一个面向网络入侵检测的实时协同系统[1]

汤鲲 龚俭

（东南大学 计算机系，210096 南京）

【摘要】本文结合当前国内外相关领域的研究成果，给出了一种面向网络入侵检测系统的实时协同模型。包括协同框架、协同方式、协同规则及协同过程等方面的设计和实现思路。该模型可提高网络入侵检测系统的检测精度和检测能力，并能为后继的响应提供决策依据。

【关键词】计算机网络；入侵检测；实时协同

中图分类号：TP393

A NIDS-Oriented Real-time Cooperation System

Tang Kun， Gong Jian

(Southeast University, Computer Science Dept., 210096 NanJing, P.R.China)

【Abstract】The paper provides a NIDS-oriented real-time cooperation model by combing currently relevant research work of abroad and home. It includes the design and implementation of cooperative framework, method, rule and process. This model can improve detective accuracy and detective ability of NIDS, and provide decision-making warranty for succeeding response.

【Key words】Computer Network；Intrusion Detection (ID)；real-time cooperation。

1. 引言

当前，网络间相互依赖性日益增强的趋势加重了网络的安全问题。一个被攻破的网络不仅会影响其自身，还可能成为攻击其它系统的跳板,同时网络的被入侵对象也从仅涉及单一结点发展到跨距处于不同管理域中的多个结点，这种情况只能由基于网络的入侵检测系统来处理。同基于主机的入侵检测系统一样，基于网络的入侵检测系统的功能也是检测安全事件并对事件进行描述和响应，但因网络的复杂性、攻击范围的随意性以及攻击手段的多样性使得后者在从入侵检测、安全事件描述以及基于描述的响应等各个方面要较前者复杂得多。为了提高安全事件的检测与决策精度，需要在网络入侵检测系统中引入分布协同机制，从全局范围来描述和验证所检测到的安全事件并为后继的响应提供更充分的决策依据。对安全事件进行协同有两种方式：实时协同和事后协同。前者通过实时的决策和响应可以将正在发生的安全事件对系统可能造成的损失降到最小；而后者则可以为管理人员对安全事件对系统造成的损失进行评估提供依据。本文将介绍一种实时协同模型的设计和实现，重点讨论协同体系结构和实时协同的系统设计问题，同时也给出实现中的一些细节考虑。

协同需要信息交换，而信息交换可能发生在连接不同的管理域的协同点间或同一管理域内的协同点间。这些管理域可能有不同的甚至是冲突的安全策略，对于同样的协同信息往往会使用不相同响应机制。对协同点角色和关系的定义就构成协同框架。目前在协同体系结构方面比较著名的研究成果有由加州大学 Davis 分校安全实验室提出的 CIDF（Common Intrusion Detection Framework）和由 IETF 安全领域的 IDWG（Intrusion Detection Work Group）负责建立的 IDEF（Intrusion Detection Exchange Format）标准。但两者都未形成完整的协同体系结构概念。根据网络入侵检测系统的协同需要和 CIDF 与 IDWG 工作的不足，作者结合 863 课题的研究内容，对网络入侵检测系统的协同体系结构进行了扩展与完善。为了表述方便，本文将协同决策前的结点称为“监测点”，将参与协同的结点称为“协同点”(一个监测点发起协同或接受到协同信息即成为协同点)。协同方式主要是根据 CIDF 的研究成果，CIDF 把入侵检测系统组件的协同方式分为：分析；互补；互纠；核实；调整检测和响应这些场景。协同规则是决定协同与否及协同的方式和范围的机制。协同过程则是指协同发起者和参与协同的其它协同点之间相互交换信息的过程。

---

[1]作者简介： 汤鲲，硕士研究生，主要研究方向为网络安全。 龚俭，工学博士，东南大学计算机系教授、博导，主要研究方向包括网络管理、网络安全、网络体系结构、开放分布式处理等。

