联动式入侵监视系统的体系结构设计①

Design of a Collaborative Intrusion Monitoring System Architecture

马小龙　陈 喆 （河南郑州 解放军信息工程大学电子技术学院 450004）

摘要：近期互联网出现了许多分布式协同攻击，各单位原有的入侵检测系统不能很好的检查出这些攻击行为，并且误报率较高。为了克服这些不足，本文提出了一种新的保护框架——联动式入侵监视系统。该系统实现不同管理域网络之间告警信息共享、执行集中式告警相关性分析并提供入侵预警服务而提高各个网络的安全性。

关键词：入侵检测 网络安全 环形网络

1 引言

如今，入侵检测系统已经成为网络安全基础设施的一个重要的组成部分，但在实际的配置和使用中仍然存在着一些问题：一方面，基于特征的入侵检测系统只有在及时更新特征库的前提下，才可以有效检测已知特征的网络入侵活动，但对于一些未知特征的网络入侵则无能为力。另一方面，基于异常的入侵检测系统可以有效检测一部分未知的入侵，但误报率高；再者，由于网络安全管理是独立实施的，因为入侵检测系统所产生的告警信息数据量大，大多网络系统没有充足的资源可以进行及时和正确的分析，因此及时检测入侵是很困难的。此外，对于近期互联网出现的协同式入侵这种新的入侵方式，各网络原有的入侵检测系统很难对此类攻击方式发挥有效的作用。

本文中，我们提出了一种跨网络管理域的联动式入侵监视方法，将各单位网络的独立的局部防护模式改变为各单位网络之间互相协同的全局防护模式。通过各分布式网络间构建一个对等的环形网络实现安全信息共享，由一个安全监测中心集中对分布式网络的告警信息进行相关性分析，即实现一种分布式监测和集中安全管理机制。由于安全监测中心拥有了各个子网中比较完整的入侵特征信息，所以可以更为全面的分析网络攻击和入侵活动的情况，特别是对于协同式入侵活动，此种方法能够有效的控制和检测入侵活动的实施，而且可以通过安全监测中心进行策略的平衡和共享。

2 联动式入侵监视系统的内部结构

联动式入侵监视系统是一个基于网络的、实时监测入侵与响应的分布式系统，它收集不同管理域的子网的安全告警信息，集中地处理告警信息，及时地为各子网提供有价值的、有关各个网络入侵的预警与响应服务。在这里每个单位的内部网络被定义成从属于安全监测分中心的会员子网。联动式入侵监视系统的结构如图1所示，不同于一般的分层结构的分布式入侵检测系统，联动式入侵监视系统采用了含有加权层次的图结构。

安全监测中心管理着会员子网的构成，它具有最高的权重。安全监测中心的次级是多个安全监测分中心，为了提高系统的可扩展性，这些分中心之间采用对等的环网结构，安全监测分中心与会员子网之间为一种星型结构。安全监测分中心和会员子网之间通过广播来实现告警。

为了能够达到系统的设计目标，需要解决数据采集协同和数据分析协同这两个问题。对于各单位异构的网络，联动式入侵监视系统应该将各子网中的安全信息综合汇总到分中心上。数据分析协同需要在两个层面进行，一是对一个检测引擎采集的数据进行协同分析，综合使用模式匹配和异常检测技术等，以发现较为常见的、典型的攻击行为；二是对来自多个检测引擎的审计数据，利用数据挖掘技术进行分析，以发现较为复杂的攻击行为。考核 IDS 数据分析能力可以从准

① 基金项目：国家 863 资助项目（2002AA1Z2101，2004AA1Z2020）

©《计算机系统应用》编辑部 http://www.c-s-a.org.cn

确、效率和可用性三方面进行。基于这一点，各单位子网的检测引擎应是完成第一种数据分析协同的最佳地点，安全监测分中心则是完成第二种数据分析协同的最佳地点。实验表明，上述方法既充分利用了各单位原有的检测系统，又能够极大的提高联动式入侵监视系统的检测率，而不会降低任何一种检测模型的效能。

