基于多源异构传感器的网络安全态势感知系统结构研究

赖积保[1,2] 王 颖[1,3] 王慧强[3] 郑逢斌[1] 周 兵[1]
(河南大学计算机与信息工程学院 开封 475004)[1] (中国科学院遥感应用研究所 北京 100101)[2]
(哈尔滨工程大学计算机科学与技术学院 哈尔滨 150001)[3]

摘 要 针对大规模网络安全监控需求,采用"分布式获取,分域式处理"的思想研究基于多传感的网络安全态势感知系统框架结构,并在此基础上给出系统的环形物理结构和层次概念模型;该框架结构自下而上依次分为"信息获取层-要素提取层-势决策层"3个层次,对每个层次所涉及的模块进行详细设计,并给出多源异构安全信息XML格式化的解决方案。该结构是一个开放、可扩展的环形结构,能有效地降低系统实现复杂性,避免单点失效问题。此外,还从整体上明确了层次与层次、组件与组件的关系,以指导工程实践和关键技术的进一步开展。

关键词 网络安全,态势感知,异构传感器,体系结构
中图法分类号 TP393 **文献标识码** A

Research on Network Security Situation Awareness System Architecture Based on Multi-source Heterogeneous Sensors

LAI Ji-bao[1,2] WANG Ying[1,3] WANG Hui-qiang[3] ZHENG Feng-bing[1] ZHOU Bing[1]
(School of Computer and Information Engineering, Henan University, Kaifeng 475004, China)[1]
(Institute of Remote Sensing Applications, Chinese Academy of Sciences, Beijing 100101, China)[2]
(College Computer Science & Technology, Harbin Engineering University, Harbin 150001, China)[3]

Abstract Combined with the large-scale network security monitor application requirements, network security situation awareness system(NSSAS) architecture based on multi-sensors was studied with using the idea of 'distributed acquisition, multi-domain processing', and then the corresponding ring physical architecture and hierarchical conceptual model of NSSAS were put forward. The architecture of NSSAS is composed of three levels, including information acquisition level, element extraction level and situation decision-making level from bottom to top successively. The modules of every level were designed in detail, and the solution of multi-source heterogeneous security information XML format was given. The NSSAS architecture based on multi-sensors is an open and extensible ring architecture that can reduce system implementation complexity and avoid single-point failure problem. At the same time, it can clearly describe the relationship among levels and components, and guide the development of engineering practice and key technologies.

Keywords Network security, Situation awareness, Heterogeneous sensors, Architecture

随着网络规模的不断壮大,网络得到了广泛的应用,而随之而来的安全问题也越来越受到重视。早期的IDS, Firewall, VDS等在一定程度上缓解了安全问题,但随着网络规模和应用需求的不断变化,很多机构和组织已经开始意识到仅依赖于某些安全产品无法有效地保护整个网络的安全,亟需构建一个统一的网络安全集成平台,用于解决异构安全设备之间的信息处理问题,进而及时调整安全策略,以满足网络安全动态性和整体性需求。

网络安全态势感知系统(NSSAS)框架结构是构建安全集成平台的基础,相关研究成果较少[1]。而大部分研究集中在网络安全管理方面,所采用的组织结构主要有集中式处理结构[2]、层次式结构[3]、协作式结构[4]和移动代理结构[5,6]。表1比较了现有不同拓扑结构下的网络安全管理系统。借鉴已有网络安全管理系统结构的优点,运用到网络安全态势感知系统框架结构中,本文提出一种基于多源异构传感器的NSSAS框架结构,并给出了对应的系统物理结构和概念模型,详细描述了框架结构"信息获取层-要素提取层-态势决策层"的设计思路,为进一步研究关键技术提供指导。

表1 不同拓扑结构下的网络安全管理系统结构对比

拓扑结构	优点	缺点
集中式	结构简单,易于管理,结果延迟较小	存在单点失效,网络规模小

到稿日期:2010-04-12 返修日期:2010-07-13 本文受国家863计划(2007AA01Z401),国家自然科学基金(90718003,60973126)和省部共建河南大学科研项目(SBGJ090602)资助。

赖积保(1982—),男,博士,主要研究方向为网络安全、空间数据处理等,E-mail:laijibao@163.com;**王 颖**(1982—),女,博士生,主要研究方向为人工智能等;**王慧强**(1960—),男,教授,博士生导师,主要研究方向为信息安全、自律计算等;**郑逢斌**(1963—),男,教授,主要研究方向为自然语言理解、空间数据处理等。

层次式	网络规模大，实现较简单	存在单点失效，结果延迟较大
协作式	网络规模大，无单点失效	结构复杂，难于实现，结果延迟大
移动代理	网络规模大，网络负载小	结构复杂，难于实现，资源开销大

1 网络安全态势感知系统结构

网络安全态势感知系统的功能需求可简要地描述为：1）能实时监控和采集网络、服务、系统软件以及应用的安全状态数据，及时发现网络攻击行为或其他安全异常，支持大规模网络的安全态势感知；2）能融合、关联来自多种安全事件源的海量数据，通过综合分析判断网络攻击和其他事件的类型，确定攻击行为的性质和可能造成的影响，并及时报警和预警；3）能集中监控系统的安全态势，融合生成全局安全态势，提供多角度、多尺度的安全态势表示，实现统一态势图的集成。在明确系统功能需求的基础上，接下来分别给出基于多传感器的网络安全态势感知系统框架结构、物理结构以及概念结构。

