基于协同的安全事件确认

邢苏霄，龚俭

(东南大学 计算机科学与工程学院，南京 210096)

摘要：为减少 IDS 检测手段相对单一、误报率过高带来的影响，本文提出一种基于协同的安全事件确认方法及其模型实现，它能充分利用入侵检测协同框架的综合检测优势，将时/空间关联分析方法及其他安全事件信息有效地融合起来，对安全事件进行多层次确认处理，将安全事件区分为有效事件、无效事件和待定事件三类，以便系统管理员进行有针对性的事件响应。通过在 CERNET 主干网的初步实践表明，对安全事件进行分类标记，可以有效地减少误报、提高 IDS 检测结果的处理效率。

关键词：入侵响应；安全事件确认；协同；网络安全；入侵检测

中图分类号：TP393.08　　**文献标识码**：A　　**文章编号**：1000-436X(2006)11A-0092-06

Security event verification based on cooperation

XING Su-xiao, GONG Jian

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

Abstract：In order to reduce the impact caused by the comparatively single IDS detection method and the excessive amount of false positives, a method and model of security event verification based on cooperation was explored. It can verify security events through multi levels, taking full advantage of the comprehensive detection method based on intrusion detection cooperation framework and combining the time/space correlation analysis with assistant security event information. By classifying the security events into valid events, invalid events and pendent events, system manager can do incident response pertinently. With the primary practice on the CERNET backbone, this method can effectively reduce the amount of false positives, and advance the processing efficiency of IDS detection result.

Keywords：incident response; security event verification; cooperation; network security; intrusion detection

0 引言

近年来，入侵检测系统（IDS）作为一种帮助用户及时了解网络安全信息的实际解决方法，已成为网络安全防护领域内不可缺少的安全防护技术。但由于其检测手段相对单一，功能和系统基本上都是孤立的，所以 IDS 误报率过高、检测精度亟待提高。而入侵检测协同框架的提出为综合利用入侵检测优势带来了希望。由美国加州大学 Davis 分校安全实验室研究的 CIDF（Common Intrusion Detection Framework，通用入侵检测框架）[1]主要讨论入侵检测系统协同的问题，安全事件确认正是 CIDF 定义的协同功能之一，它通过将安全事件信息与其他相关信息综合分析，从而验证 IDS 产生的安全事件的正确性。

为了给本地或异地后续安全分析和处理提供数据支持，以便及时响应病毒入侵、黑客攻击等安全事件，根据十五“211 工程”公共服务体系建设项目“CERNET 高速地区网和重点学科信息服务体系建设”中专题 “CERNET 主干网运行安全基本保障系统”的需求， CERNET 主干网与各省接入网的接口处（共 38 个节点）已部署了 IDS 服务器和安全协查系统，初步实现了各省网的安全事件协同（如图 1 所示）。该协同平台中各节点的安全事件记录参照 IDMEF 格式封装为 XML 文本，使用基于 SSL 的连接进行交互。本文在此协同平台基础上提出一种安全事件确认方法，以达到鉴别 IDS 误报、提高入侵检测结果处理效率的研究目的。

收稿日期：2006-10-09

基金项目：教育部“十五”211 工程公共服务体系建设资助项目

Foundation Items: 211 Infrastructure Construction Project of MOE for the 10th Five-year Program

