分布式计算机应急响应事件管理系统

朱礼智[1]，龚俭[1]，杨望[1]

（1. 东南大学计算机科学与工程学院，南京，211189）

摘　要：随着网络安全事件日益增长，安全事件相关的应急响应在网络安全体系结构中已经成为不可或缺的重要环节。本文根据国际上最权威的应急响应 PDCERF 六阶段的总体框架，结合华东（北）地区网络中心应急响应小组的响应实践整理且规范设计了 CERNET 网络中心的事件响应工作流，并参考票据系统，开发出了应急响应系统 DIM，部署应用在 CERNET 的 38 个主节点。运行结果表明，该系统能够有效支持事件应急响应工作。

关键词：安全事件;应急响应;工作流;分布式;票据系统

Distributed Incidents Management System for Computer Emergency Response

Lizhi Zhu[1], Jian Gong[1], Wang Yang[1]

(1. School of Computer Science and Engineering, Southeast University, Nanjing, 211189)

Abstract: With the rapid development of Internet technology, the response of related security incident is an essential part of the network security architecture. This thesis brings forward an incident response workflow that fit for the requirement of CERNET Eastern China(North) Network Center, based on the whole frame of the most authoritative PDCERF six phases incident response procedure in the world,and develops DIM(short for distributed incidents management system) according to the workflow and ticketing system. DIM has been deployed in the 38 key nodes in CERNET.The system has been proved efficient for supportingt the Incident Response through practice.

Key words: security incident; incident response; workflow; distributed system;ticketing system

当前，我们正处在一个安全事件多发和频发的信息时代[1]。2013 年，斯诺登披露的“棱镜门”事件，引发了国际社会和公众对网络安全的空前关注。而在我国，随着互联网升级全面提速，用户规模快速增长，移动互联网新型应用层出不穷，网络安全问题也变得日趋严重。2013 年度，我国境内感染木马僵尸网络的主机为 1135 万个，控制服务器为 16 万个，境内 6.1 万个网站被境外通过植入后门实施控制，较 2012 年大幅增长 62.1%[2]。同时针对我国银行等境内网站的钓鱼页面数量和涉及的 IP 地址数量分别较 2012 年增长 35.4% 和 64.6%。其中，针对僵尸网络，CNCERT(National Computer Network Emergency Response Technical Team)会同基础电信企业、域名注册服务机构共清理木马僵尸网络控制服务器 3.4 万余台，受控主机近 72 万个，分别只占总数的 21.25%和 6.34%。

目前看来，事件的发生是不可避免的，我们所能做的就是在各种意外事件发生后采取必要的措施，避免、降低危害和损失，以及从危害和损失中恢复[3]。事实上，成功的事件处理需要大量的组织和计划，需要大量的专业人力和物力。首先，事件报告要能够及时的反馈到相关部门，并做好记录工作。相关部门和负责人收到事件报告，在确定核实后，要能够及时的部署抑制措施，并尽快确定方案根除事件。在事件根除后，相关负责组织还要进行恢复和跟踪工作。

“十一五”211 工程建设在 CERNET(China

作者简介：朱礼智，（1989-），男，硕士研究生，E-mail：lzzhu@njnet.edu.cn；龚俭，（1957-），男，教授、博士生导师，E-mail：jgong@njnet.edu.cn；杨望，（1979-），男，讲师，E-mail：wyang@njnet.edu.cn

Education and Research Network)网络中心和38个核心节点建设高性能网络管理与安全保障系统，对CERNET主干网运行安全基本保障系统升级改造，保持对网络流量数据的实时监控能力。DIM(Distributed Incidents Management System)作为该项目应急响应协同服务系统的一部分，旨在根据事件应急响应的过程和华东（北）地区网网络安全事件响应组的事件响应经验，设计一套适用CERNET的事件响应工作流，并开发出相应系统部署应用到CERNET各节点。该系统要能够反映出安全状态并能有效支持事件响应工作。本文第1节对事件相关的知识以及系统需求的简单分析。第2节给出系统的设计及数据来源。第3节为系统实现及系统结果分析。第4节为最后一节，对全文进行总结并提出下一步的研究重点。