1.1 系统总体框架结构

图1给出了网络安全态势感知系统框架结构。此结构是一个分布式开放结构，采用的主要思想是“分布式获取，分域式处理”，可分为信息获取层、要素提取层和态势决策层3个层次。信息获取层通过部署所设计的日志类传感器、SNMP传感器、NetFlow传感器和服务传感器，获取网络环境中主机、交换设备、安全设备等各种异构信息；要素提取层针对所获取的各种异构信息，采用聚合和融合方法对其进行必要的数据精简和安全事件提取；态势决策层采用层次评估思想和非线性时间序列预测方法分别完成多源信息的综合理解和动态预测，为上层用户提供直观的安全态势视图。信息获取层、要素提取层和态势决策层的实现都需要与相应的数据库进行交互。数据库包含事件库、资产库、网络信息库、知识库等，这些数据库的形成需要专家、安全管理人员以及网络扫描器等进行辅助。

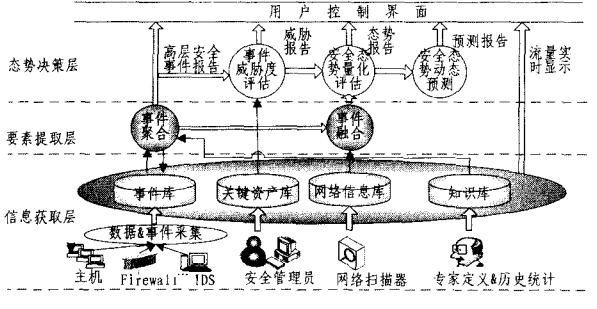


图1 网络安全态势感知系统框架结构

整个系统框架结构形成一个由安全“监控-分析-决策”组成的感知环。安全监控由多类传感器来实现，各个传感器通过实时获取各个设备的安全状态数据，实现对整个网络的监控；安全分析通过对所获取的信息进行过滤、验证和融合来实现对数据的分析；安全决策通过对整个网络安全的态势评估和态势预测来完成。

1.2 系统物理结构

图2给出了系统物理结构图。此结构中包含传感器、分析器、决策器以及相应的数据库。每一个安全域内都包含若干传感器和一个分析器，而在全局安全域中除包含有传感器和分析器外还有决策器。传感器负责监控主机或本地网络并向分析器发送异常行为或者可疑行为报告。分析器负责接收本地传感器的数据，并将分析后的结果发送至全局数据库。决策器依据各安全域的分析结果进行高级综合处理，得出整个网络的安全状况，并存入数据库中。传感器与传感器之间采用环形连接，旨在通过传感器之间信息的互补来提高各传感器的初步分析能力，达到精简数据的目的；分析器之间也采用类似的连接，便于提高要素提取的精度和全局策略的统一下发；分析器与传感器之间采用双向交互的模式，一方面传感器主动向分析器提交所获取的信息，另一方面分析器可以通过下发指令重新配置传感器或探询传感器状态信息；所有局部分析器的分析结果除了需要存储在本地外，还必须通过加密通道传送至远端集中控制中心数据库，与全局分析器所得结果一并提交给决策器。

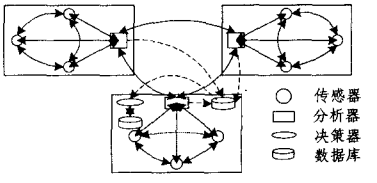


图2 基于多传感器的网络安全态势感知系统物理结构

由于大规模网络分布范围广、节点多，所提供的应用服务、所采用的操作系统与网络设备具有多样性的特点，因此应用多级信息融合与决策技术，通过部署多源异构传感器来实现分布式网络的全局、实时、动态的安全态势感知，使其具有自适应、自学习特性，体现分布性与动态性，对内外网均具备动/静态攻击检测能力。此结构不依赖于网络拓扑结构，可对系统进行动态配置和裁剪，以适应各种分布式应用环境和安全需求。此外，此结构能有效地避免单点失效问题并增加系统的灵活性。由于每个安全域内的组织结构仍然采用层次结构，使得在一定程度上降低了整个系统的实现复杂性，便于分布式大规模网络的安全态势感知。

1.3 系统概念结构

依据所提出的网络安全态势总体框架结构，给出其相对应的概念结构，其主要用于反映不同感知层次的数据流向。如图3所示，感知层次由低到高依次包括网络安全态势要素提取、态势评估和态势预测，对应的输入分别是数据信息、特征信息和态势信息。第1层：网络安全态势要素提取是网络安全态势感知的基础，如果无法合理准确地提取态势要素信息，就无法生成正确的安全态势图。该层次的主要任务是从海量多源安全状态数据中提取影响网络安全态势的信息，并转化为统一的XML格式，为网络安全态势评估和预测提供必要的数据支持。第2层：网络安全态势评估是网络安全态势感知的核心，是对当前整个网络安全态势的一个动态推理综合理解过程。通过识别态势信息中的安全事件，依据它们之间的关联关系，计算出服务、主机和网络所受到的威胁，并生成相应的安全态势图，动态地反映整个网络的安全态势状况。第3层：网络安全态势预测即是依据历史网络安全态势信息和当前网络安全态势信息预测网络安全趋势（即已知$T+1, T+2, \cdots, T+n$时刻的网络安全态势，预测$T+(n+1)$时刻的网络安全态势），使决策者能预先掌握可能发生的安全事件，为制定合理准确的决策提供依据。

