第45卷增刊
2005年10月

大连理工大学学报
Journal of Dalian University of Technology

Vol. 45, Suppl.
Oct. 2005

文章编号: 1000-8608(2005)S-S157-04

面向报警处理生命周期的入侵响应管理系统

龚　俭[1], 李　杰[2]

(1. 江苏省计算机网络技术重点实验室, 江苏 南京　210096;
2. 东南大学 计算机科学与工程系, 江苏 南京　210096)

摘要: 在分析现有入侵响应工作模式的基础上, 提出一种面向报警处理生命周期的入侵响应管理模型, 并根据该模型设计一个入侵响应管理系统. 该系统可以基于报警的各个生命周期状态, 对响应过程进行有效的管理和控制, 使得响应动作能够适应环境的变化, 并有助于响应的自动实现.

关键词: 入侵响应; 报警; 生命周期; 响应管理; 网络安全
中图分类号: TP393.08　　**文献标识码**: A

0　引　言

近几年来, 网络安全事件不断增长, 技术也不断进步. 根据 CERT/CC 的调查[1] 显示, 安全事件的数量从 1989 年的 6 例上升到 2004 年的 16 万例; 网络安全问题受到越来越多的关注, 网络入侵的检测与防范已经成为一个亟待解决的问题, 入侵检测和响应系统作为保障网络安全的重要设施成为研究的焦点.

入侵检测系统不能作为独立保护网络的设施, 因为它的作用仅限于发现入侵行为和记录入侵行为, 所以入侵响应系统的研究显得越来越重要. 入侵响应是指对检测系统检测到的网络安全事件进行响应决策, 并生成响应策略. Crutis[2] 将目前的入侵响应系统分为以下 3 类:

(1) 预警型系统: 预警型系统只是将检测到的安全事件简单通知管理员而不作处理;

(2) 人工响应系统: 提供预先编制的响应程序, 管理员根据安全事件报告来选择对应的响应程序进行安全事件的响应;

(3) 自动响应系统: 自动进行响应决策并及时地对入侵作出响应, 从而留给攻击者尽量短的时间窗口.

自动响应系统是入侵响应中最优的实现方式, 目前有少部分响应系统支持主动响应, 但是响应效果不够理想, 并且缺乏对响应生命周期的管理; 安全事件从报警报告到处理过程的管理都由人工完成. 由于目前的入侵检测系统精度较低, 误报很多, 面对海量的安全事件报警和处理信息, 管理员的能力和经验严重地影响了事件响应的效率. 因此如何对事件进行有效的自动响应是入侵响应中一个值得关注的问题.

事件响应生命周期是指从安全事件报警到安全事件被成功处理所经历的过程, 其中涉及安全事件预处理、响应决策、响应执行等不同的处理环节. 事件响应是一个非线性的过程序列, 响应动作会随着环境的变化而进行调整, 通过响应生命周期的管理使得网络安全事件的处理过程变得更加高效、清晰.

1　入侵响应管理模型

1.1　响应管理模型概述

目前网络攻击呈现集群化、自动化、复合式、快速化的特点, 每次攻击通常由多个动作组成, 产生多个安全事件. 另外由于现有 IDS 的精度不高, 会产生很多误报. 目前安全事件的响应在其生命周期内应当包括以下 3 个处理步骤.

安全事件处理(预处理): 对报警的安全事件进行预处理并得到待响应的安全事件;

响应决策: 对待响应的安全事件进行响应决策得到响应要求;

响应执行: 根据响应要求选择响应程序执行响应动作.

上述处理过程与很多外部因素相关; 安全事件处理与目标主机配置和安全日志相关, 响应决策则和网络安全状态与响应策略等因素相关. 例如一次

收稿日期: 2005-08-09.
基金项目: 江苏省网络与信息安全重点实验室资助项目(BM2003201).
作者简介: 龚　俭(1957-), 男, 博士, 教授, 博士生导师, E-mail: jgong@njnet.edu.cn; 李　杰(1983-), 男, 硕士生, E-mail: jli@njnet.edu.cn.

DOS 攻击的开始步骤会是扫描, 获得目标的详细信息后再进行攻击. 响应系统需要发掘安全事件内在的关联才能进行有效的响应. 针对某个安全事件的响应方式通常有多个. 例如针对一次栈溢出攻击有如下的响应措施:

(1) 杀死主机上相应的服务进程及子进程;

(2) 查找并封锁主机上的可疑帐户;

(3) 监测外部到该主机可疑端口的通信, 并隔离攻击源;

(4) 将主机从网络中隔离.

