

移动代理入侵检测系统中的自适应技术的研究

何向荣¹, 沈佐民¹, 吴 璞¹, 王汝传^{1,2}

(1. 池州师范专科学校, 安徽 池州 247000;

2. 南京邮电大学 计算机科学与技术系, 江苏 南京 210003)

摘 要:介绍了入侵检测及入侵响应系统中的自适应技术。提出了基于代理的自适应分层入侵检测系统(AAHIDS, Agent-based Adaptive Hierarchical Intrusion Detection System)和基于代理的自适应入侵响应系统(AAIRS, Agent-based Adaptive Intrusion Response System)。它们通过调整负责检测入侵行为的系统资源来实现自适应性, 动态调用新的底层检测代理的组合以及调整与这些底层代理相关的置信度来适应变化的环境。通过增加过去已获得成功的响应机制的权值, 使成功的响应机制获得更多的调用机会来实现响应的自适应性。

关键词:入侵检测; 入侵响应; 移动代理; 自适应

中图分类号:TP393.08

文献标识码:A

文章编号:1005-3751(2006)02-0229-03

Research on Adaptive Technique of Intrusion Detection and System Based on Mobile Agent

HE Xiang-rong¹, SHEN Zuo-min¹, WU Pu¹, WANG Ru-chuan^{1,2}

(1. Chizhou Teachers College, Chizhou 247000, China;

2. Dept. of Computer Sci. and Techn., Nanjing Univ. of Posts and Telecomm., Nanjing 210003, China)

Abstract: It introduces adaptation in intrusion detection and intrusion response. An agent-based adaptive hierarchical intrusion detection system (AAHIDS) and agent-based adaptive intrusion response system (AAIRS) are brought forth. They adjust the system resource used to detect intrusion action to realize adaptation, adapt to the variant circumstance by invoking new combination of low level detection agent dynamic and adjusting the confidence metric of these low level agent. Finally they increase the weight of the successful response, which make the response get more chance to be called to realize the adaptation of the response system.

Key words: intrusion detection; intrusion response; mobile agent; adaptive

0 引 言

入侵检测及响应技术^[1]是近年来出现的新型网络安全技术, 目的是提供实时的入侵检测及采取相应的防护手段, 它以探测和控制技术为本质, 起着主动防御的作用, 是网络安全中极其重要的部分。人们在构建高效的入侵检测系统(IDS)和入侵响应系统(IRS)方面进行大量的研究, 并取得了很大的成就, 出现了很多IDS和IRS的原型系统以及商业化的产品。

但目前入侵检测和响应中仍然存在如下问题:

(1) 一般的入侵检测系统中中央数据分析器是唯一

的分析处, 所以中央检测管理节点是一个单一的失效点。因此如果入侵者以某种方式阻止它运行, 网络就得不到保护。

(2) 单一检测管理节点处理所有的信息意味着被监控的网络规模将受到限制, 不能适应现在的大规模膨胀的网络。

(3) 为入侵检测增加功能有一定难度, 通常需要修改配置文件才能为入侵检测系统增加功能。因此当入侵者采用新的入侵方案时入侵检测系统不能及时做出响应。

(4) 不能根据出现的误警(false positive)和漏报(false negative)的历史数据的反馈动态调整入侵检测和响应系统。

(5) 传统的基于移动代理的入侵检测系统中分配给检测代理的资源是一定的, 这些资源不能根据实际的变化而相应的改变, 既不能在攻击大量发生时增加, 也不能在系统处于相对安全的时期减少占用的有效资源。

(6) 一般的移动检测代理都是针对特定的攻击行为, 因此对于新的攻击方法必须设计增加新的移动检测代理,

收稿日期:2005-05-04

基金项目:国家自然科学基金(60173037, 70271050); 江苏省自然科学基金(BK2005146); 江苏省自然科学基金预研项目(BK2004218); 江苏省高技术研究计划(BG2004004, BG2005037); 国家“八六三”高科技项目(2005AA775050); 江苏省计算机信息处理技术重点实验室基金(kjs050001)