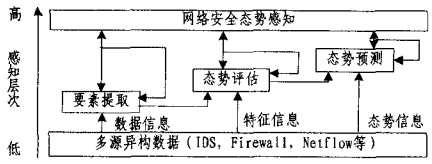


图3 网络安全态势感知概念结构

2 信息获取层

信息获取层位于系统框架结构底部，其主要职能是获取当前网络状况及预测未来趋势所需的态势信息，在系统中发挥着基础性支撑作用。信息获取层可进一步细分为3个子层，分别是设备层、传感器层和信息集成层，如图4所示。信息获取层的结构采用了分层设计，封装各子层的实现细节，分层可保证各子层的相对独立性和透明性，减少各子层的耦合性；与此同时，各层之间通过自底向上的数据流和自顶向下的命令流有机融合为一个整体。

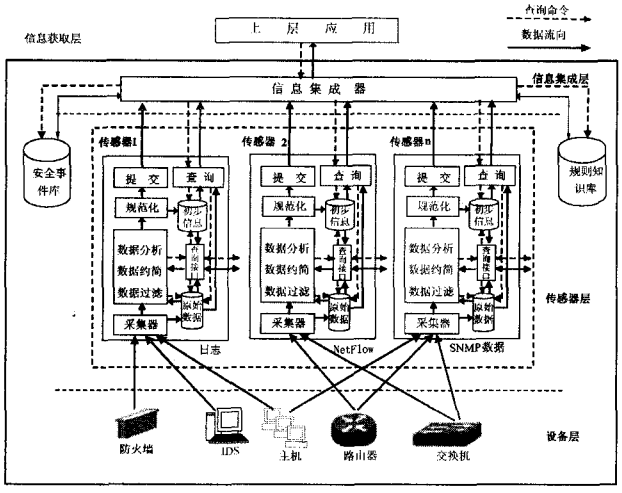


图4 信息获取层结构

设备层是原始数据的来源，设备层设备的选取取决于数据源的选取以及系统目标网络的设备安装和部署情况。数据源的分类和选取将在下一小节中论述。传感器层由多种类型的传感器组成，各传感器之间存在一定的数据互补性。采用统一的接口规范，满足该接口规范的传感器都可以加入到传感器层中。信息集成层具有集成和初步融合来自各传感器的初步信息（安全事件）的功能。另外，由于上层应用需要针对特定安全事件查询判定该安全事件的相关数据，因此信息获取层还需要提供一个面向上层应用的查询响应接口。通过该接口接收和解析上层应用的查询命令，并从安全事件库或传感器初步信息库及原始数据库中查询数据并返回。为了使得信息获取层对上层应用透明，只在信息集成器提供面向上层应用的查询响应接口。

2.1 数据源选取及分类

由于网络系统庞大复杂，运行过程中往往产生海量的多源异构数据，系统限于种种因素几乎不能获取全面、准确和及时的数据。因此，只能选取那些具有代表性、信息量相对丰富、可靠度较高、实时性较强以及冗余度较低的数据作为系统数据源。在选取数据源时，还应充分考虑到各数据源之间存在的交叉与互补特性，尽量扩大覆盖面并避免过度重复。为贯彻上述思想，有必要对数据源进行分类选取，从信息源宿主类型、数据源类型等角度对数据源进行选取和分类。依据数据源选取原则确定了4类数据源，如表2所列。表中并给出了每种数据源对应的信息获取方式。

表2 数据源信息及获取方式

数据类型	来源设备	具体分类	获取方式
NetFlow数据	支持NetFlow的网络交换设备	NetFlow V5 NetFlow V9	UDP方式 SCTP方式
SNMP数据	所有支持SNMP的设备	SNMP V2 SNMP V3	轮询 中断(Trap)
日志	网络交换设备 终端设备 网络安全产品	Widows日志 Linux日志 应用程序日志 IDS日志 防病毒日志 防火墙日志	Widows Log Syslog
服务	网络交换设备 终端设备	关键服务 非关键服务	Nagios

上述4类数据源具有代表性，并且各数据源具备较强的互补性、较小的冗余度和较大的覆盖面，符合数据源选取的指导思想。根据数据源的相对独立性，针对4类数据源分别开发各自的传感器进行获取。需要指出的是，上述4类数据源虽然具有典型性和代表性，但仍没达到全面覆盖。考虑到日后新增数据源，传感器层采用了统一的接口规范，满足该接口规范的传感器都可以加入到传感器层中，这样可获得更好的可扩展性，以便根据需要扩展数据源。下面将分别介绍日志传感器、SNMP传感器、NetFlow传感器和服务传感器。

2.2 日志类传感器

日志类传感器能够采集多源日志并初步分析处理，最后形成格式统一的安全事件格式，为上层应用提供数据，其体系结构如图5所示。日志采集器通过日志采集代理、专用日志访问协议、安全设备的日志输出接口等方式采集关键主机、安全设备以及其他日志。采集器具有可定时自启动并完成采集任务的功能，能够自动从控制模块的配置数据中获取采集参数，包括采集的时间间隔、采集的日志文件存储的路径、数据库配置及传感器编号等信息。日志文件由于具有易损性，很容易被修改或破坏。比较典型的是入侵者入侵后往往会修改或删除与其相关的日志，甚至伪造日志以迷惑网络安全人员。因此在采集器中加入了日志完整性检测模块，在设备日志系统中嵌入日志完整性检测算法，对日志完整性进行检测。采集器收集到的日志不一定全部都用于数据分析，可依据安全规则库对收集到的日志指定过滤条件，丢弃无价值的数据，将注意力集中到所关心的日志上。过滤条件可以从宏观的角度指定日志类型，也可以从微观的角度通过正则表达式进行更精细的过滤。预处理器还会依据安全规则库合并指定时间片内的重复日志，删除大量存在的冗余事件。日志的过滤和合并是依据特定的规则及采集策略在日志采集解析时直接完成，即对已经采集到的日志按照规则知识库中的规则执行过滤功能，然后按照数据合并算法以时间片为单位对存入临时数据库中的日志进行合并，将经过预处理后的日志上传给数据分析模块。日志分析模块包括日志的实时处理及离线分析两个部分。实时处理的分析算法相对简单，只需要分析处理过的日志的安全性即可；而离线分析部分要加入复杂的关联分析算法，最大范围地挖掘及初步融合日志所提供的有效信息，分析系统的安全性，并形成完整的事件，通过安全事件生成模块把提交上来的日志转化为统一格式的安全事件描述提供给上层应用。