本文首先对研究现状进行阐述，然后介绍了基于协同的安全事件确认方法的处理流程及模型的简单实现，并利用实例进行具体分析，最后是总结与展望。

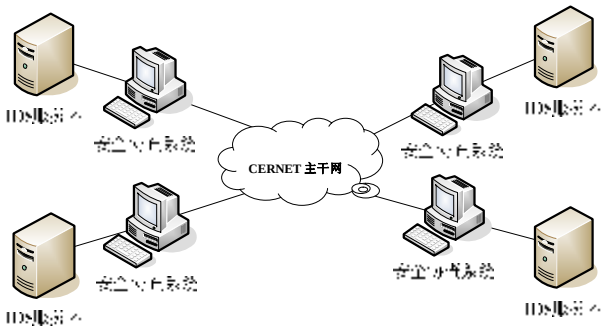

图 1 CERNET 主干网协同平台

1 研究现状

入侵检测系统（IDS）通常会报告大量安全事件，使安全管理员淹没在事件洪流中不知所措，严重影响了后期的入侵响应，这已是科学界和工业界的广泛共识[2]。许多学者都致力于降低安全事件误报率的研究，已经采用的分析方法有聚类[3]、关联[4]、时序分析[5]等等，它们也能大幅降低安全事件数量，但有效性验证是一个公认的难题。另外，由于对安全事件的检测通常包含了大量复杂的步骤，许多相对孤立的入侵检测系统[6]很难提供完备的检测能力，因此，需要协同多个检测系统以达到完整的检测效果，如引言中提到的 CIDF 以及 IDWG 建立的 IDEF[6]等，都已初步解决了协同时数据交换格式和交互协议的问题，但要真正实现分布广泛的协同系统，并在此基础上对安全事件进行确认，却有相当的难度。报警验证[7, 8]类似于本文的安全事件确认，目前已逐渐成为入侵检测后处理（对入侵检测结果进行分析、响应等）的研究热点之一，但通常其研究焦点主要集中在主机信息上面，如主机漏洞、操作系统、应用服务系统信息等等，并没有充分利用聚类、关联等各种较为成熟的分析技术来对安全事件加以确认。

如引言所述，CERNET 教育网已基本实现了各省网综合数据交互的协同平台，因此它为本文安全事件确认方法的提出和论证提供了必要的前提条件和实验环境。本文提出的安全事件确认方法将协同与时/空间关联分析方法有效地融合起来，对安全事件进行多层次确认处理，以达到分类标记安全事件的结果。方法的形式比较新颖，综合信息较为全面。

2 安全事件确认方法

在协同环境下，有三种信息对于安全事件确认来说非常重要。首先是其他协同点的安全事件信息，它的主要作用是核实本地 IDS 检测所得安全事件的正确性。其次是攻击场景信息，主要说明安全事件产生的前因后果。如果说这两种信息都是从安全事件本身出发的话，那么最后一种则是通过从其他信息寻找佐证来验证安全事件的正确性，即辅助信息。

针对这三种重要信息，本文提出的安全事件确认方法主要通过协同匹配、协同关联和协同辅助信息验证三个层次来对安全事件进行确认处理。原始安全事件经过确认处理之后，将被分别标记为有效事件、无效事件和待判事件，下面首先说明相关定义。

定义 1：无效事件是指对入侵检测后处理影响不大的事件。

故无效事件可以作为无兴趣的部分而被忽略，然而忽略这些事件并不意味着要将它们删除，因为在入侵检测后处理进行进一步数据分析时，它们可能是有用的。无效事件可以是被误认为某种攻击的正常事件，可以是被误认为另一种攻击的安全事件，也可以是实施了攻击却没有达到目标的安全事件。

定义 2：有效事件是指对入侵检测后处理能够产生重要影响的安全事件。

入侵检测后处理将主要围绕它来进行。方法的最高目标是使有效事件范围正好覆盖 IDS 正确报告的安全事件范围，但现实中许多不确定因素的存在，使得方法只能逐渐逼近这个最高目标。

定义 3：待判事件指根据现有方法还无法判断其对入侵检测后处理影响程度的安全事件。

定义 4：原始安全事件的标准格式 security event := <eventType, securityLevel, srcIP, dstIP, startTime, endTime, srcPort, dstPort, eventTypeNo, attackCount, analyzerID, srcIPCount, srcPortCount, dstIPCount, dstPortCount, protocol, offset, postAttack, attachType>

标准格式为 19 元组，属性包括安全事件类型、严重程度、源 IP 地址、宿 IP 地址、起始时间、终止时间、源端口号、宿端口号、事件类型号、攻击数、分析 ID、源 IP 数、源端口数、宿 IP 数、宿端口数、协议、偏移量、后攻击、攻击附件，均由 IDS 检测得知。

安全事件确认方法中还引入了安全事件确认度 V 的概念，用来指示安全事件被方法确认的程度。三层确认处理可分别计算得到安全事件确认度的三个因子：协同匹配因子 M、协同关联因子 R 和协同辅助验证因子 F，它们将决定最终的安全事件确认度。最后通过安全事件确认度 V 同标记阈值 x 的比较来对安全事件进行标记。安全事件确认方法流程如图 2 所示。