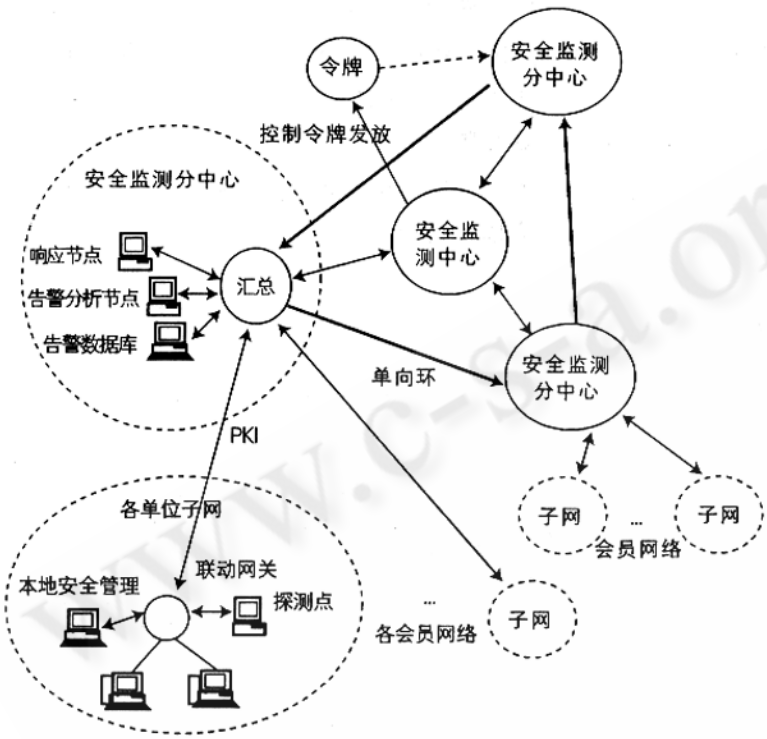

图 1　联动式入侵监视系统结构

(1) 安全监测中心。由告警汇聚数据库、告警相关性分析模块、响应模块、管理评判模块和 PKI 认证监测模块组成。告警汇聚数据库是一个综合数据库，存贮历史和当前的来自分中心的综合分析告警信息；告警相关性分析模块统计并分析历史告警信息和实时分析各分中心的告警信息；响应模块是将告警相关性分析报告安全地、迅速地发布到各分中心；管理评判模块实时判断来自各分中心上报的报告是否可靠以及目标分中心资源是否可用；PKI 认证监测模块要实现安全监测中心与分中心之间的通信双方是可信的、通信过程是安全可靠。

(2) 安全监测分中心。从属于安全监测中心，是一组会员网络的具体管理者，由告警数据库、告警相关分析模块、响应模块、联动网关和 PKI 认证模块组成。与安全监测中心类似，告警数据库存贮历史和当前的来自本地会员网络的原始告警信息和来安全监测中心的汇总告警信息，以及已知的入侵特征和安全漏洞等数据；告警相关分析模块统计分析历史告警信息和实时分析本地会员网络、全局网络的当前告警信息；响应模块是将告警相关分析模块对告警信息的分析结果安全地、迅速地发布到各会员网络；联动网关是联动式入侵监测系统的协同构件；PKI 认证模块要实现安全监测中心之间、安全监测中心与会员网络之间确保通信双方是可信的、通信过程是安全可靠。

(3) 会员子网。由一组探测点、一个可选的本地安全管理节点和至少一个联动网关组成。会员子网综合利用原有的网络安全设施，在不影响原有的网络构成的情况下，将本子网安全设备生成的信息及时地提交给所属的联动式网络监测分中心，同时对于分中心反馈的安全信息进行及时地更新和防护。在对原有设备进行微小修改的基础上，实现了防护能力的升级。

2.1 联动网关

联动网关是联动式入侵监视系统的协同构件，它实现告警预处理、数据净化、信任管理与安全信息交换等功能。联动网关实现告警归一化和过滤两个预处理功能。告警归一化是将本地网络各个探测点所产生的告警信息转换为一种统一的告警消息格式。告警过滤是对本地网络多个探测点产生的一些重复告警信息进行初步组合，以减少安全监测中心告警相关分析的开销。

各本地网络向安全监测分中心提交的告警中包含本地网络的一些机密信息，数据净化是根据本地网络设置的安全策略去除告警消息含有的本地网络的机密信息，以保护本地网络的安全性和隐私性。联动网关实现信任管理与安全信息交换功能，保证本地网络和安全监测中心之间、安全监测分中心之间通信是可认证的，保证相互之间交换的告警消息和预警消息是完整和机密的，从而保证联动式入侵监视系统的安全性。