1 背景知识介绍

1.1 事件

安全事件(简称事件)，指的是影响计算机系统和网络安全的不当行为。这些行为包括在计算机或网络上发生的可以观察得到的任何现象，包括通过网络连接到另一个系统、获取文件、关闭系统等。恶意事件包括对系统的破坏，在某个网络内IP包的泛滥，未经授权的情况下使用另一个用户的账户或系统的特殊权限，入侵一个或若干个网页以及执行了恶意代码并毁坏证据。广义的事件还包括自然灾害和能源有关的破坏，但并不在本论文的讨论范围之内。

安全事件可分为很多类别，但由于“安全”传统上认为是保证保密性、完整性和可用性（CIA），因此从最基本的意义上讲，事件都是对CIA的某种程度的破坏。安全事件发生的方式具有多样性，根据事件的不同类型可划分为拒绝服务攻击、恶意代码、非授权访问、不当使用等。

1.2 事件响应

事件响应是事件发生后采取的措施和行动。这些行动措施通常是阻止和减小事件带来的影响。行动可能来自于人也可能来自于计算机系统。

事件响应一般需要多组织、多机构间的相互协作才能有效完成。事件响应的许多方面涉及到事件的准备工作和如何使事件响应人员更有效的工作。另外，事件响应还涉及到如何管理随着事件的发生而不断增长的大量数据。

通常事件响应是只有技术人员才能胜任的工作。实际情况下，技术人员也是事件处理中的主要人员，事件响应除了需要技术技能，还需要管理能力、法律知识、人际关系方面的培训、技术说明写作技巧，甚至心理学方面的知识。

1.3 事件响应方法学

应急响应六个阶段包括准备、检测、抑制、根除、恢复、总结。在检测系统检测到有安全事件发生之后，下一步则限制攻击范围和潜在的损失与破坏；在事件被抑制以后，应该找出事件根源并彻底根除；然后着手恢复系统，恢复的目的是把所有受侵害的系统、应用、数据库等恢复到正常的工作状态。应急响应方法学中的这六个阶段是循环的，每一个阶段都是在为下一个阶段做准备。如图1所示为应急响应的生命周期。

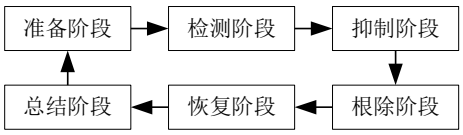

图1 应急响应生命周期

应急响应本质上是一个知识积累与应用的过程：准备与检测阶段是对具体环境的知识积累；抑制、根除和恢复阶段是对积累知识的应用，总结阶段是知识的更新或累加。从这个角度上讲，应急响应系统（包括DIM）也是一个知识管理系统。响应人员运用DIM的知识进行事件响应，并通过响应总结将新的知识反馈给DIM进行新的积累。当然，如前文所述，DIM只是应急响应协同服务系统的一部分，并不包括检测功能。

由于DIM面向教育网内的安全事件，但教育网有38个主节点，对于各个节点来说，他们能够看到和自己相关的事件即可。考虑到事件数量的庞大，DIM采用分布式结构，每个节点都有自己独立的子系统，存储和本节点相关的事件。

DIM 为各节点事件响应人员提供事件知识管理和知识交换的功能。知识交换为应急响应人员提供了多种获取事件信息的方式，包括从其他CERNET主节点查看其相关案例等。事件知识管理为应急响应人员提供了事件从立案、响应、归档各

阶段知识管理。此外 DIM 还可以提供知识总结归纳功能，即安全状态查看功能。

1.4 工作流

工作流[4]，就是业务过程的部分或整体在计算机应用环境下的自动化，它能够使在多个参与者之间按照某种预定义的规则传递文档、信息、任务的过程自动进行，从而实现预期的业务目标，或者促进此目标的实现。

工作流具有图形化、可视化设计流程图，功能强大的表单功能，丰富的统计、查询、报表等特点。因此本文将基于工作流来完成，以提供图形化的操作界面，强大的统计、查询、报表功能，方便的通信机制，从而提高事件响应的效率。