其中: (1) (2) (3) 并不能完全消除攻击的危害, 因为攻击者可能在系统中种下其他形式的后门; (4) 能完全消除攻击的危害, 但是却造成了正常用户的损失. 因此响应要求的选择同时要考虑响应策略、网络安全状态等外在因素. 当确定一种响应要求后, 响应动作的实施分步骤进行, 且每个步骤的执行要依赖于当前的响应状态和外部条件的满足, 例如人工干预的完成等. 执行过程可能是并发多步或是循环多步. 因此从事件响应的一般过程看, 事件在到达后首先需要进行甄别和过滤, 以筛选出真正需要响应的事件, 即那些确实可能会对系统产生危害的事件. 然后系统要根据预定的响应策略对事件作出响应, 而这些响应往往由动作序列组成并需要一定的外部条件. 因此响应表现为一个条件不断被满足, 动作不断被执行的过程, 直至问题被根除为止. 基于这种思路, 事件响应生命周期可以体现为事件响应状态的变迁过程, 安全事件在其生命周期内可能会经历应该包括: 报警、待处理、处理、更除、残余等状态, 其状态机见图 1. 其中报警代表初态, 根除代表终态; 预处理过程包括事件筛选和关联型分析; 响应条件满足表示残余事件可以被响应; 事实上, 根据外部条件的满足情况, 响应动作序列中的动作可能可以并发执行, 所以需要通过一个调度来从待响应事件中选择事件进行响应.

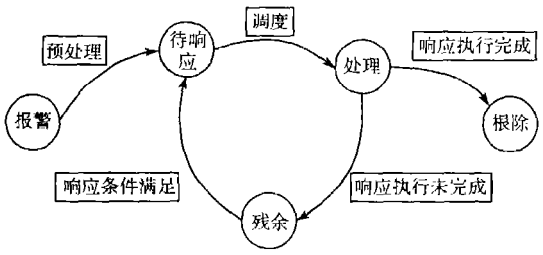

图 1　事件响应生命周期的状态机

Fig. 1　State machine of incident response life-cycle

综上所述, 安全事件响应是有生命周期的, 且在其生命周期内响应过程是动态的、非线性的, 甚至是循环的, 因此响应系统必须对响应生命周期进行有效管理才能进行有效响应. 依据这个思路, 本文设计并提出了一种面向安全事件生命周期的响应管理模型. 该模型综合考虑了安全事件响应所需要的各种信息资源, 包括安全事件管理、响应决策管理和响应执行管理等响应处理的主要环节; 其结构如图 2 所示.

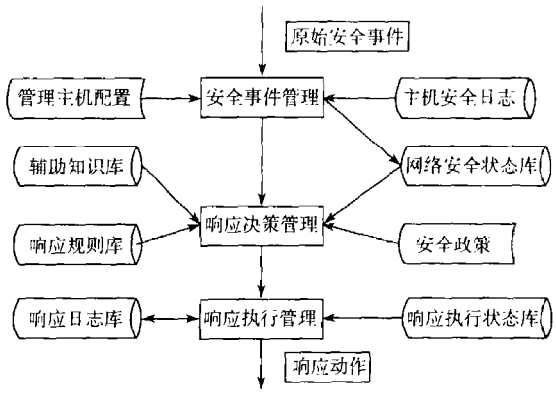

图 2　事件响应生命周期内的管理模型

Fig. 2　Management model in incident response life-cycle

1.2　安全事件管理

入侵检测系统精度不高的问题导致了网络安全事件误报很多, 面对大量的报警信息, 无法进行有效响应. 响应系统必须对 IDS 报警的安全事件进行有效管理, 筛选掉不需要响应的安全事件, 并对待响应的安全事件进行关联性分析, 把安全事件重组到攻击会话当中, 同时对安全事件进行统计并对网络安全状态进行分析.

安全事件筛选以事件特征与目标主机配置和安全日志的匹配为基础. 通过对事件针对的服务、操作系统等与目标的配置进行匹配和响应代价分析进行筛选. 例如针对一报警事件, 如果该安全事件是针对 http 服务而目标主机并未开放 80 端口则认为此事件不需要响应.

安全事件的统计根据同类型安全事件、同源地址事件、同宿地址事件等来进行. 若针对某一网络地址范围的安全事件很多并且安全事件的严重级别较高, 则说明该网络的安全状态较差, 则针对该网络的安全事件的响应优先级较高.