2.2 内部交互消息

联动式入侵监视系统主要存在两类消息。一类是告警相关消息，包括由本地网络发送到安全监测分中心的单条告警消息和安全分中心之间交换的汇总告警

©《计算机系统应用》编辑部 http://www.c-s-a.org.cn

消息，另一类是响应消息，是由安全监测中心向本地网络发布的入侵报警消息和风险评估消息。

联动监视系统采用由 IETF 提出的 IDMEF 作为统一告警消息格式。IDMEF 告警消息用 XML 语言表示，其格式如图 2 所示，包括来源地址、源端口、目的地址、目的端口、协议、时间标签、探测点标识符、告警计数及等级、附加数据等。

安全监测分中心所监测的会员子网一段时间内存在的各种情况进行总结，通过 IDMEF 向安全监测中心上报。

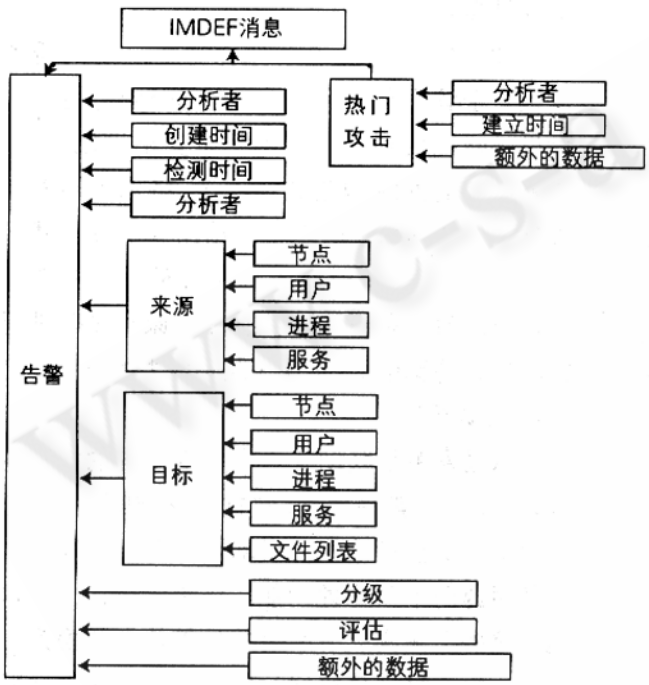

图 2　IDMEF 消息

入侵报警消息是安全监测分中心经过告警相关性分析，如果检测到会员网络被入侵，就向会员网络发布实时入侵报警，同时进行必要的网络修复。在进行了上述操作后，安全监测分中心会及时地将情况上报给安全监测中心对告警库进行更新。风险评估消息是安全监测分中心根据一段时间内存在的网络攻击与入侵活动以及会员网络安全策略而做出一个安全评估报告。它将提交给安全监测中心，以便监测中心的管理员进行系统风险分析。

3　可扩展的环形网络

为了实时监测和响应网络攻击和入侵活动，联动式入侵监测系统采用应用层多播的方法通过构造一个对等的环形网络来提高告警和预警消息交换性能。

由于安全监测分中心数目相对较少，安全监测分中心的联动网关之间构成环状互连结构，如图 3 所示。

安全监测分中心与会员子网之间采用一种星形结构，这样同时兼顾了网络的可靠性和扩展性。由于令牌环网结构能够为安全监测分中心提供一个访问时间的上限，所以安全监测中心能够明确会话令牌所在的分中心是否能够有效的提供服务。安全监测分中心通过获得会话令牌，向安全监测中心提交预警分析报告。由安全监测中心将这些分析报告进行分析并统一发放到各分中心以便进行相应的处理。

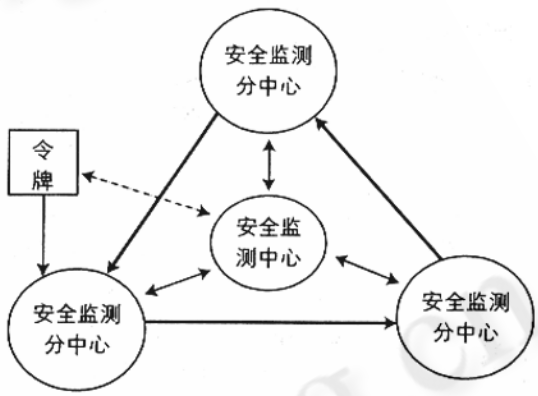

图 3　可扩展环形网络

4　告警相关分析

安全监测分中心采用告警相关分析方法，处理来自本地网络告警消息和安全监测中心的汇总告警消息，一方面要将低级告警消息组合为高级入侵过程，降低入侵检测的误警率和漏报率，识别入侵企图，另一方面要获取本地和全局网络的入侵和攻击活动情况及其发展趋势。