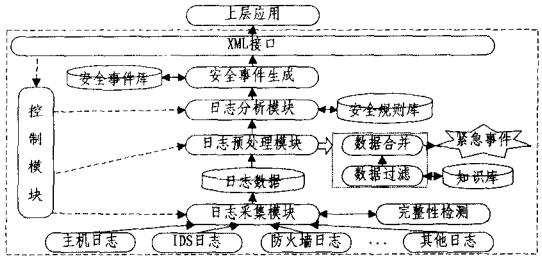


图 5　日志传感器结构

2.3　SNMP 传感器

SNMP 传感器根据 SNMP 协议实时采集网络内网络交换设备和终端设备等可控设备 MIB 库中的相关数据，并对其进行分析，可获得网络拓扑信息、网络流量信息和安全事件信息等系统的所需信息，并以规范统一的格式提交给上层应用或网络管理员。SNMP 传感器结构如图 6 所示。SNMP 数据采集模块负责实时采集网络设备中 MIB 库数据，获取各网络设备 MIB 中的态势数据，进而将其传递给数据分析模块。数据采集主要是通过定时轮询采集，由 SNMP 传感器动态地对每类态势数据的采集设置不同的轮询时间，然后用时间触发器控制，每隔一段轮询时间采集一次数据，把采集到的数据送往数据分析模块进行相应的分析处理。网络拓扑发现模块通过 SNMP 协议访问 MIB 获取网络拓扑发现的相关信息。首先通过 SNMP 协议访问直接相连的交换机的 ARP 表和 MAC 地址表，关联 ARP 表和 MAC 地址表，从而获取与交换机相连的网络设备的 IP 地址。其次，确定这些网络设备的存活性：如果存活，则通过 SNMP 协议继续访问这些网络设备，并区分网络设备的类型；如果网络设备类型为交换机或者路由器，则重复上述步骤，直至最终的网络设备是个人计算机。通过上面的步骤，可以分析出目标网络的物理层拓扑结构。流量图形显示模块用图形直观地反映网络流量信息。该模块通过特定算法计算网络流量，并通过动态的数据折线图直观地表示网络流量的实时变化情况。该模块具有自动调整、缩放、保存和打印等功能，并可以同时显示多个监控流量窗口，可以比较精确地显示出网络流量值。网络性能分析模块需要利用一定的算法对这些原始数据进行分析，可以选择对出错率、平均利用率和总吞吐量等项设置阈值，当达到一个特定的出错率或使用率时，形成报警事件并提交上层。

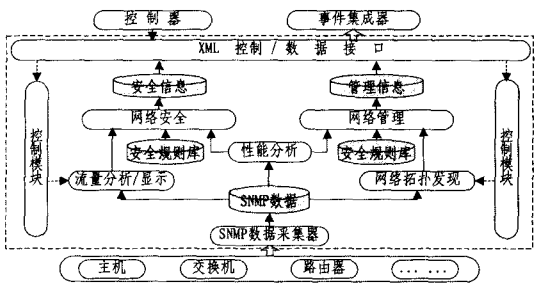


图 6　SNMP 传感器结构

2.4　NetFlow 传感器

NetFlow 传感器负责采集网络交换设备产生的 NetFlow 数据，对其进行统计分析。由于该类传感器不需要对网络数据包内容进行分析，大大减轻了传感器运算处理的负担，因此非常适合用来在全局上实时监测大规模高速网络。NetFlow 传感器能够实时或近实时地提供多层次、多角度、多粒度的流量信息、全方位的网络连接信息，以及对上述信息进行分析得出网络事件信息等系统所需要的信息，具有视角宽广、信息量大、实时性强等优点，适合于网络安全态势感知系统的信息获取部件，其结构如图 7 所示。收集器是接收路由器或三层交换机输出的 NetFlow 信息部件，是传感器的基础模块。流量信息获取模块是对全部的 NetFlow 数据进行统计分析，给出当前网络的流量信息。该模块提供的流量信息分为 3 个层次，从宏观到微观依次排列为自治域之间的流量信息、路由器间的流量信息（包括网内路由器间，网络边界路由器与网络外围相邻路由器间）、主机间的流量信息，并对这 3 个层次的流量信息都给出特定服务的数据量、数据包数和网络流数，而传统的基于 SNMP 的流量测量方法是做不到的。安全事件信息获取模块是 NetFlow 传感器的核心模块，该模块采用基线检测法与特征检测法相结合的层次化检测法来检测安全事件，并结合流量信息获取模块所获取的流量信息进行分析，生成安全事件警报。规则库存放分析模块所用的规则，包括分析规则和事件规则，其中事件规则又分为异常事件规则和正常事件规则。为规则库中的每一条规则设置可信度，以表征该规则判断事件的准确程度。分析模块根据规则库中的分析规则分析当前流记录，得出其特征并与规则库中的事件规则进行匹配，如果匹配为异常事件，则上报给系统上层。控制模块主要负责解析传达系统上层部件对传感器的控制信息和反馈信息。控制流量测量模块提供流量信息的时间粒度、控制流量信息的类型；控制分析模块应采用的分析方法、对传感器所提出的安全事件警报进行反馈等。XML 控制/数据接口模块的功能是提供一个便于传感器和上层系统交互的统一接口。XML 是新一代数据交换语言，具有很强的可扩展性和可交互性。因此，采用 XML 设计的控制/数据接口将保证传感器与上层系统交互的简易性，保证传感器的可扩展性。