攻击会话的重组可以根据源宿地址进行. 将在一定时间间隔内同源地址、同宿地址的安全事件组合到一个初级攻击会话当中, 若干初级会话又可以组合成高级攻击会话. 攻击会话的重组为事件响应提供了攻击上下文.

安全事件的过滤可以大大减少待响应事件的数

量; 安全事件的统计给网络安全状态的评估提供了基础, 并能作为基于网络安全状态分析和响应决策的基础.

1.3　响应决策管理

响应决策是指针对待响应事件生成响应策略的过程, 该过程根据事件类型、网络安全状态、攻击上下文进行. 对决策过程进行管理使其能够根据网络安全状态和反馈的变化以及攻击上下文进行决策和自适应性的调整.

在响应决策模型的研究中, Fisch[3] 首次对事件响应进行了分类, Curtis[4,5] 在 Fisch[3] 的基础上提出了一种基于六维的面向响应的安全事件分类方法. Wenke Lee[6] 提出了成本敏感模型并将代价评估技术应用到响应决策中, 还根据 Lindqvist[7] 分类对 MIT 林肯实验室的 DARPA 入侵检测评估数据集中的攻击进行分类和代价估算.

对网络安全状态的评估和攻击上下文的分析可以确定安全事件的优先级, 事件响应总是选择优先级高的事件进行. 对安全事件进行基于事件分类和成本敏感的响应决策, 选择最优的响应策略并根据反馈机制进行响应决策的自适应性调整, 使得响应决策能够对响应策略进行量化, 增强决策的准确性并能够根据环境变化和反馈进行自适应性调整.

1.4　响应执行管理

响应执行是指根据响应策略从响应工具集中选择响应程序来进行响应动作的过程. 由于入侵技术的复杂性使得一次入侵相关的安全事件往往有多个, 同一次攻击中的安全事件彼此相关联, 一次处理并不能保证完成响应过程. 管理员往往要进行多个响应步骤才能完成对一个安全事件的响应, 步骤之间存在一定的时间跨度.

响应执行管理要针对响应的执行步骤进行; 每个响应步骤的执行都与当前的执行状态和过去的执行经验相关, 对执行步骤的管理使其能够根据响应的执行情况来调整后续的执行. 为每个事件的响应建立一条响应记录, 每完成一个步骤则更新此记录, 直到事件被根除. 执行时通过对已执行步骤、执行效果、其他执行情况, 以及过去经验的分析来决定后续的动作.

响应记录被保存在系统响应日志中, 其内容反映了系统对安全事件响应及其处理结果的历史信息. 这些信息不仅为响应过程管理提供了依据, 而且也为响应要求的自动生成提供了基础. 例如过去成功的响应要求是可以参照的, 不成功的响应要求是可以借鉴的.

2　入侵响应管理系统的设计

基于本文第 1 章所提出的管理模型, 本章介绍一个入侵响应管理系统 IRIS (incident response information system) 的设计.

2.1　系统体系结构设计

系统包括安全事件采集模块、事件管理模块、响应决策管理模块、响应执行管理模块和响应执行代理组成. 其总体结构如图 3 所示.

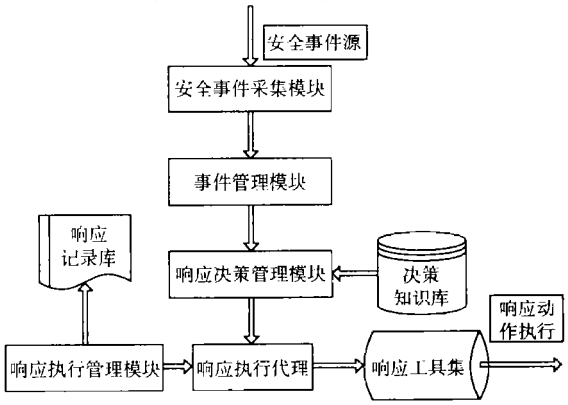

图 3　系统体系结构

Fig. 3　System architecture

2.2　安全事件采集模块

响应系统通常处于安全管理域内, 而检测系统则通常在管理域的网络边界上, 所以响应系统必须能够与检测系统进行通信并从检测系统的安全事件报告中采集原始安全事件. 安全事件也可能来自管理员的人工报告. 安全事件采集模块从入侵检测系统和管理员人工报告中采集原始安全事件, 将格式调整为系统要求的格式, 并送入事件管理模块进行处理.

2.3　事件管理模块

事件管理模块根据安全事件采集模块采集到的安全事件进行安全事件管理, 根据“1.2”节所述的安全事件管理模型对事件进行过滤、关联性分析和统计得到待响应事件, 并送入决策模块进行响应决策.