告警相关分析是一个复杂的告警消息处理过程，将由一系列处理子过程组成，各个具体的处理子过程包括告警汇聚、攻击验证、攻击会话重构、攻击焦点识别、多阶段攻击相关、风险评估及告警严重性，其中，告警汇聚、攻击验证、攻击会话重构适用于所有告警类型，攻击焦点识别、多阶段攻击相关主要适用于多目标攻击分析。安全监测分中心的告警相关分析的过程和方法如下：

©《计算机系统应用》编辑部 http://www.c-s-a.org.cn

(1) 告警汇聚。识别告警消息是否属于同一个网络攻击活动,将属于同一个网络攻击的告警消息组合在一起,采用时序近似性和属性近似性来处理。时序近似性:两个告警的开始时间、结束时间的差异小于某一个时间门限。属性近似性:告警类型、地址、端口和负载等属性的相似性。

(2) 告警验证。验证告警消息是否属于误报,若是不成功入侵,标识为误警,采用主动扫描的方式来处理。

(3) 攻击会话重构。将一系列相关的基于主机或网络的告警消息合并,构成一个完整的入侵场景。通过综合告警汇聚的有关信息并分析攻击的起因和造成的影响来重构攻击的实施。

(4) 攻击焦点识别。识别一个结点为一个攻击源或者为一系列攻击的目标。通过设置一个门限值来识别目标结点是否遭到攻击或作为攻击的源头对其它系统实施攻击。

(5) 多阶段攻击相关。识别由多个相对独立的入侵过程组成的一种高级入侵模式。使用状态图表示入侵场景,使用基于概率推导方法将孤立告警消息组成的一种攻击树,显示入侵过程。

(6) 风险评估及告警严重性。对本地会员网络的安全风险评估和确定各种攻击活动的严重性。将结合前面的相关处理子过程的输出结果与告警特征库存贮的漏洞、本地会员子网服务信息、安全策略等对相关会员网络安全性进行评估,汇总攻击源列表、汇总攻击目标列表,汇总严重入侵活动列表模式等。

5 系统安全性

一个完整的计算机安全产品应该同时具有安全功能和安全保障两部分内容。在有效的构件了联动式入侵监视系统的实现基础上,系统自身安全性如何解决显得尤为重要。

作为整套设施的关键,它主要存在两种风险:一种是发布的预警消息在传输过程被更改、被丢弃或被假冒;另一种是联动式入侵监视系统本身被分布式拒绝服务等攻击。对于以上出现的问题将采用一下方法来解决。

对于第一个问题,主要采用公钥密码技术,它一方面保证参与联动式入侵监视系统的网络或结点是可信的和机密的,另一方面网络内部所传输消息采用数字签名机制,这样能够从全局保证信息的安全。

对于第二个问题,联动式入侵监视系统采用一种动态监测服务选择协议,允许会员子网在发现一个安全监测分中心不能提供有效地监测服务时,查询目录服务器动态地选择其它安全监测分中心,安全分中心之间可以重构环形网络。另外可以采用蜜罐技术将攻击者从关键系统引诱开,怂恿攻击者在蜜罐系统上停留足够长的时间以供管理员对分布式拒绝服务攻击进行有效的响应。

6 结论及进一步工作

通过分析现有入侵检测系统存在的问题,提出并设计了一个联动式入侵监视系统的框架和系统结构。联动式入侵监测系统由一个以可扩展环形网络为基础互连的安全监测分中心和一些分别与安全监测分中心构成星形互连结构的会员网络组成,实现分布式告警消息收集与共享、集中式处理,目标是使会员网络更安全。我们正在着手实现联动式入侵监测系统,接下来将对系统进行全面的验证以评判该系统带来的安全性能的提高和系统性能的改进。

参考文献

1 P. A. Porras and P. G. Neumann. EMERALD: Event monitoring enabling response to anomalous live disturbances. In Proceedings of the 20th National Information Systems Security Conference, National Institute of Standards and Technology, 1997.

2 F. Cuppens and A. Miége. Alert Correlation in a Cooperative Intrusion Detection Framework. Proceedings of the 2002 IEEE Symposium on Security and Privacy. 2002. Pages 187 – 200.

3 P. Ning. Y. Cui and D. S. Reeves. Constructing Attack Scenarios through Correlation of ntrusion Alerts. Proceedings of the 9th ACM conference on Computer and communications security. ACM Press, 2002. Pages 245 – 254.

©《计算机系统应用》编辑部 http://www.c-s-a.org.cn