作者简介:何向荣(1958—), 男, 安徽池州人, 讲师, 研究方向为计算机软件和应用。

这将延缓系统对于新的人侵行为的响应。

1 目前入侵检测和响应中的自适应技术

上文提到的问题都和入侵检测系统所保护的系统环境的开放性和多变性有关,如果能够将自适应技术利用起来,可以获得很好的效果。但由于人们忽视了自适应性在这方面的优点,到目前为止对于如何在这些系统中支持具有自适应性的检测和响应的能力的研究工作还很少。目前的系统支持的自适应性主要集中于表示入侵行为的学习和发现模式。一些系统具有较高的自适应性,它们能根据系统的当前状态来调整它的保护状态。例如当检测系统认为当前的系统环境是安全的时候,它就自动配置使得自己占用的系统资源达到最小;而当系统被攻击的时候,它又自动配置到全面监测状态。另外一些系统则通过一种协议来实现,这个协议允许检测系统根据当前检测到的威胁性来动态调整其内部的一个入侵检测组件与其他入侵检测组件之间的协定。

随着入侵检测系统的不断发展^[2],其中大部分的系统都针对入侵行动提供了响应机制。这些响应系统可以分为 3 类:通知系统、人工响应系统、自动响应系统。大多数入侵检测和响应系统都采用通知系统,它仅仅用于生成报告和发出警报。一些系统提供了额外功能,系统管理员可以通过使用一个预先编制的有限的响应集合来启动一个人工的响应机制。尽管这种功能比单纯的通知系统更有效,但是在入侵行为被检测出来到响应机制被启动之间仍然存在一个时间间隙。自动响应系统则通过预编制的响应机制对入侵立即做出响应。一般的自动响应系统使用一个简单地判决表来将一种特定的攻击方式与特定的响应机制联系起来。一旦攻击发生,响应机制立即执行,这种预编制的响应机制就可以简单地执行一条命令而不需要调用一系列的操作来限制攻击者的危害。然而也有的自动响应系统是例外的。它们提供了一定程度的实时自适应响应,使用一个专家系统来选择合适的响应机制并可随正在发生的攻击的可疑程度的变化而改变,将不同的响应同不同的可疑等级关联起来,系统就可以针对不同程度的可疑行为来调整它的响应机制。

现有的入侵响应系统不能根据对入侵检测系统生成的入侵检测报告的有效性的可信程度动态调整响应机制^[3],也不能根据已使用过的各种不同的响应机制实际的成功率来进行调整。

2 移动代理入侵检测中的自适应技术

首先,文中提出基于代理^[4]的自适应分层入侵检测系统(AAHIDS),它具有完全分布式、多代理的体系结构。

整个系统中包括了几个主要的组件:管理代理(MA)、监督代理(DA)、备用代理(SA)、工具代理(TA)。系统的框架结构如图 1。

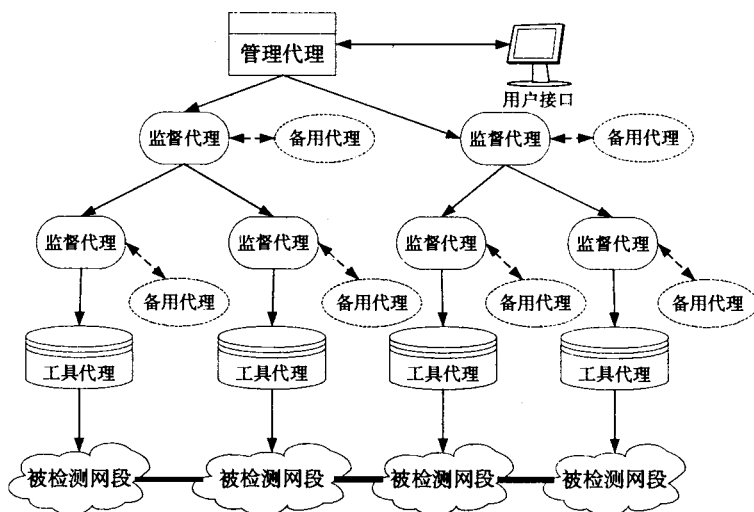


图 1 入侵检测系统框架图

管理代理提供了用户与入侵检测系统间的操作接口,负责管理最顶层的监督代理(DA)。监督代理负责在网络中检测入侵行为。当网络规模较大时,将网络根据拓扑结构来划分层次结构,由多个 DA 分别进行控制,每个 DA 负责一个子网中的检测。同时最底层的 DA 负责管理一个工具代理(TA)的集合。每一个 DA 都与一个 SA 相关联。这些 SA 驻留在网络中,一旦 DA 出现问题不能完成检测任务,对应的 SA 就会自动替代 DA 来执行相同的功能。使用 SA 既解决层次管理结构中的缺点,如单点失效性,同时又继承了层次管理的优点。