定稿日期：2001-05-19，本文研究内容受国家 863 计划重大课题 863－317－01－03－99 支持

2.实时协同的系统设计

如上所述，实时协同是为了从全局范围内来精确描述所发生的安全事件并为后继的响应提供决策依据（如图 1 所示）：

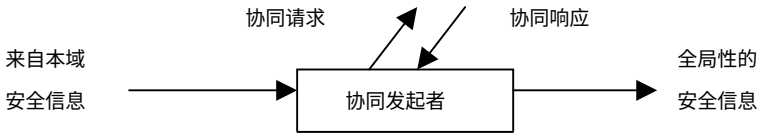

图 1　协同交互过程

在本基于网络的入侵检测系统中，每个监测点均为具有自治能力的 IDS 组件，这样的实现一方面考虑到 IDS 的扩展性，另一方面可使整个系统具有很强的防御能力（个别监测点的失效不会影响整个系统）。但这样的实现给协同带来了问题：由于安全事件仅触发检测到它的监测点，从而导致对该事件的协同只能从局部出发，因此各监测点必须了解 IDS 所监测网络的全局拓扑以及自身的位置。这又进一步要求有良好的协同决策机制的支持，协同决策还决定后继协同动作的具体实施。协同过程其实是协同信息的交互过程，为保证协同的正确性和可靠性，协同信息的传输要加以安全控制，这主要体现在两个方面：协同信息的安全传输和协同点间的相互鉴别。要想为后继的响应提供决策依据，在协同结束后需进行协同结论的生成。从这些方面出发，本文的实时协同系统结构如下：

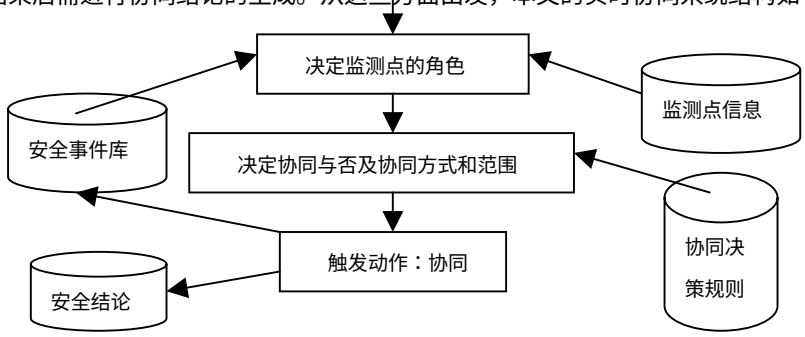

图 2　实时协同的系统结构

据此结构，整个协同过程分为四个步骤：协同定位、协同决策、协同的信息交换和协同的结论产生。

3.实时协同的实现

3.1 协同定位

实时协同要做的第一件工作是决定被安全事件触发的监测点在安全事件路径中的位置，以便进一步确定是否需要协同。可能被触发的监测点有四种类型，分别为：连接攻击源的监测点；连接攻击宿的监测点；连接敏感域（需重点保护的管理域）的监测点；其它中间监测点。监测点的定位与网络的拓扑分不开。从协同的角度出发，网络的拓扑可简化为两部分：监测点和监测域，监测点和监测域相互连接。基于此实际运用的定位方法是：首先，取得对应于该监测点的被监测域；然后，查看攻击源或宿 IP 地址是否隶属于上一步取得的监测域；最后，查看第一步取得的监测域是否敏感域。

3.2 协同决策

协同决策决定安全事件是否需要协同及协同的方式和范围。由于被安全事件触发的监测点有多种类型，因此协同决策算法要对各种情况进行分析，协同决策算法如下：

CASE 1 ：一边连接攻击源一边连接攻击宿的监测点。处理动作：无需对该类安全事件进行协同。理由：这类安全事件仅需在一个监测点进行检查即可；

CASE 2 ：连接攻击源的监测点。处理动作：该监测点无需作为协同动作发起者。理由：事件的攻击源一般不可靠；

CASE 3 ：第四类监测点。处理动作：该监测点无需作为协同动作的发起者。理由：为了避免过多的监测点成为协同动作的发起者及由此带来过多的网络流量；

CASE 4 ：连接敏感域的监测点。处理动作：涉及到敏感域的任何安全事件都需进行协同，协同的范围由事件的严重程度决定。理由：敏感域作为需加以重点保护的监测域，任何与之有关的安全事件都可能意味着安全域其中的系统被攻破或有安全隐患；