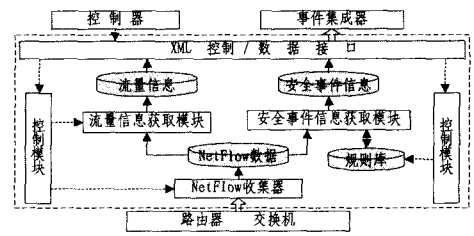


图 7　NetFlow 传感器结构

2.5　服务类传感器

服务类传感器负责监视和采集服务的安全状态数据，对其进行分析并刻画关键服务的运行状态。在服务发生严重偏离或失效时，以事件的形式报告给上层应用系统或网络管理员。服务传感器是系统重要的信息获取部件之一，能向上层管理者提供关键服务的运行态势，还能为其它传感器的数据分析提供参考依据。图 8 给出了服务传感器结构。

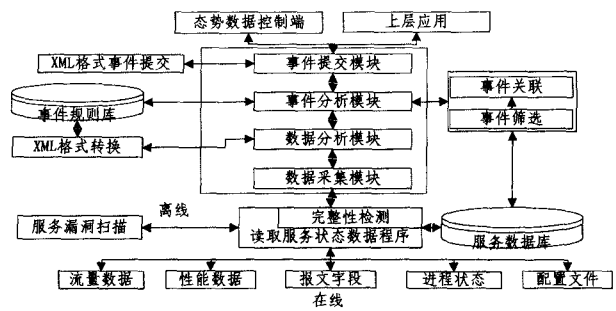


图 8　服务传感器结构

数据采集模块负责对服务数据源进行在线或离线采集，其中在线采集包括实时读取流量数据、性能数据、服务配置文件信息、关键进程状态信息等，离线采集如漏洞扫描，对服务的漏洞进行扫描并获取服务的漏洞数据。数据分析模块负责对所采集的数据进行分析处理并判断服务状态数据是否异常。如果发现异常，则报告为异常事件。具体方法是对流量数据和性能数据建立正常模型，并得出正常的阈值区间，分析当前服务运行状态数据，计算其偏离度。若服务偏离正常模型，则以事件形式报告异常。事件分析模块对生成的事件进行关联分析，并结合服务本身的漏洞风险情况判断服务的安全态势。由于产生的事件信息很多，存储量很大，需要对事件进行筛选和标注，然后进行事件关联分析。关联分析是将不同的事件联系起来，找出现象背后的更高层次的事件。事件提交模块负责提交 XML 格式化后的异常事件和服务的态势情况（正常、偏离还是失效），便于对服务数据统一访问和其他数据源的集成分析。

2.6 基于 XML 的多源安全信息格式化

各种传感器获取的数据以及初步分析所得到的安全信息之间存在异构性、格式差异大，倘若直接提交，将给上层应用的数据统一存储及融合分析造成较大的困难。因此有必要提出统一的态势信息模型，实现信息获取层提供统一化信息功能。建立统一的态势信息模型主要有以下几个方面的优势：①提供统一的数据结构，简化系统的处理复杂度；②减少系统上层应用程序对多源异构数据处理的开销；③明确多源异构传感器的数据提交需求，对传感器的设计有一定的指导意义；④为上层应用程序提供统一数据格式，提高信息获取层对上层的透明性。现有的公共数据模型主要有 OEM，OIM 和 XML 3 种。在信息获取层中，需要使用公共数据模型即态势信息模型进行定义的数据主要有两类：一类是多源异构数据，将各类传感器采集到的数据统一到 XML 数据模型；另一类是态势感知事件，将传感器分析得出的事件以及信息集成器中融合得到的事件统一表示为 XML。最后，信息获取层向上层应用提供统一化的、反映网络状态的安全数据以及经过分析的网络安全事件。

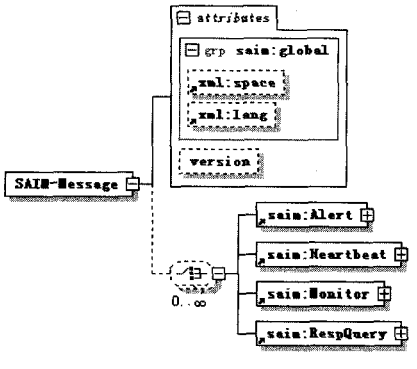


图 9　态势感知信息模型

态势感知信息模型（Situational Awareness Information Model，SAIM）的设计充分考虑了上层应用对信息的需求以及传感器的功能定位。该模型采用树状层次结构，其中树根是顶级元素 SAIM-Message，顶级元素包含版本号属性以及 4 个一级子元素 Alert，Heartbeat，Monitor 和 RespQuery，如图 9 所示。其中 Alert 元素包含传感器报警的具体信息，Heartbeat 元素包含传感器心跳的具体信息，Monitor 元素包含传感器监控的具体信息，RespQuery 元素包含传感器响应的具体信息。各一级子元素包含若干属性以及若干二级子元素。依此类推。