底层的工具代理 TA 则封装了许多不同类的入侵检测系统的功能,因此它们可以使用各种不同的方法来分析由传感器发送来的大量数据。每一个独立的 TA 检测侧重的对象角度各有不同,可以是主机、路由器、交换机等等,也可以是一个或多个网段。TA 和系统中的其他代理一样是高度自治的,可以独立完成一定的功能。

工具代理与负责管理它的 DA 及对应的 SA 之间的通信使用基于通用入侵描述语言(CISL, Common Intrusion Specification Language)的通信方法,原始事件信息(审计踪迹记录和网络数据流信息)、分析结果(系统异常和攻击特征描述)以及后文所涉及的响应提示(停止某些特定的活动或修改组件的安全参数)等都可以使用这种语言加以描述^[5]。

上面提到的 AAHIDS 在以下 3 个方面提供了检测的自适应性:

(1) 它通过动态调整负责执行入侵检测任务的系统进程在系统中所站资源数量来提供自适应性。这里存在一个矛盾,即系统总的资源数量一定的情况下,负责运行有效工作的资源与负责系统安全工作所占用的资源之间的矛盾。在一段时间内,如果观察到系统受到威胁的可

能性较低,那么只需要提供一小部分系统资源负责入侵检测。然而如果一段时间内系统受到威胁的可能性较高,则显然需要分配更多的资源来保护系统安全。在 AAHIDS 系统中就可根据危险等级来决定资源的占用率,从而使系统资源得到最大程度利用的情况下保证系统的安全性。

(2) AAHIDS 系统还会根据系统所处环境来动态调整不同的底层入侵检测代理的组合。当给定的系统条件发生变化时,负责入侵检测的系统资源会相应增加或减少,入侵检测所需的各种不同类型的底层入侵检测代理也需要相应的发生变化。例如当一种特定类型的攻击行为不断发生时,IDS 需要调用更多的用于检测这种攻击行为的代理来检测入侵行为。

(3) 最后 AAHIDS 系统对自适应性的支持还可以通过调整与底层检测代理相关的置信度。所有的 IDS 都能够产生误警(false positive)、漏报(false negative),遗憾的是在这些系统中大部分误警和漏报一般都不能转换成相应的优先级。解决的方法是 IDS 跟踪这些底层代理的执行效果并维护一个与之对应的置信度。

3 基于移动代理的入侵响应中的自适应性技术

针对传统响应系统中存在的问题,文中也提出了一个基于代理的自适应入侵响应系统(AIRS, Agent-based Adaptive Intrusion Response System)^[6],其总体框架如图2所示。

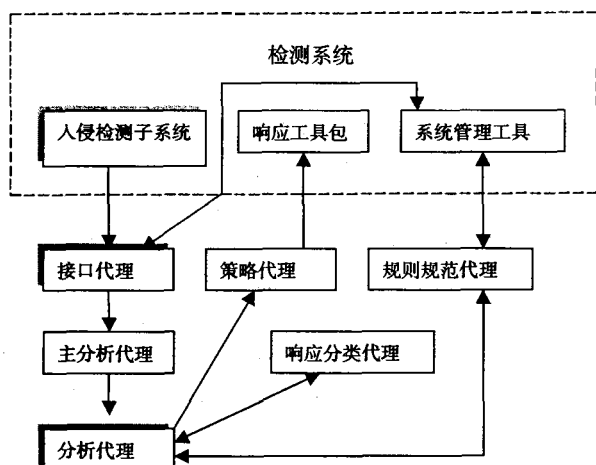


图2 入侵响应系统框架图

使用多个子 IDS 同时监视一个目标系统并在入侵行为发生时产生相应的警报。接口代理(Interface Agent)根据每个 IDS 之前产生的误警和漏报的数目维护一个模型,并使用这个模型产生一个置信度,将其与入侵报告一起发送给主分析代理(Master Analysis Agent)。主分析代理将它们分类,分析它们是原有攻击行为的继续还是一个新的攻击行为。如果这是一个新的攻击,主分析代理就会构建一个新的分析代理(Analysis Agent)来产生相应的响应计划;而如果这是原有攻击行为的继续,主分析代理就会将新的攻击置信度和入侵报告发送给原有的负责处理