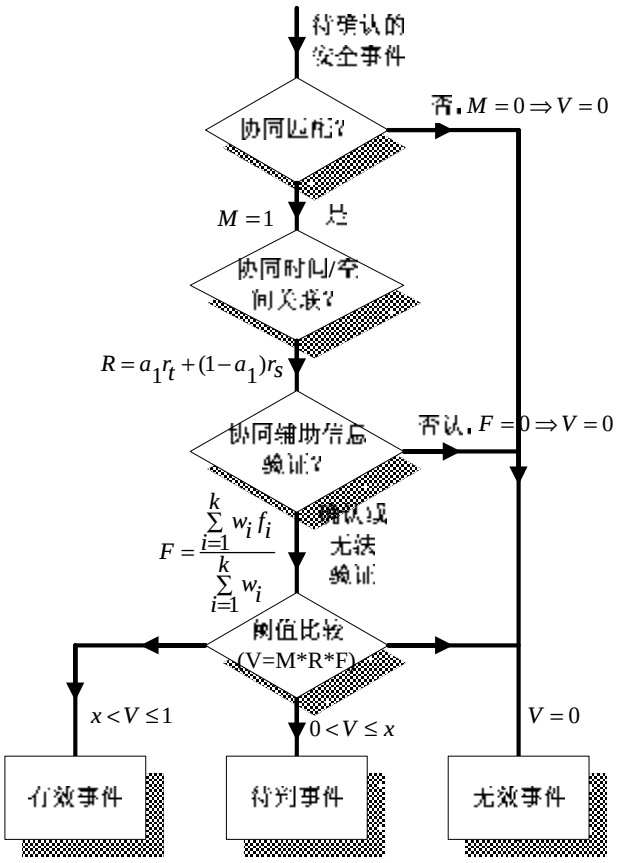

图 2　安全事件确认方法流程

2.1 协同匹配

利用其他协同点安全事件信息匹配的方法可以处理源 IP 地址伪造的情况。IP 地址伪造，即通过伪造某个 IP 地址的数据包来让某台计算机鉴别另一台计算机的复杂攻击技术。如果机器受到从外网进行的攻击，那么仅仅依靠相对孤立的 IDS 提供安全事件报告是无法确认真实攻击源的。

定义协同匹配因子 $M=\begin{cases}1, & \text{成功匹配}\\ 0, & \text{无法匹配}\end{cases}$。设 e_1 为待确认安全事件，若通过协同在源 IP 地址所处网域中找到了相应安全事件 e_2，则认为该安全事件协同匹配成功，这意味着在攻击源网域找到了该事件的攻击迹象，核实了该安全事件，但至于其是否为有效事件，还需要进一步确认处理；如果安全事件源 IP 地址所处网域没有找到相应安全事件，则认为无法匹配。

成功的协同匹配主要依据以下逻辑规则进行协同：

$$\begin{aligned}\forall e_1, M(e_1)=1 \Leftarrow \exists e_2, &(e_2.eventType=e_1.eventType)\wedge\\ &(e_2.srcIP=e_1.srcIP)\wedge(e_2.dstIP=\\ &e_1.dstIP)\wedge(e_2.srcPort=e_1.srcPort)\wedge\\ &(e_2.dstPort=e_1.dstPort)\wedge\\ &(e_2.startTime\approx e_1.startTime)\wedge\\ &(e_2.endTime\approx e_1.endTime)\end{aligned}$$

即对六个安全事件属性值：事件类型、源 IP 地址、宿 IP 地址、源端口、宿端口、起始时间和结束时间，进行约束协同。

2.2 协同关联

协同关联主要涉及时间关联和空间关联两个方面。

时间关联可依据各安全事件发生的先后顺序进行分析。设 IDS 检测到一次攻击 a，那么它会按照时间顺序向安全管理员报告构成这次攻击的各个安全事件{$e_1, e_2, e_3, \ldots$}，各事件的时间属性相应为{$t_1, t_2, t_3, \ldots$}，一定满足 $t_i<t_j$（其中 i<j）。另外，相邻事件的源/宿 IP 地址问题也需要注意，因为许多攻击需要攻击发起方和受攻击方进行信息交互才能正式成形，比较典型的是特洛伊木马。攻击发起方首先向受攻击方植入木马，然后木马利用受攻击方的某些漏洞与发起方进行交互，以实现攻击的目的。这种交互可能持续多次，交互内容和次数主要由攻击类型来决定。