3 要素提取层

要素提取层对信息获取层得到的各种异构信息，采用聚合和融合方法进行数据精简和安全事件提取。图 10 给出了大规模分布式网络的安全要素提取结构图，主要分为局部分析和全局分析两大部分。局部分析是在各个安全域传感器所获取的信息的基础上，首先对其执行 XML 格式化，再采用基于相异度计算方法对其进行局部聚类分析，并对聚类后的结果采用基于指数加权的 DS 证据理论进行融合关联，最终提交到全局分析模块。采用相同的聚合和融合方法完成全局聚合和融合，经过局部分析和全局分析之后便完成了对安全要素的提取[7]。

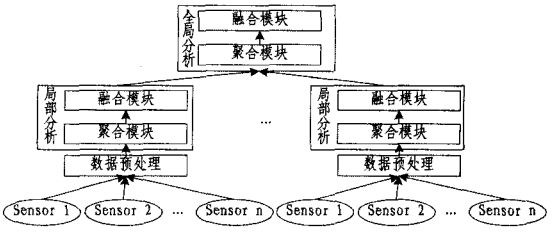


图 10　网络安全要素提取结构

3.1 多源异构安全信息聚合

要素提取层首先对多源异构安全信息执行聚合操作，聚合的流程如图 11 所示。

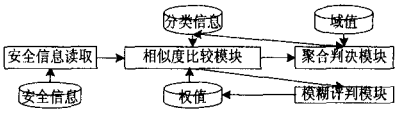


图 11　多源异构安全信息聚合流程

安全信息读取模块从数据库中读取已格式化的安全信息，并输入到相异度计算模块。依据每条标准化安全信息的特征属性分别与分类模板中的结果进行比较，并将结果输入到聚合判决模块中，将满足阈值条件的安全信息划分为同一类别。支持数据库主要有 4 个，分别是标准化安全信息库、分类模板库、权值库、阈值库。分类模板库主要用于指导属性相异度计算和聚合判决，并接收聚合判决更新结果；权值库依赖于专家经验，采用模糊综合评判方法及时更新；阈值库依据历史统计数据给出不同字段对阈值的要求。其中所考虑的特征属性主要有源/目的 IP、源/目的端口、检测时间、攻击类别等，分别计算其相异度，最终计算出综合相异程度。

3.2 多源异构安全信息融合

对安全信息执行聚合之后，采用基于指数加权 DS 证据理论对聚合结果进行融合分析，旨在进一步精简安全信息数量和识别攻击行为。整个融合过程的模块设计如图 12 所示。从分类信息库中获取安全事件信息，并依据不同传感器的检测率分配置信度；传感器权重分配模块依据攻击情况，获取各个传感器的权值；DS 推理模块根据不同传感器具有的不同重要性，综合理解攻击行为发生的概率，给出推理结果并提交至上层的融合判决模块，判决模块依据阈值要求得出相应的结果，存入数据库中，即完成安全要素提取。整个过程主要涉及到 4 个数据库，分别是安全事件分类信息库、传感器权重库、

判决阈值库和安全要素库。安全管理人员可以依据对当前和历史安全事件信息的统计和分析，并结合不同安全域的重要性，动态更新配置传感器权重库。

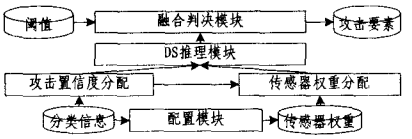


图 12　多源异构安全信息融合流程

4　态势决策层

态势决策层主要由事件威胁度评估模块、安全态势量化评估模块和安全态势动态预测模块构成。事件威胁度评估是为了将高威胁度的安全事件排在所有事件的前面，以便引起安全管理人员的关注，因此安全事件威胁度的划分就显得至关重要。通过设计一个匹配器，即将 Snort 攻击威胁分类情况与安全态势要素提取结果进行匹配，得出结果为高、中、低的安全事件排序情况，直观地呈现给管理人员。接下来重点介绍一下安全态势量化评估和动态预测模块。

4.1　安全态势量化评估

安全态势量化评估模块主要完成整个网络当前安全态势的评估，其流程图如图 13 所示。安全威胁统计模块针对一定时间段内从安全要素库中提取的安全事件进行威胁度统计分析，得出不同主机服务在不同时间间隔内所受到的高、中、低威胁程度的安全事件数量，并将统计结果提交给服务安全态势评估模块；服务安全态势评估模块依据不同时间间隔的重要性分别计算出对应的服务安全态势，存入态势库中；主机防御措施配置获取模块根据不同主机的安全防御机制，结合对安全属性的要求，计算得到相应主机的防御强度，与主机上的服务安全态势一并提交到主机安全态势评估模块；主机安全态势评估模块依据主机上所运行的服务情况，从权值库中读取其对应服务的权值，估计服务相对于主机的安全影响情况，并将其与该主机的防御强度作比较，便可得该主机的安全态势，存入到态势库中，并提交到网络安全态势评估模块；网络安全态势评估模块依据各个主机在网络中的不同地位（即权值），计算整个网络的安全态势情况，并将结果提交到态势呈现模块，把评估结果显示给决策者。支持数据库主要有 4 个，分别是安全要素库、配置信息库、权值库和态势库。

