第 29 卷第 5 期
1999 年 9 月

东 南 大 学 学 报
JOURNAL OF SOUTHEAST UNIVERSITY

Vol.29 No.5
Sept. 1999

网络安全监测的集成管理*

陆 晟 龚 俭

(东南大学计算机科学与工程系, 南京 210096)

摘 要 根据网络安全统一管理的需要,详细地分析了各种现有的安全监测功能,并对它们加以分类.针对这些功能的不同特点,提出了安全监测集成管理的观点.并分别从体系结构和实现技术支持等不同角度对其进行了详细的阐述.

关键词 计算机网络; 网络安全; 安全监测分析; 安全监测体系

分类号 TP393

网络安全监测的主要目的是检测所保护的网络存在的安全缺陷,并发现可能的非法访问.具体包括安全检测、漏洞扫描等功能.

目前存在各种不同的网络安全监测软件,它们通常仅仅针对安全监测中的特定问题.管理员要保证整个网络的安全性,就需要分别维护各种不同表述方式和处理方式的安全系统,使得网络的安全监测管理工作变得非常繁琐.此外,安全监测功能需要安全管理员在许多主机中分别管理,容易造成不一致性.而且,安全监测工具会随着时间的推移而逐渐过时.因此网络安全管理员始终面临着稳定的安全需求与不稳定的安全工具之间的矛盾.

把握安全监测管理这一变化领域中的不变因素,构造集成的安全监测管理系统,提供一致的安全监测架构,是解决上述矛盾的一个有效方法.通过一致地进行安全监测功能裁剪,统一地进行安全信息的描述和分析,可以把整个域中的安全监测功能统一管理,并根据需要进行功能分布,从而保证安全监测管理的整体性和一致性.本文对网络安全监测集成管理的功能分类和结构模型进行了讨论.

在本文中使用了端系统这个词汇表示网络中能够自主运行的,具有独立处理能力的自治系统.使用安全域表示通过网络互联,能够被统一管理的,在安全上互相依赖的端系统集合.用组件来表示能够独立运行的安全功能(该定义和一般 ID—Intrusion Detection 系统中的定义不同.在一般 ID 系统中,组件指系统自身的功能模块).本文还使用安全结论表示对于系统目前安全状况的一种主观认识或定性评价.

1 安全监测的功能分类

网络安全监测的目标是对网络中存在的安全漏洞和网络中发生的安全事件进行监测,因此至少可以分为检测功能和处理功能两部分.网络安全监测中的检测功能可以被进一步分为

1) 基于网络的安全漏洞扫描功能 这一类功能从系统外部仿照入侵者的行为,使用端口扫描工具和其它针对具体安全漏洞的测试功能,对系统的安全状况进行分析.例如目前比较著名的系统 SATAN, ISS 等.

* 国家"九五"攻关项目(96—743—01—02—06).
收稿日期:1999 - 04 - 06. 第一作者:男, 1974 年生, 博士研究生.

2) 基于网络的安全事件监察功能　这种安全监测方式在 1990 年就已经被提出*,是目前许多安全监测系统的基本形式.这种安全监测功能是在网络上不断监听信息,分析可能发生的各种安全事件.

3) 基于主机的安全漏洞检查功能　这一类安全功能查看系统内部的主要配置文件是否正确,主要文件、程序的权限是否正确.比较有代表性的是 COPS(Computer Oracle and Password System).

4) 基于主机的安全状态检查功能　这一类是对安全状态进行定期检查的功能,例如采用 CRC 校验或 MD5 校验文件,比较有代表性的程序是 Tripwire.这类方法还包括记录系统中的特殊程序,以防止攻击者的后门.

5) 基于主机的安全监察功能　这一类功能通过修改服务器等方式及时查看系统中的事件和状态,这类监察功能的历史从 1991 年就开始了**,例如, courtney 程序可以发现攻击者的端口扫描[1].

6) 基于主机的安全事件记录功能　这类安全功能通常被称为日志采集功能,该功能对系统的各种行为进行记录,并且把这种记录信息保存在日志中供事后的审计之用.如 Axent 的 OmniGuard.

7) 陷井功能　这类安全功能通过提供虚假的环境引诱攻击者上当.