1.5 票据系统

票据系统[5]（Ticketing System）是一种基于 Web 的解决管理问题的全新方法。它的工作原理是把相关工作人员、问题组织到一个独立而统一的支持系统中，并把问题以票据的方式分配给处理人员。每个工作人员仅能够处理指派给自己的票据。每个工作人员的票据列表可以看成一个单独的队列，同时票据可以从一个队列移到另一个队列，直到它被解决。一旦问题以票据形式出现在系统中并且指派人员去处理，工作量将会大大减小。总之，票据系统可以使处理人员和大量问题变得井井有条。

2 系统设计

2.1 总体结构设计

由 1.3 节可知，各个节点的 DIM 子系统对等，且具有相同、完整的事件响应管理功能。此外，为了能够监控整个教育网的安全状态，并获知每个节点 DIM 子系统的运行状态，系统提供一个总控节点，但该节点不支持具体事件响应。因此，DIM 最终采用易扩展、易维护的星型结构，总体结构如图 2 所示。图中威胁评估系统为上文所述应急响应协同服务系统的另一个子系统。

图 2 中的数据来源主要包括以下三种[6] [7]：

1. NBOS(Network Behavior Observation System)：NBOS 目前在 38 个教育网主节点所管理的网络边界均已部署，它基于 NETFLOW 进行异常检测，其检测出的 DDoS 和主机扫描事件汇报到 DIM，而 DIM 将这两类事件归为 DDoS 和被攻破主机事件[8]。
2. 蜜罐系统：清华大学开发并在 38 个教育网主节点部署，采用低交互蜜罐完成 Botnet 主机活动信息采集。报告给 DIM 的是 Botnet 相关事件。
3. 恶意代码监控系统：上海交通大学开发并部署在北京、上海、广州三个节点，采用全包文采集方法，检测 Webshell，木马活动，在 DIM 中归为挂马网站类事件。

此外,用户事件报告，可报告各类事件。进入 DIM 的数据为 2.2 节介绍的事件基本信息及相关报告信息。

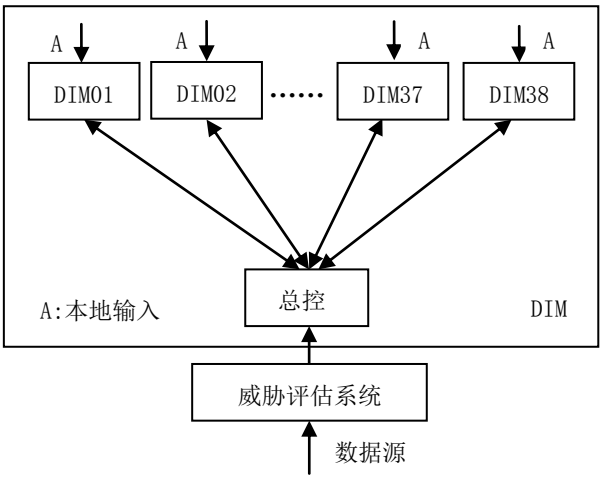

图 2 DIM 系统总体结构图

2.2 事件知识设计

DIM 面向事件对象。事件知识在 DIM 中包括事件基本信息、相关报告、响应知识。事件基本知识包括事件相关 IP 信息、事件类型、事件状态、发生时间等信息。对于每一个事件，包括事件的证据知识以及响应知识。相关报告主要是上述响应过程在检测阶段发现的异常信息，对于不同种类的事件不尽相同。响应知识记录事件响应过程，包括响应人员的处理方法和处理结果等。证据知识和响应知识在系统中表示为文本和附件，本文不作详细介绍。

2.4 工作流设计

事件基本知识中的事件状态反映了整个事件处理流程。按照 NJCERT 事件应急响应实践，事件在其生命周期中包括 2 个宏观状态： open（打开）、resolved（解决）。具体如下：