空间关联则主要依据各类型安全事件的攻击方式来进行验证，由源/宿决定的攻击方式主要有一对一（如基于 ICMP 的 Large Ping 攻击）、一对多（如 Address Sweep 攻击）和多对一（如 Ping Flood 攻击）攻击。

定义协同关联因子 $R=a_1r_t+(1-a_1)r_s$，$0<a_1<1$，时间关联因素 r_t（$0<r_t<1$）和空间关联因素 r_s（$0<r_s<1$）共同对安全事件的协同关联因子产生影响。具体的协同逻辑规则将依据相关攻击场景信息，主要涉及的安全事件属性包括安全事

件类型 eventType，源 IP 地址 srcIP，宿 IP 地址 dstIP，起始时间 startTime，以及终止时间 endTime。

2.3 协同辅助信息验证

最后通过协同辅助信息对安全事件进行验证，辅助信息包括 netflow 异常流量检测、攻击发起方或受攻击方的主机性质分析、主机脆弱性分析、主机日志管理等等。协同逻辑规则将主要依据辅助信息进行具体协同验证。

辅助信息验证的可能结果有三：一是辅助信息完全否认了安全事件发生的可能性，例如某安全事件是针对 http 服务而目标主机并未开放 80 端口；二是辅助信息为安全事件的发生提供了相关证据；三是辅助信息不能说明任何问题，既无法否认也无法确认安全事件。

设共有k种辅助信息，定义相应的子辅助验证因素f_i，$1 \leqslant i \leqslant k$。根据实际情况，可为每种辅助信息分配相应的权值$w_i$，$1 \leqslant i \leqslant k$。根据上述辅助信息验证的三种可能结果，$f_i$也有三种取值。

$$f_i = \begin{cases} 1, & \text{给予确认} \\ 0, & \text{给予否认} \\ a_2 (0 < a_2 < 1), & \text{无法验证} \end{cases}$$

定义辅助验证因子

$$F = \begin{cases} \dfrac{\sum_{i=1}^{k} w_i f_i}{\sum_{i=1}^{k} w_i}, & \min\{f_1, f_2, ..., f_k\} \neq 0 \\ 0, & \min\{f_1, f_2, ..., f_k\} = 0 \end{cases}$$

2.4 阈值比较

设安全事件确认度为 V，它由协同匹配因子、协同关联因子和协同辅助信息验证因子共同决定，$V = M * R * F$。安全事件被确认为无效事件、有效事件或待判事件将通过 V 值与标记阈值 x 进行比较来判断，如表 1 所示（表中$0 < x < 1$）。这样就可以为每个安全事件打上标记：有效事件、待判事件或无效事件。

阈值范围	确认结果
$V = 0$	无效事件
$0 < V \leq x$	待判事件
$x < V \leq 1$	有效事件

表 1　确认处理结果

通过对历史事件标记结果进行统计分析，可计算出安全事件可信度从而调整标记阈值 x，以便对后续安全事件进行确认处理，提高安全事件确认的精度。当某一类型安全事件的可信度上升时，其标记阈值 x 将下降；可信度下降，则标记阈值 x 相应上升。

3 安全事件确认模型

在提出基于协同的安全事件确认方法的基础上，本文建立了安全事件确认的简单实现模型，模型框架如图 3 所示。

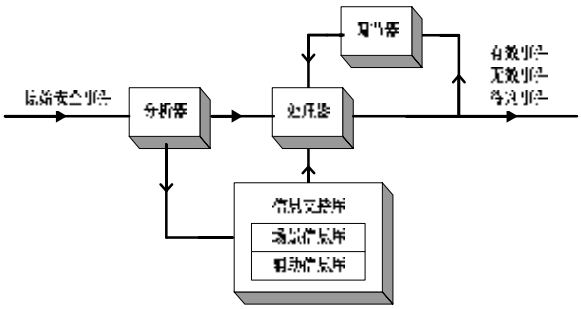

图 3　基于协同的安全事件确认模型框架

分析器的主要功能是对原始安全事件进行分析，将原始安全事件与相应的攻击场景信息联系起来，进行描述并形成相应的信息支持库，为安全事件在处理器中的确认处理做好充分准备。由于模型是基于已经实现的 IDS 系统和安全协查系统，所以原始安全事件来源于 IDS 报告给安全管理员的原始数据，且已经由安全协查系统转换成为安全事件的标准格式。