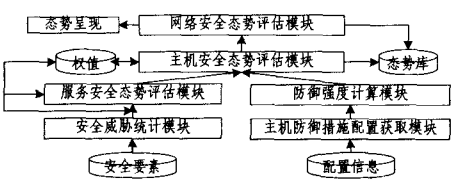


图 13　网络安全态势量化评估流程图

4.2　安全态势动态预测

网络安全态势动态预测模块主要完成整个网络安全态势的前向预测功能，如图 14 所示。获取模块分别从态势库中读取历史和当前网络安全态势数据；历史数据提交给态势预测训练模块，用于模型的训练，而当前数据提交给态势预测测试模块用于模型的测试；评价优化模块依据训练和测试评价结果采用改进遗传算法对小波神经网络预测模型进行优化，直到训练结果满足误差要求，才能确立态势预测模型；态势预测模块将预测结果显示给安全管理人员，用于决策分析。

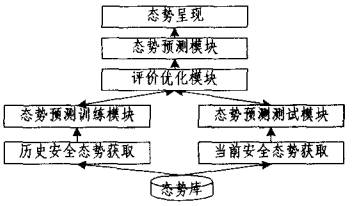
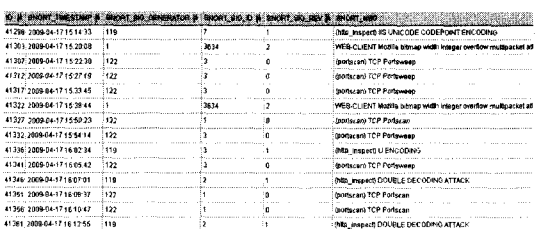


图 14　网络安全态势动态预测流程图

5　NSSAS 结构应用

在 NSSAS 框架结构的指导下，基本实现了信息获取层子系统，并进行了实验验证，结果表明能满足预期要求。在此基础上，正着手对要素提取层、态势决策层进行实现。由于存在较大的不确定性，因此在进行系统设计时充分考虑了可扩展性，尽可能地将层与层之间和各层子系统内部设计成标准化的接口。当需添加新功能时，仅需通过相应接口将其集成到现有系统即可，而无需改变原有系统的其他部分。限于篇幅，下面仅以信息获取层的 4 类传感器为例说明 NSSAS 框架结构的应用。

日志传感器采集的日志种类繁多，并且大都包含事件级的信息，比如 IDS 报警日志；而其他类型传感器所采集的数据较为单一，并且数据通常较为原始。这些特点在设计和实现日志传感器时均有体现。图 15 给出了面向 Snort 所采集到的部分数据。



ID	SNORT_TIMESTAMP	SNORT_SID_GENERATOR	SNORT_SID_ID	SNORT_SID_REV	SNORT_MSG
41298	2009-04-17 15:14:33	119	7	1	(http_inspect) IIS UNICODE CODEPOINT ENCODING
41303	2009-04-17 15:20:08	1	3634	2	WEB-CLIENT Mozilla bitmap width integer overflow multipacket att
41307	2009-04-17 15:22:30	122	3	0	(portscan) TCP Portsweep
41312	2009-04-17 15:27:19	122	3	0	(portscan) TCP Portsweep
41317	2009-04-17 15:33:45	122	3	0	(portscan) TCP Portsweep
41322	2009-04-17 15:38:44	1	3634	2	WEB-CLIENT Mozilla bitmap width integer overflow multipacket att
41327	2009-04-17 15:50:23	122	1	0	(portscan) TCP Portscan
41332	2009-04-17 15:54:14	122	3	0	(portscan) TCP Portsweep
41336	2009-04-17 16:02:34	119	3	1	(http_inspect) U ENCODING
41341	2009-04-17 16:05:42	122	3	0	(portscan) TCP Portsweep
41346	2009-04-17 16:07:01	119	2	1	(http_inspect) DOUBLE DECODING ATTACK
41351	2009-04-17 16:09:37	122	1	0	(portscan) TCP Portscan
41356	2009-04-17 16:10:47	122	1	0	(portscan) TCP Portscan
41361	2009-04-17 16:12:55	119	2	1	(http_inspect) DOUBLE DECODING ATTACK

图 15　Snort 报警日志

SNMP 传感器不但能够提供统一形式的数据来源，而且可与其他类型传感器所获得的数据进行融合分析，达到监测整个网络状态的目的。如图 16 所示，在拓扑图上反映出某局域的安全状态，图中由两个星型网络构成，网络中心是两台交换机，其中右上角星型网络的交换机级联在左下角星型网络之中，绿色代表所监控设备处于正常状态，红色代表所监控设备出现异常行为。