网络安全监测功能中的处理功能往往被检测功能触发,主要包括

1) 安全追踪功能　这种功能一般在实时检测到攻击时采用,用于对攻击者进行反向追踪.因此,这种功能需要被各种实时功能(例如,基于网络的安全事件监察功能、陷井功能等)所激活.

2) 安全事件分析功能　这类功能(日志分析功能)需要和事件记录功能(日志采集功能)联合使用.仅仅记录日志并没有实际的意义,只有对日志进行分析才能够获得需要的信息,因此该功能需要被事件记录功能所触发.不同的事件记录方式会导致不同的事件分析方式.

3) 安全事件报警功能　这是安全事件的处理功能中最简单直接的一种,也就是向管理员报告所发现的安全事件,要求管理员具体处理.

4) 安全状态配置功能　这类安全功能对系统进行自动配置,其目的是将系统的安全状态维持在某一设想的水平.这种功能并不需要被其它功能所触发.可以使用的手段有:修改配置文件、修改权限等等.例如 Axent 的 Enterprise Security Manager 等.

5) 安全状态修复功能　如果系统的安全状态不能够满足要求,该功能能够对安全配置进行自动修改,以期达到设定的安全状态.这种功能是对安全事件最大程度的处理方式.

2　安全监测管理的结构模型

网络安全监测集成管理的基本思想是:构造安全监测功能的集成框架,实现安全监测功能的组件化,根据系统的安全目标来确定安全监测功能需求,从整体角度考虑网络的安全性能和进行安全监测功能的选择.使用这种集成思路的理由是:网络安全和系统安全涉及的内容非常广泛,系统存在的漏洞变化很快,原有的漏洞会不断被修补,新的漏洞会不断被发现.攻击者会逐渐熟悉系统的监测机制,从而制造或发现新的漏洞,所以封闭的、专用的监测系统的生命力就相当有限,需要系统能够不断增加监测能力.

---

* Heberlein L. A network security monitor. IEEE Computer Society Symposium: Research in Security and Privacy. 1990. 296 ~ 303

** Snapp S, Dias R Brentano J, et al. System for distributed intrusion detection. IEEE COMPCON'91. San Francisco, CA(USA). 1991. 170 ~ 176

从层次结构上看网络安全监测功能的集成管理结构如图 1 所示.

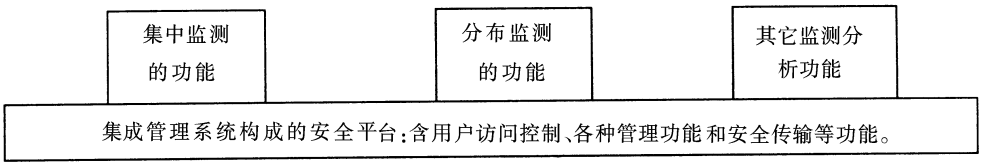

图 1　网络安全监测功能的集成管理结构

支撑平台构成了具体安全功能的运行环境,不同运行方式的安全功能均可以方便的加入整个体系结构中,并且能够获得良好的支持.

从分布结构看,监测功能可分为集中式和分布式两种.集中监测功能主要有基于网络的安全漏洞扫描功能、基于网络的安全事件监察功能等,其控制方式是由独立的一台主机对整个域进行安全监视和测试,因此安全功能仅涉及一个称为安全服务器的主机.分布监测功能主要包括各种基于主机的安全监测功能以及陷井功能,通常在每一个被保护端系统中安装测试功能,通过各自的测试功能对监测端系统的安全进行监测.

分布监测可以获取端系统内部的情况,例如系统文件是否被修改等,因此可以更容易地区分非正常活动;但是需要在各个端系统中安装,受端系统平台的影响.集中监测可以对端系统的安全性作外部测试,还可以对信道上的报文进行分析.由于安全服务器是专职主机,因此可以有较多的资源运行安全监测系统.但是集中监测受监测程序立足点的限制,无法获得某些内部信息.考虑到安全监测所产生的系统开销,应尽可能把监测功能集中于安全服务器上,在端系统中的安全测试功能则应该简单,不应对系统性能有明显的影响.