处理器是整个模型的核心。在协同平台的基础上，它充分结合其他协同点的安全事件信息、攻击场景信息和相关辅助信息，对安全事件进行确认处理，以达到为安全事件标记的目的。

调节器是安全事件类型的标记阈值调节器。通过对处理器得出的历史事件标记结果进行统计分析，根据可信度来调节安全事件类型的标记阈值，并反馈给处理器，从而对后续待确认安全事件的标记结果产生影响。

这里引入了反馈机制，因为反馈是控制理论中一种能够有效、动态修正系统的经典方法，它的引入将会有效克服模型中参数设置的合理性问题。

4 实例分析

CERNET 协同平台经过较长时间的运行，已经

积累了不少数据。下面就以 2006 年 7 月 1 日 23 时 22 分 07 秒在节点 A 发现的 DDOSmstr5 安全事件为例来说明基于协同的安全事件方法的确认流程，并进行简单分析。

首先给出基于协同的安全事件确认方法中的已知变量值：$a_1 = 0.5$，$a_2 = 0.5$，DDOSmstr5 安全事件标记阈值 $x = 0.3$（由历史数据统计分析得出的经验值）。

根据安全协查系统提供的安全事件描述，DDOSmstr5 是一个利用分布式拒绝服务攻击工具 mstream、从 client 发往 handler 的事件记录。由源/宿 IP 地址知，client 是源 IP 地址 IP_1（属于节点 B），而 handler 正是宿 IP 地址 IP_2（属于节点 A）。更明确地说，即节点 A 的某机器（handler）试图通过工具 mstream 控制节点 B 的某机器（client）进行 DDOS 攻击，这条记录是 client $\rightarrow$ handler 通信时被捕获的。

设该安全事件为 e_1，为进行协同匹配，设置具体的协同匹配逻辑规则如下：

$$(eventType = \text{DDOSmstr5}) \wedge (srcIP = IP_1) \wedge (dstIP = IP_2) \wedge (srcPort = 10134) \wedge (dstPort = 12754) \wedge (startTime \approx 20060701 \quad 23:22:07) \wedge (endTime \approx 20060701 \quad 23:22:07)$$

结果发现节点 B 处检测所得的安全事件 e_2 能完全匹配上，故协同匹配因子 M=1，协同匹配成功。

在协同时间关联方面，根据 DDOSmstr5 的安全事件描述知，若该事件为真实攻击，则 handler 必须首先与 client 进行通信。即 IDS 系统应至少报告两个安全事件来反映此 DDOS 攻击：$\{e_0, e_1\}$，时间属性相应为$\{t_0, t_1\}$，且满足 $t_0<t_1$。而协同空间关联方面，也会形成一对多的源/宿控制方式。

设置协同时间关联逻辑规则如下：

$$(srcIP = IP_2) \wedge (dstIP = IP_1) \wedge (srcPort = 12754) \wedge (dstPort = 10134) \wedge (startTime < 20060701 \quad 23:22:07) \wedge (endTime < 20060701 \quad 23:22:07)$$

设置协同空间关联逻辑规则如下：

$$(srcIP = IP_1) \wedge (srcPort = 12754) \wedge (startTime \approx 20060701 \quad 23:22:07) \wedge (endTime \approx 20060701 \quad 23:22:07)$$

结果发现 DDOSmstr5 事件（即 e_1 事件）之前的确存在 DDOSmstr6 事件（即 e_0 事件），两事件均由工具 mstream 产生，且 DDOSmstr6 事件是在 handler $\rightarrow$ client 通信时被捕获的。此外，发现节点 A 处的 handler 还企图控制很多其他节点的机器，有形成僵尸网络的迹象，但规模并不大。由此计算得协同时间关联因素 r_t=0.9，空间关联因素 r_s=0.9，可得协同关联因子 $R = a_1 r_t + (1-a_1) r_s$ =0.9。