这类行为的分析代理^[7]。

分析代理不断分析这个攻击行为直到它被解决并产生一个解决的抽象的操作序列。为了产生一系列响应行为,分析代理必须调用响应分类代理(Response Taxonomy Agent)将攻击行为进行分类,并调用规则规范代理(Policy Specification Agent)以产生响应目标。可以根据法律、道德或者系统资源限制等条件来裁剪响应的结果,然后分析代理将选中的一系列响应行为传送给策略代理(Tactics Agent)。策略代理则将这一系列抽象的行为明确为每一个特定的行动并调用响应工具包(Response Toolkit)中的合适的组件,分析代理和策略代理都会根据前面成功的响应来自适应地做出决定。

上文的入侵响应系统中有3个组件提供了自适应功能:接口代理、分析代理和策略代理。接口代理的自适应性通过修改与各个 IDS 相关的置信度来实现。由于 IDS 不可避免地会产生误警和漏报,所以响应系统必须根据可信程度来判断发生的事件是一次真正的攻击还是一次错误警报。这里的置信度是误警与真实警报之间的比例,每次事件发生以后,系统管理员可以指出这是一次攻击还是一次误警,这样就可以在接口代理与系统管理工具之间形成一个反馈并产生误警的实际数目,从而不断更新与各个子 IDS 系统相关的置信度。最终来自产生了较少的误警的 IDS 的事件可以比产生了较多误警的 IDS 报告的事件获得更高优先级的响应。

分析代理和策略代理也提供自适应性^[8]。一旦分析代理收到进一步的分析报告,就将攻击进行重新分类,并根据新的分类来制定新的计划或修改已经制定好的响应目标。如果更新的步骤可以实现,分析代理也可以用新的步骤来取代计划中的原有步骤。同时分析代理也可以请求策略代理来执行自适应。因为策略代理可以有多种技术来实现制定好的步骤,所以系统可以通过修改相同计划使用的不同步骤来调整自己阻止入侵者行为的手段。最后分析和策略代理还各自维护它们计划和行动的成功度,在解决入侵问题时成功的计划和步骤会获得更高的调用频率。

4 结束语

显然自适应的入侵检测和响应系统比传统的静态、非自适应的系统能够提供更完善的保护。它们能够在更好的保护系统的同时占用尽量少的系统有效资源,并能够有效地减少误警和漏报的情况的发生,克服了传统的入侵检测系统的一些缺陷。但其中涉及到具体问题,如如何准确划分系统的安全等级以便分配相应的有效资源和负责安全检测的资源等还有待进一步研究。

参考文献:

- [1] Spafford E H, Zamboni D. Intrusion Detection Using Au-

```
uint16_t serialnum[10];
struct fakepdetstr * next; //指向下一个检测的 AP
}_attribute_((packed));
```

因为 AP 发送数据包的序列号根据网络的通信情况,在十分钟左右就可能循环一遍,跳变一次,所以只对最近一段时间内的序列号分析情况进行统计,这段时间用 t 来表示,是动态改变的。把 t 细分为相等的 10 小段,每小段的时间长度用 intervaltime 来设置;用 startmarks 来记录 t 与开始检测时间的差(以 ms 为单位)。serialnum 数组用来记录在每小段时间内出现的不符合制定的序列号规则的数据包的数目。在这 10 小段时间中,包括最近捕获数据包的捕包时间的小段内发生的序列号错误累积在 serialnum[endid],统计时间 t 中时间最早的小段内发生的序列号错误累积在 serialnum[startid]。在实际的检测过程中,发现 AP 可能在准备发送的数据包的时候是严格按照序列号递增的,但是发送出来的数据包不是严格递增的。有时先发送了序列号大的管理帧,然后发送序列号小的数据帧,或者先发送了序列号大的数据帧,然后发送序列号小的管理帧,不同的 AP,情况不一样。但是前后两个数据包序列号差值一般在 10 以内,而且管理帧的序列号是严格增加的,数据帧的序列号也是严格增加的。根据这些情况,确定的检测原则是:设立两个标准,一个是检测管理帧序列号的严格增加,用 serialnum 记录已经检测到的管理帧的最大序列号,如果当前检测到的数据包是管理帧,且其序列号比 serialnum 小,则记为一次序列号错误;另一个是,对所有的数据包,用 abserialnum 记录检测到的数据包序列号最大值,如果当前检测的数据包的序列号值与 abserialnum 差值的绝对值大于 30,则记为一次错误。检测中用到的时间关系如图 2 所示。