由于报警信息众多, 面对海量并且杂乱的数据, 响应系统不可能进行有效的决策. 系统必须对原始安全事件进行管理, 筛选掉不需要响应的事件, 减轻系统负担并为响应决策提供网络安全状态分析和关联性分析的结果以进行有效决策.

2.4　响应决策管理模块

决策管理模块对事件管理模块输出的待响应事件根据决策知识库的知识进行响应决策, 得到响应策略. 决策算法根据“1.3”节提到的基于分类和成本敏感的决策模型得到, 在决策过程同时根据网络

安全状态的变化和反馈机制进行自适应调整.

响应决策是响应系统的核心,是进行响应动作的基础,要求其能够随环境的改变进行自身调整.决策管理使其能够针对待响应安全事件进行有效的响应决策,并使其随着网络安全状态和反馈的变化自适应性地调整策略,为响应的实施提供良好的指导.

2.5 响应执行管理模块

响应执行模块对响应过程进行管理,管理模型基于"1.4"节所提到的办法,生成响应记录并存入响应日志.

响应系统对安全事件进行响应的过程可能由若干个响应步骤组成,每个步骤之间可能存在一定间隔.响应动作的执行要根据响应动作执行的上下文来进行;系统提供对响应步骤的管理,使得每个步骤的执行都更准确并具有自适应型;管理模块同时提供对响应记录的查询和统计分析接口.

2.6 响应执行代理

响应的执行通常是从响应工具集之中选择响应程序执行响应动作.响应工具集提供调用接口,系统必须存在一个功能单元通过该接口调用响应程序.响应执行代理就是通过调用接口来调用工具集中的响应程序进行响应动作的功能模块.

3 结 语

入侵响应系统是保护网络安全的一个重要的措施,入侵自动响应系统应能够对入侵检测系统报警的安全事件进行响应决策并生成相应的响应要求.为支持入侵自动响应系统的实现,定义安全事件的生命周期是一种有效的方法.通过对安全事件生命周期的管理,系统可以对各种响应要求作出自动的调度,控制响应的进度,自动评估响应的效果,从而可对响应动作进行必要的动态调整.这种安全事件响应模型与系统安全评估模型和入侵检测功能结合在一起,可以构造出一个综合的安全管理系统,可以对网络和应用系统进行有效的自动管理.

参考文献:

[1] CERT Coordination Center. CERT/CC Statistics 1988-2004[EB/OL]. 2004[2005-08-05]. http://www.cert.org/stats/cert_stats.html.

[2] CARVER C A. Intrusion response systems: A survey [EB/OL]. 2003[1005-08-02]. http://faculty.cs.tamu.edu/pooch/course/CPSC665/Spring2001/Lessons/Intrusion_Detection_and_Response/rtirs2.doc.

[3] FISCH E A. Intrusion damage control and assessment: A taxonomy and implementation of automated response to intrusive behavior[D]. Austin: Texas A&M University: College Station, 1996.

[4] CARVER C A, JOHN M D. HILL U W. Pooch limiting uncertainty in intrusion response[A]. **Proceedings of the IEEE Workshop on Information Assurance and Security** [C].[S.l.]:[s.n.], 2001.

[5] CARVER C A, POOCH U W. An intrusion response taxonomy and its role in automatic intrusion response [A]. **Proceedings of the 2000 IEEE Workshop on Information Assurance and Security**[C]. NY: United States Military Academy, West Point, 2000: 129-135.

[6] LEE W, FAN W, MILIER M, *et al*. Toward cost-sensitive modeling for intrusion detection and response[J]. **Journal of Computer Security**, 2002, **1**: 318-336.

[7] LINDQVIST U, JONSSON E. How to systematically classify computer security intrusions[A]. **Proceedings of 1997, IEEE Sympcsium on Security and Privacy**[C]. Oakland:[s.n.], 1997: 154-163.

Incident response management system based on alert life-circle

GONG Jian[1], LI Jie[2]

(1. Computer Network Technology Key Laboratory of Jiangsu Province, Nanjing 210096, China;
2. Dept. of Computer Science and Engineering, Southeast University, Nanjing 210096, China)

Abstract: Based on the existing security incident response working scheme, a novel incident response management model is proposed in the paper, which is based on the concept of alert life-circle. An implementation structure of this new model is also given. The system can manage and control the incident response process according to its current state in its life-circle, and adjust the response actions as the environment changes. This model can provide an efficient response management and is beneficial to the implementation of automatic response as well.

Key words: incident response; alert; life-cycle; response management; network security