CASE 5 ：连接攻击宿的其它监测点（除连接攻击宿所在敏感域的监测点）。由于这类监测点的复杂性，所用的处理动作是前述的“ 协同规则 ”，而协同规则的定义离不开对安全事件的分析。在对安全事件的描述中，攻击类型、严重程度、可信程度是决定安全事件是否需要协同的主要因素。同时协同规则还应包含对协同方式和范围的说明：攻击类型(Event Name)、严重程度（Severity)、可信程度（Confidence)、协同范围（Cooperation Scope)、协同方式（Cooperation Type)。

协同规则的定义可能存在矛盾，处理方法是：当任何一个协同规则被匹配后就不再尝试新的协同规则，越前的协同规则具有越高的优先权。协同规则中还必须有对协同时间的限制，原因是在协同时可能存在协同信息丢失或延时过长，这会导致调用协同处理的节点处理能力下降而影响整个 IDS 的性能。

3.3 协同的信息交换

这里“ 协同客户 ”指协同的发起方，对协同信息做出响应的一方称为“ 协同服务器 ”。协同需要信息交换，从客户端到服务器端的是协同请求信息，包括：协同请求标识、被查询的安全事件描述；从服务器端返回的是协同响应信息，包括：协同请求标识、被查询安全事件是否存在、本地观察到的安全事件、以及查询安全事件描述之间的偏差或本地对该安全事件的描述。从统一接口和安全考虑，协同点间的信息交换涉及：协同信息的数据格式定义、协同信息的安全传输以及协同点间的相互鉴别。这部分的实现主要参照 IDWG 的工作：协同决策后，协同客户先将 IDMEF 表示的协同请求信息用 XML 编码封装，然后交给底层的 IAP 和 TLS（这两层分别用于协同信息的安全传输和协同点间的鉴别），最终通过物理传输协同请求信息到达协同服务器。协同服务器则首先通过 TLS 和 IAP 对请求信息进行验证，确定其请求者拥有被信任的证书，然后调用 XML 解码程序获取协同请求信息。图 3 给出了流程示意图：

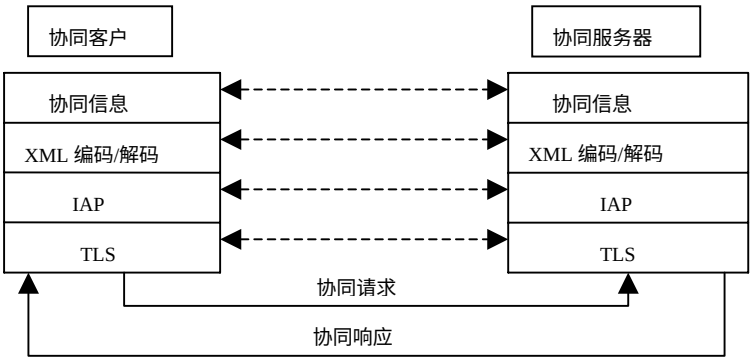

图 3 协 同 过 程 框 架

3.4 协同的结论产生

协同结束后，协同动作的发起者对其他协同点返回的结果进行综合分析，从中得出安全结论。分析的结果可能包括：

- 安全事件可靠性的证明：根据协同参与点返回的信息是“ YES ”或“ NO ”来判断；
- 安全事件的攻击路径信息：对攻击路径的表述由四部分组成：事件源（真正的源或最后“ 看到 ”事件的监测点)、事件宿、中间监测点和监测域，为此需将协同参与点的返回信息同网络的拓扑结合起来才可描述安全事件的攻击路径；
- 可能被攻破的主机或系统：最后追溯到的事件源属于 IDS 某一监测域内，且类型是诸如“ Backdoor ”、“ DoS（Denial of Service）”之类的安全事件，这就意味着事件源所在的主机或系统可能已被攻破。

4.结论

入侵检测系统的使用在一定程度上为维护系统及网络的安全提供了保障，但它还有很多有待完善的方面，尤其是有关协同问题的解决仍处于探索阶段。本文的研究工作是这方面的一个尝试，还有许多方面值得进一步改进，如对协同决策算法的优化等。进一步的探索和研究工作仍在进行中。

5.参考文献（略）