把两者的优点合并,并互补地使用,可以在不对网络和端系统性能有影响的情况下,把整个安全域的安全监测功能统一管理,以实现安全域安全监测功能的集成,如图 2 所示.

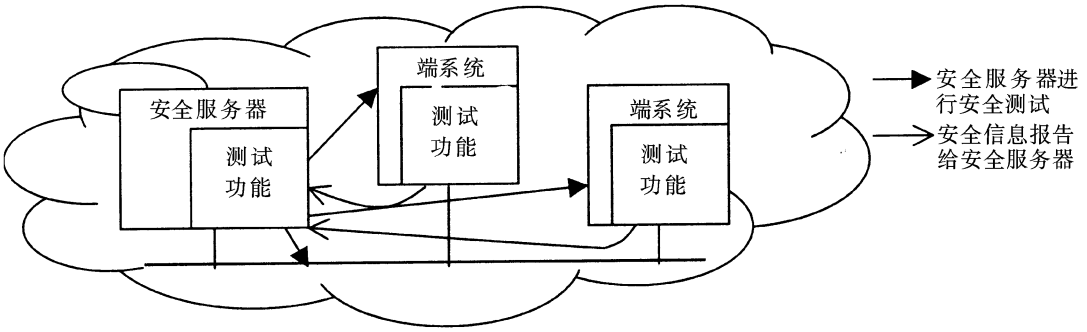

图 2　网络安全监测功能的集成管理方式

3　安全监测的集成框架

3.1　基本模型

由于各种安全监测功能的运行方式、获得信息的方法以及产生的结果几乎都是不同的,因此安全监测的集成管理需要考虑 2 个方面:运行方式(控制流)和运行结果(数据流).

在规范了安全监测功能的运行方式之后,使用安全政策管理机制全面控制整个安全域的安全功能,维持安全策略的统一.在规范了安全信息的结果形式后,使用形式化手段全面分析整个安全域的状况,得出合理的安全结论,减少人工的大量信息分析.如图 3 所示.

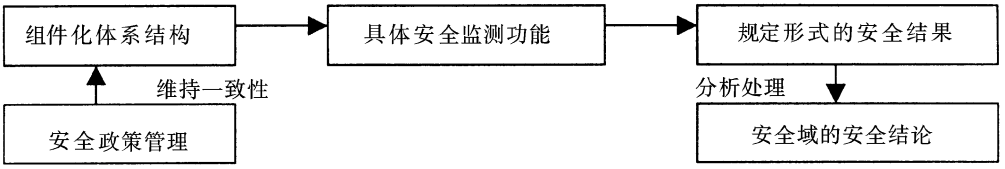

图 3 网络安全监测功能的集成

安全政策管理和安全结论的产生都是比较复杂的问题,需要专门分析,因此将另文讨论.

组件是安全功能的运行单位.安全监测集成框架就是为不同的组件提供合理的运行支持,能够在适当的时间和位置启动组件,能够把组件产生的安全信息及时有效地汇总处理.

3.2 运行方式的规范

运行方式的定义可以被分解成通用定义部分和具有自身特点的定义部分.通用运行方式定义可以包括:功能分布的位置(集中或分布、具体分布的端系统)、功能运行的方式(一直执行、手工执行、定期执行或触发执行)、定期执行功能的运行频度等.自身运行方式的统一则比较复杂,需要用各种规范或者形式化技术处理.

第 1 节中描述的各种安全监测功能以运行方式分类可以分为

1) 独立运行(standalone)方式 这一类的安全监测功能能够单独运行,无时无刻地观察系统的安全状况,实时发现问题并调用各种处理功能.

2) 定期运行(timer)方式 这种类型的安全测试功能按预定义的周期定期运行,通常对系统负荷的影响比较小,管理员可以根据需要提高或者降低运行的频度.

3) 触发运行(trigger)方式 这种运行方式和被其它功能触发方式不同,这种运行方式是被安全事件所触发.以这种方式运行的安全功能开销小、信息的可靠性高,但是获得的信息不全面.

4) 被其它功能触发方式 第 1 节中枚举的各种安全处理功能都能够被其它安全功能所触发,它们的运行方式取决于在整个安全监测功能体系结构中的上下文位置.简单地说,就是如何被触发、被谁触发以及产生的结果交给谁的问题.