1. open（打开）：事件处理过程中。

2. resolved（解决）：事件已解决。

随着事件处理的进展，事件状态将发生转换，对应于状态转换图，其转换规则如下：

① ：事件进入系统，默认按单位进行分配。

② ：事件获得新的汇报信息。

③ ：事件解决。

④ ：事件归档。

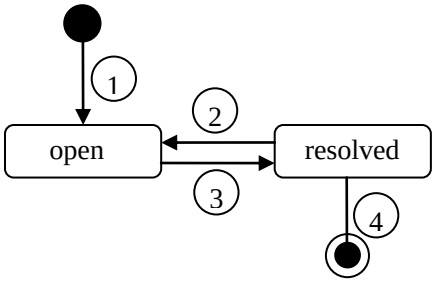

图 3 事件状态转化图

在 DIM 中，事件以 Ticket 形式管理。事件进入系统时，即是一条新 Ticket。根据事件的 IP 信息，DIM 可以自动获取负责单位，并将此事件分配给该单位的处理人员。至此，Ticket 进入该处理人员的处理队列。通常情况下，Ticket 将一直归当前处理人员负责，直到响应结束。

此外，DIM 提供事件知识归纳总结功能。以图表形式给出各单位事件数量统计、事件分类统计、事件威胁 IP 信息统计、事件变化趋势统计等信息。

2.4 权限设计

表 1 系统权限设计表

编号	角色	数量	权限	权限描述
1	普通用户	若干	低	响应所属事件，浏览
2	管理员	1	高	系统管理

对于 CERNET 下的各个单位，DIM 采用各单位分管各自事件的策略，他们只对自己的事件有修改响应权限，对其他事件有浏览权限。在 DIM 中，他们属于“普通用户”，每个用户有自己的 Ticket 队列。管理员负责系统管理，包括用户管理、系统配置等。同时,管理员有权限修改普通用户的误操作。

2.5 子系统结构功能设计

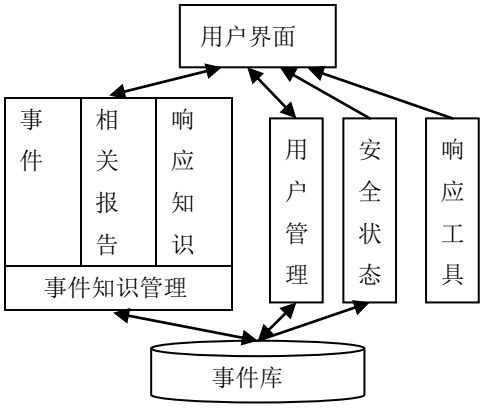

图 4 DIM 子系统结构功能图

如图所示，根据 2.1 节到 2.3 节的设计，该系统主要包括五个功能模块：事件知识管理、用户管理、安全状态、响应工具、用户界面。其中事件知识管理包括事件、相关报告、响应知识三个子模块。事件部分提供浏览、搜索、增加、修改、删除操作；相关报告提供浏览以及对误报的删除操作；响应知识提供浏览、增加、修改、删除操作。用户管理为管理员提供响应人员信息的添加、修改、删除操作。为各响应人员提供各自信息的维护功能。安全状态提供各节点事件整体情况统计，包括事件类别统计、事件数量变化趋势、IP 相关信息统计等。响应工具部分供响应人员参考使用，具体参见 3.2 节。

3 系统实现及结果

3.1 系统实现及部署

DIM 目前已经部署在教育网 38 个主节点，在总控端，用户可以查看各子系统运行状态。如图 5 所示，页面顶部显示所有节点的事件汇总情况。接来下的列表显示各个节点的运行状态，“安全状态”列和 DIM 相关，蓝色状态灯表示正常运行，红色状态灯表示总控子节点运行异常。

图 6 是各个节点的 DIM 首页截图。该首页上方时响应人员负责处理的事件总数、待处理事件数、已处理案件数。中间部分是该节点的事件统计，包括挂马网站、内部后门、攻击、外部威胁点的事件数量和涉及主机数量统计。下方是响应人员待处理的事件列表。