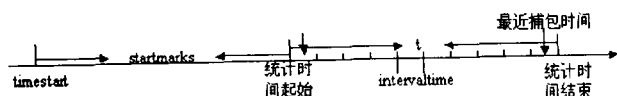


图 2 检测方法中用到的时间关系

检测过程:首先根据数据包源地址,查看是否是要检测的 AP 发出的。如果是,找到对应 AP 的数据结构,根据捕包时的时间和开始检测的时间求差值,由 startmarks 的值,查看捕包的时间是否在统计时间 t 的最后一个时间小

段内,如果不在,需要将统计时间 t 向后移动一个 intervaltime,对应的 endid = (endid + 1) % 10,如果此时 endid = startid,则需要将 serialnum[startid] 的值清零,同时 startid = (startid + 1) % 10,并将 startmarks 增加一个 intervaltime。设 tempoint 为指向检测 AP 数据结构的指针,即: tempoint->serialnum[tempoint->startid] = 0; tempoint->startid = (tempoint->startid + 1) % 10; tempoint->startmarks = tempoint->startmarks + tempoint->intervaltime;

循环进行,直到当前捕包时间落在统计时间段内。然后分析当前的数据包的序列号是否符合标准,如果不符合,将对应的 serialnum 数组内容加 1。最后统计 serialnum 数组的和,如果大于某个值,将 isfakeap 置为 True,同时向用户报警。考虑到突变情况的存在,经过实验测试,把这个值设为 4。

4 结束语

由于目前无线局域网安全的脆弱性,使得无线网络容易被攻击。要保证数据的安全,只采用新的安全措施和标准是不够的。加强无线局域网的检测,及时发现安全问题,并采取措施加以解决,才能更好地维护网络的安全。通过试验测试,文中提出的 MAC 地址欺骗的检测方法具有良好的性能。

参考文献:

- [1] 李庆,梁学俊,江汉红. 无线局域网 WEP 协议安全漏洞研究[J]. 微机发展, 2004, 14(11): 133-135.
- [2] Mishra A, Arbaugh W A. An Initial Security Analysis of the IEEE 802. 1x Standard [EB/OL]. <http://www.memestreams.net/users/jlm/blogid1785350>, 2002.
- [3] Bellardo J, Savage S. 802. 11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions [EB/OL]. <http://ramp.ucsd.edu/bellardo/pubs/userix-sec03-80211dos-html/index.html>, 2003.
- [4] What hackers don't want you to know about securing your wireless LAN [EB/OL]. www.AirMagnet.com, 2004-04.
- [5] Geier J. 无线局域网[M]. 王群, 李馥娟, 叶清扬译. 北京: 人民邮电出版社, 2001.

(上接第 231 页)

- onomous Agents[J]. Computer Networks, 2000, 34(4): 547-570.
- [2] White G B, Fisch E A, Pooch U W. Cooperating security managers: a peer-based intrusion detection system [J]. IEEE Network, 1996, 10(1): 20-23.
- [3] Li Zhitang, Yang Hongyun. A fuzzy intrusion detection model [J]. Computer Engineering & Science, 2000, 22(2): 49-53.
- [4] 晓明, 杨大鉴. 移动代理的体系结构分析[J]. 计算机工程与应用, 2001(1): 62-64.
- [5] Vigna C, Fuggetta A, Picco G P. Understanding code mobili-

ty[J]. IEEE Transactions on Software Engineering, 1998, 24(5): 342-361.

- [6] Tao XianPing, Lu Jian, Dong Huan. Mobile agent: one of the main paradigm of future distributed computing[J]. Computer Science, 1999, 26(2): 1-6.
- [7] 王汝传, 徐小龙. 移动代理安全机制的研究[J]. 计算机学报, 2002, 25(12): 1294-1301.
- [8] 王汝传, 赵新宁. 基于网络的移动代理系统安全模型研究和分析[J]. 计算机学报, 2002, 25(4): 477-483.