最后是协同辅助信息验证。由于缺乏当时的相关辅助信息，故协同辅助信息无法进行验证，即 $f_i = a_2 (1 \le i \le k)$。故协同辅助验证因子

$$F = \frac{\sum_{i=1}^{k} w_i f_i}{\sum_{i=1}^{k} w_i} = \frac{\sum_{i=1}^{k} w_i a_2}{\sum_{i=1}^{k} w_i} = a_2 = 0.5。$$

根据三个协同因子，可计算得该安全事件 e_1 的确认度 $V = M * R * F$ = 1*0.9*0.5 = 0.45。由于 $x < 0.45 \le 1$，所以该安全事件被标记为有效事件。

同理，无效事件或待判事件的确认流程与此类似。当然标记阈值会根据历史事件标记结果的统计分析自动调节，经过时间的积累，会逐渐达到稳定。

根据在 CERNET 主干网的初步实践表明，通过将安全事件进行如上的分类标记，可以在一定程度上减少误报、提高 IDS 检测结果的处理效率，使系统管理员能够针对值得关注的有效事件进行事件响应。在特殊需求下，也可对待判事件或无效事件进一步分析、处理。

5 结束语

本文提出的基于协同的安全事件确认方法及其模型实现，在入侵检测协同框架综合检测的基础上，结合协同匹配、协同关联（时/空间关联）及协同辅助信息验证等方法，对安全事件进行多层次确认处理，并为安全事件分类标记。该方法的形式比较新颖，信息综合性强，且有 CERNET 协同平台上的初步实践作为研究基础。若通过实验对安全事件确认方法中的参数设置进一步研究，则方法会更加合理化，事件确认的效果会更好。

参考文献：

[1] KAHN C, PORRAS P A., STANIFORD-CHEN S, *et al*. A Common intrusion detection framework[EB/OL]. Submitted to the Journal of

Computer Security. 2000. http://gost.isi.edu/cidf/.

[2] AXELSSON S. The base-rate fallacy and the difficulty of intrusion detection [A]. ACM Transactions on Information and System Security (TISSEC) [C]. New York, NY, USA: ACM Press, 2000: 186-205.

[3] JULISCH K. Clustering intrusion detection alarms to support root cause analysis[A]. ACM Transactions on Information and System Security (TISSEC)[C]. New York, NY, USA: ACM Press, 2003: 443-471.

[4] NING P, CUI Y, REEVES D S, *et al*. Techniques and tools for analyzing intrusion alerts[A]. ACM Transactions on Information and System Security (TISSEC)[C]. New York, NY, USA: ACM Press, 2004: 274-318.

[5] VIINIKKA J, DEBAR H, ME L, *et al*. Time series modeling for IDS alert management[A]. Proceedings of the 2006 ACM Symposium on Information, computer and communications security[C]. New York, NY, USA: ACM Press, 2006: 102-113.

[6] 龚俭，陆晟，王倩等. 计算机网络安全导论[M]. 南京：东南大学出版社，2000：247-255.

GONG J, LU S, WANG Q, *et al*. Introduction to the security of computer network[M]. Nanjing: Southeast University Press. 2000: 247-255.

[7] KRUEGEL C, ROBERTSON W. Alert Verification: Determining the success of intrusion attempts[A]. Proc. First Workshop the Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA)[C]. Germany: GI, 2004: 25-38.

[8] 穆成坡,黄厚宽,田盛丰. 基于多层模糊综合评判的入侵检测系统报警验证[J]. 计算机应用, 2006, Vol.26 No.3: 553-557.

MU C P, HUANG H K, TIAN S F. Intrusion detection alert verification based on multi-level fuzzy comprehensive evaluation[J]. Computer Applications, 2006, Vol.26 No.3: 553-557.

作者简介：

邢苏霄（1984-），女，江苏高淳人，硕博连读生，主要研究方向为网络安全。

龚俭（1957-），男，吉林长春人，东南大学教授、博士生导师，主要研究方向为网络安全、网络管理、网络体系结构。