图 5 总控首页

图 6 各节点 DIM 首页

3.2 事件响应

3.2.1 事件响应过程

事件进入 DIM 时，生成事件 Ticket，并自动分配给负责单位。这些单位的响应人员登录系统后，可以查看到自己需要处理的事件队列。进行事件响应时，响应人员主要根据事件基本信息和相关报告来采取相应措施。当然，通过搜索事件库，他们能够查找到相似事件以获取更多的信息。此外，他们还可以借助 DIM 提供的以下工具：IPDB，WHOIS，NBOS 等。IPDB 是教育网为 CERNET 运行管理和安全保障所建立的 IP 综合信息系统，提供 IP 地址的使用信息，包括 IP 地址的管理归属、使用位置、服务类型、通信特征和活动历史。通过 IPDB 可以查询 IP 相关信息，WHOIS 可以查询域名相关信息，NBOS 可以查询相关 IP 是否存在热点信息等。

3.2.2 事件响应实例

本文以 2013 年 12 月 17 日发现的一个僵尸网络主机为例，详细阐述 DIM 中事件响应的过程。首先该主机属于某地区网络中心，所以这个事件在进入系统时，已经自动被分配给该地区网络中心响应人员，事件状态为“open”，即是从“检测阶段”进入了“抑制阶段”。图 7 为该事件基本信息。

图 7 事件基本信息

同时，我们在事件中可以看到检测到这个事件的相关报告(图 8)。针对这个僵尸主机，系统中有 4 条相关报告显示此次攻击属实。

图 8 事件相关报告

响应人员可以根据案件基本信息和相关报告处理此事件。DIM 提供响应过程的添加、编辑、删除功能，同时能够上传证据附件。从图 9 中可以看出，响应人员首先对该事件僵尸主机进行了安全检查。以便决定下一步采取何种措施。从检查结果来看，该僵尸主机仅存在异常流量信息，并且目前不在第三方黑名单中，其危害并不是很大。因此响应人员给出了抑制措施：协同 NOC 进行相关处理。事件进入“根除阶段”。当 NOC 反馈处理信息时，响应人员可以清楚地知道该 NOC 已经通知用户进行清理。至此，响应人员可以认为事件响应的“根除阶段”和“清理阶段”已经完成，进入“总结阶段”。在 DIM 中，响应人员只要将事件状态标记为“resolved”，即可完成总结，该事件知识将作为案例保存在 DIM 中。当然，并不排除用户清理和恢复不成功的情况，当“检测阶段”再次发现该僵尸主机活动时，根据 2.4 节状态转换规则②可知，该事件将再次进入“open”状态，重复上述响应过程。

图 9 事件响应过程

4 总结

本文的主要工作是以华东（北）地区网络中心为应用背景，研究和设计分布式应急事件响应管理系统。通过系统实际运行，可以看出这个系统可以反映安全状态并有效支持事件响应工作。但同时该系统也存在一些不足之处。比如针对东南大学事件较多的情况，相关处理人员可能无法及时进行响应。下一步工作可以针对对系统的事件库进行数据挖掘，总结事件发生、处理规律，对事件的预防、解决都会有很大的帮助。进一步地，在事件分类的基础上，研究针对各类安全事件的响应对策，从而建立一个应急响应决策专家系统，以减少繁复的响应工作。

参考文献

[1] （美）E.Eugene |Schultz，Russell Shumway．网络安全事件响应[M]．中国教育和科研计算机紧急响应组（CCERT），段海新等译．北京：人民邮电出版社，2002

[2] CNCERT．2013 年我国互联网网络安全态势综述[EB/OL]．http://www.cert.org.cn/publish/main/upload/File/2013%20Network%20Security%20Situation(1).pdf，2014-03-28

[3] 国家计算机网络应急技术处理技术协调中心(CNCERT/CC)，全国网络与信息技术培训项目管理中心(NTC-MC) 编著．网络安全应急实践指南[M]．北京：电子工业出版社，2008．

[4] 吴朝晖，邓水光．工作流系统设计与关键实现[M]．杭州：浙江大学出版社，2006．1-9

[5]Internet Man, Inc.．Ticketing System[EB/OL] ．http://ticketingsystem.com/，2014-04-02

[6]杨望等．CHAIRS 总体设计报告[EB]．2013．10．

[7]杨望．CERNET2013 年会 CHAIRS 介绍[EB]．2013．10．

[8] 龚俭，吴桦，杨望编著．网络安全导论（第二版）[M]．南京：东南大学出版社，2007．9．