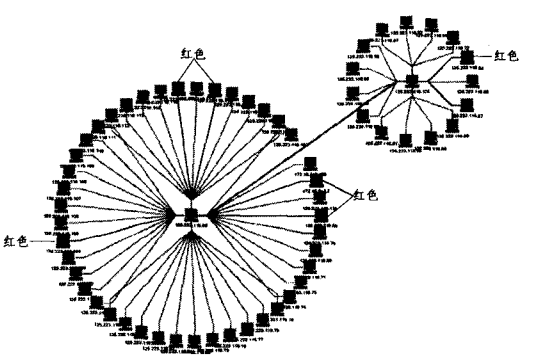


图 16　局域网拓扑图

NetFlow 传感器不仅生成了符合态势信息模型的流量信息，而且实现了流量视图的可视化。流量视图的可视化使得

（下转第 158 页）

based Software Development[J]. American Programmer, 1995, 8(11)
[2] 杨芙清,王千祥,梅宏,等. 基于复用的软件生产技术[J]. 中国科学(E辑),2001,31(4)
[3] 胡海涛,李刚,韩燕波. 一种面向业务用户的大粒度服务组合方法[J]. 计算机学报,2005,28(4):694-703
[4] 房俊,虎嵩林,韩燕波,等. 一种支持业务端编程的服务虚拟化机制 VINCA-VM[J]. 计算机学报,2005,28(4):549-557
[5] Majithia S, David W, Gray W. A Framework for Automated Service Composition in Service-oriented Architectures[C]// 1st European Semantic Web Symposium. Heraklion, Greece, 2004: 269-283
[6] Taylor I, Shields M, Wang I, et al. Grid Enabling Applications Using Triana[C]// Workshop on Grid Applications and Programming Tools. Seattle, USA, 2003
[7] Mandell D J, McIlraith S A. A Bottom-Up Approach to Automating Web Service Discovery, Customization, and Semantic Translation[C]// Proc. of the 12th Int'l. WWW Conference Workshop on E-Services and the Semantic Web. Budapest, 2003: 89-96
[8] Sirin E, Hendler J, Parsia B. Semi-automatic composition of Web services using semantic descriptions[C]// Web Services: Modeling, Architecture and Infrastructure Workshop in conjunction with ICEIS. 2003
[9] Cardoso J, Sheth A. Semantic e-Workflow Composition [J]. Journal of Intelligent Information(JIIS), 2003, 12(3): 191-225
[10] McIlraith S, Son T C. Adapting golog for composition of semantic web services[C]// Proc. of the 8th Int'l. Conf. on Knowledge Representation and Reasoning. Toulouse, France, 2002: 482-493
[11] Shankar R P, Armando F. SWORD: A Developer Toolkit for Web Service Composition[C]// Proc. of the 11th International World Wide Web Conference. Honolulu, 2002: 786-810

(上接第 149 页)

管理员能够更直观地了解当前网络的流量信息。图 17 为局域网的数据流量视图,显示的是流入网段 125.223.118.0/24 的数据流量大小。从图中可以看出,网络的数据流量大约介于 2MB/s 和 5MB/s 之间。图 18 显示 Netflow 传感器事件分析结果,主要是水平扫描和垂直扫描。此外,该类传感器还筛选并保存了安全事件所对应的原始 NetFlow 记录,便于进一步关联和取证安全事件。

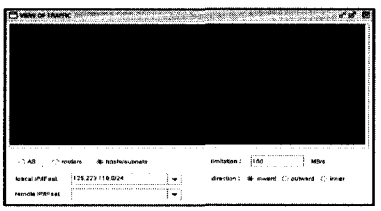


图 17 局域网的流量视图

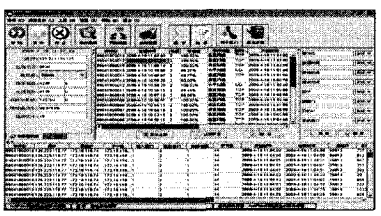


图 18 NetFlow 传感器事件分析结果

服务类传感器针对特定服务,监视和采集服务的安全状态数据,并对其进行分析。在服务发生严重偏离或失效时,以事件的形式报告给上层应用系统或网络管理员。图 19 显示了所监测服务的运行状态数据,主要涉及流量异常、性能异常、报文异常、进程状态异常、配置错误异常等,红色标记为紧急,绿色标记为正常。

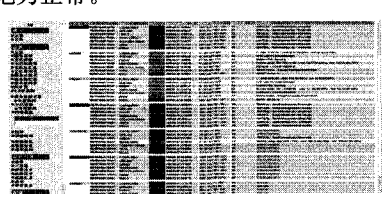


图 19 服务运行状态数据

结束语 本文在分析系统功能需求的基础上,提出了一种基于多源异构传感器的网络安全态势感知系统分层结构,并给出了相应的系统环形物理结构、系统层次概念模型以及各层次的功能实体详细设计。此结构采用"分布式获取,分域式处理"的思想,是一个开放、可扩展的环形结构,域内域间相互协作,能有效地降低系统实现复杂性,避免单点失效问题。此外,还从整体上明确了层次与层次、组件与组件关系,从而指导工程实践和关键技术的进一步开展。下一步在态势评估和预测具体实现中对整个系统架构进行必要的微调和完善。

参 考 文 献

[1] Bass T. Intrusion detection systems and multisensor data fusion: creating cyberspace situational awareness[J]. Communications of the ACM, 2000, 43(4): 99-105
[2] Ganame A K, Bourgeois J, Bidou R, et al. Evaluation of the intrusion detection capabilities and performance of a security operation center[C]// Proceedings of the International Conference on Security and Cryptography. Setúbal, Portugal, 2006: 48-55
[3] Zhang Z, Li J, et al. A hierarchical network intrusion detection system using statistical preprocessing and neural network classification[C]// Proceeding of the 2nd Annual IEEE Systems, Mans, Cybernetics Information Assurance Workshop. NY, 2001: 85-90
[4] Ganame A K, Bourgeois J, Bidou R, et al. A global security architecture for intrusion detection on computer networks[J]. Computers & Security, 2008, 27: 30-47
[5] Engelhardt D, Anderson M. A distributed multi-agent architecture for computer security situational awareness[C]// Proceedings of the 6th International Conference of Information Fusion. Cairns, Queensland, Australia, 2003
[6] 崔玉华,李涛,周仲义. 远程监控 Agent 的体系结构及其环境安全态势评估模型[J]. 四川大学学报:工程科学版,2007,39(2):127-132
[7] 王慧强,赖积保,胡明明,等. 网络安全态势感知关键实现技术研究[J]. 武汉大学学报:信息科学版,2008,33(10):995-998