))))\in C\rightarrow((\text{“}arpattack\text{”},mac,ip))\in C \tag{14}$$

式(14)证明了属于分类 1,2 的 MAC-IP 映射对如果未能经过验证,能使移动主体触发生成(“*arpattack*”,*mac*,*ip*)元组. 对于分类 3 的 MAC-IP 映射,在新映射对未能通过验证情况下,旧映射对有两种可能:通过(见式(15))或未通过验证(见式(16)). 两种情况都能触发生成(“*arpattack*”,*mac*,*ip*)元组,区别在于对 *mactoip_i* 元组空间的处理上.

$$\forall C,((((\text{“}macip\text{”},mac,ip,unexisted,1)\wedge(\text{“}macip\text{”},mactoip\_i.mac,ip,existed,1)\wedge Type3\wedge((\text{“}ipindex\text{”},k,ip\_k,checking,mac,checking)))))\in C\rightarrow((((\text{“}macip\text{”},mac,ip,unexisted,0),((\text{“}ipindex\text{”},k,ip\_k,existed,mac,unexisted)))))\in C\rightarrow((\text{“}arpattack\text{”},mac,ip),(((\text{“}ipindex\text{”},k,ip\_k,existed))))\in C \tag{15}$$

$$\forall C,((((\text{“}macip\text{”},mac,ip,unexisted,1)\wedge(\text{“}macip\text{”},mactoip\_i.mac,ip,unexisted,1)\wedge Type3\wedge((\text{“}ipindex\text{”},k,ip\_k,checking,mac,checking)))))\in C\rightarrow((((\text{“}macip\text{”},mac,ip,unexisted,0),((\text{“}macindex\text{”},i,mactoip\_i,mac,ipcount\_new)))))\in C\rightarrow((\text{“}arpattack\text{”},mac,ip),((mactoip\_macindexnew,mactoip\_i)))\in C$$

$$ipcount\_new=ipcount-1 \tag{16}$$

综合式(14)~(16),式(3)得证. 综上所述,移动主体符合系统侦测逻辑,可以有效地发现 ARP 攻击行为.

5 结束语

模型验证阶段处于模型设计和系统具体实现之间,此阶段在软件系统的研制开发周期中具有非常重要的地位. 有效的模型验证策略,可以检测出模型存在的缺陷和失误,使模型结构趋向于合理化,保证应用系统设计的正确性;它可以提高移动主体技术在入侵检测中的作用. 在移动模型的基础之上,移动主体的验证策略可以通过构建模型验证自动机,按照应用系统的实际工作流程,对模型组态迁移进行全面的验证.

参 考 文 献

1 Jansen W., Mell P., Karygiannis T., Marks D.. Applying mobile agents to intrusion detection and response. National Institute of Standards and Technology, USA: Technical Report 6416, 1999

2 Milner R.. Communicating and Mobile Systems: The π-Calculus. Cambridge: Cambridge University Press, 1999

3 de Nicola R., Ferrari G. L., Pugliese R.. KLAIM: A kernel language for agents interaction and mobility. IEEE Transactions on Software Engineering, 1998, 24(5): 315～330

4 McCann P. J., Roman Gruia-Catalin. Compositional programming abstractions for mbile computing. IEEE Transactions on Software Engineering, 1998, 24(2): 97～110

5 Mascolo C.. Formalization analysis and prototyping of mobile CodeSystem[Ph. D. dissertation]. Bologna: University of Bologna, 2001

6 Balasubramaniyan J. S., Garcia-Fernandez J. O., Isacoff D., Spafford E. H., Zamboni D.. An architecture for intrusion detection using autonomous agents. In: Proceedings of Asia-Pacific Computer Systems Architecture Conference, 1998, 13～24

7 Ciancarini P., Franze F., Masoolo C.. A coordination model to specify system including mobile agents. In: Proceedings of International Workshop on Software Specification and Design, 1998, 96～105

8 Deng Wei, Chen Ming-Qi, Ai Bo. Enhancing authenticating mechanism with mobile agent in mobile communication system. In: Proceedings of IEEE VTC2000, 2000

9 Karnouskos S.. Dealing with denial-of-service attacks in agent-enabled active and pogrammable infrastructures. In: Proceedings of the 25th IEEE International Computer Software and Applications Conference, 2001, 8～12

LI Hai-Ying, born in 1968, postdoctor, associate professor. His research interests include theory of computer, security of computer network, software engineering.

CHENG Hao, born in 1981, undergraduate. His research interests include process technology of electronic information.

YE Wei-Quan, born in 1971, postdoctor. His research interests include security of computer information, process of intelligent information.

ZHUANG Zhen-Quan, born in 1938, professor. His research interests include security of computer network, process of intelligent information

Background

The research on collaborative detection of network intrusion is supported by the National Natural Science Foundation of China under grant No. 90104030. Its purpose is to improve validity of mobile detection agent. The research group has developed a practice system to analyze packets of ARP attack, and it can alert administrator about significant security events happening on workstations and servers . This paper is about how to apply logic model design to establish the architecture of detection system.