组件的运行方式和分布方式可有表 1 所示的组合.

表 1 组件运行方式和分布方式的组合

集中式,独立执行	集中式,定期执行	集中式,触发执行(不存在)	集中式,被其它组件触发
分布式,独立执行	分布式,定期执行	分布式,触发执行	分布式,被其它组件触发

安全功能分布的简单方法是使用安全服务器和安全代理体系,这种体系提供了功能集中或分布的灵活性.在安全代理上安置各种分布功能,在安全服务器上实现各种集中功能.

3.3 安全信息的规范

安全结果的规定也同样需要形式化技术支持,否则无法把各种迥异的安全信息统一描述和处理.目前没有标准的安全信息描述方法(IETF—Internet Engineering Task Force 的 IDWG 工作组正从事有关工作,但还没有草案提出),各个安全监测工具都使用自行定义的方法.

最简单的安全信息描述方法是保存获取信息中的各种事件型信息,忽略其中的统计型信息.如果采用元组的方法可以简单表示为:

1) 安全信息的动态特性说明安全信息反映的是静态安全漏洞还是动态的安全事件;

2) 安全信息的时间特性可以包括安全信息的时间以及安全信息是否实时;

3) 安全信息的目的特性是安全信息涉及的客体以及该信息所关联端系统,如受害主机;

4) 安全信息的源点特性就是安全信息涉及的源点;

5) 安全信息的描述特性用于详细勾画安全信息,例如安全信息产生的原因、安全信息的产生者、安全信息的紧急程度等等,也可以包含安全信息的自然语言说明.

4　功能分布所引入的新问题

网络安全监测功能的分布提供了监测管理的便利和全面的监测信息.但是,功能的分布同时也增加了对统一管理平台自身安全性的挑战.如果安全管理功能在一个端系统内部,则能够控测端系统边界和内部的安全漏洞和功击,有的安全管理功能还能够对系统作出安全配置.但是无论如何都可以被端系统边界所保护,只要安全管理功能能够保护好端系统边界就可以保护自身.但当进行安全域的安全监测集成管理时,安全监测系统的管理能力却横跨在整个安全域中,例如,由于需要安全信息的汇总,信息的传输就有可能被攻击.因此安全监测系统本身也成为一个攻击目标.如果安全监测系统对端系统有控制能力,攻击者便有可能间接控制端系统.

安全域安全监测功能的集成管理系统要能够保证自身的安全,因此需要包含:用户鉴别、访问控制、安全传输等安全功能.这些仅仅是为了满足功能安全性的要求,系统还需要具备实现的安全性,能够防止欺骗、防止服务器失效攻击.此外安全系统本身的隐蔽性和生存能力也必须被考虑.

5　结　论

传统的安全监测功能之间缺乏关联的能力,导致管理员无法全面管理整个安全域的安全,造成安全监测系统过于复杂和难以维护.使用安全域的安全监测集成管理框架可以统一完整地管理整个安全域的安全.

安全域中安全监测功能的集成原则是把集中的监测功能和分布的监测功能通过一个安全管理平台统一管理起来.具体的集成方法是规范安全功能的运行方式和结论描述方式,实现安全监测功能的组件化,使其可以统一地存在于安全域的安全管理平台之上.

但是安全域的集成管理在引入利益的同时,也对安全管理本身带来了新的挑战,需要通过提供额外的安全支持功能,并且更加注重系统本身的实现加以克服.

参　考　文　献

1　Derek Atkins. Internet 网络安全专业参考手册. 严　伟,刘晓丹,王千祥等译. 北京:机械工业出版社, 1998. 318

Integrated Network Security Auditing Management

Lu Sheng　　Gong Jian

(Department of Computer Science and Engineering, Southeast University, Nanjing 210096)

Abstract: Based on the need of integrated security management, current security auditing funcitions are analyzed and classified. According to the different features of these functions, an integration model of security auditing management is suggested. The architecture and implement technique of this model are illuminated in detail. At last, some problems related are discussed as well.

Key words: computer network; network security; security auditing; security archiecture