doi: 10.7690/bgzdh.2016.07.011

一种分级部署主动防御系统可视化展示平台

张建平，李洪敏，卢　敏
（中国工程物理研究院总体工程研究所，四川 绵阳 621900）

摘要：针对现有主动防御系统在告警数据可视化展示中缺乏分级和告警数据联动功能，以及在告警数据的访问控制不足的问题，设计并实现一种分级部署的主动防御系统可视化展示平台。通过表示层、业务逻辑层和数据访问层 3 层体系设计，实现安全态势、安全分析和威胁实时感知等数据库告警数据可视化展示功能。通过服务器多级级联设计和多角色用户权设计，实现主动防御系统告警数据的受控访问。实验结果表明：该平台能为管理者提供单位防病毒和木马态势，让上级单位及时获知并提前发送相应的防护策略，从而可有效遏制病毒和木马的广泛传播。

关键词：可视化；分级部署；主动防御
中图分类号：TP393　　**文献标志码：**A

A Hierarchical Deployment Visualization Platform of Active Defense System

Zhang Jianping, Li Hongmin, Lu Min
(*Institute of System Engineering*, *China Academy of Engineering Physics*, *Mianyang* 621900, *China*)

Abstract: Aiming at the shortcomings of the existing active defense system in the visual display of alarm data, including the lacking of hierarchical display, alarm data linkage function and the weak access control of the alarm data, the paper designs and implements a hierarchical deployment of active defense system visualization display platform. Through the design of three-layer system which contains presentation layer, business logic layer and data access layer, the platform realizes the visualization of security situation, safety analysis and real-time threat perception which are contained in alarm database. Through the multilevel cascaded design of server and multi role user authority design, the access of alarm data is safely controlled within the legitimate users. The experiment demonstrates that the display platform not only provides the situation of defending viruses and Trojans to the leadership, but also informs the related personnel the alarm information to effectively curb the spread of viruses and Trojans.

Keywords: visualization; hierarchical deployment; active defense

0　引言

作为敌特间谍机构窥视和监控的重要目标，我国军工单位的办公区及 Internet 网上的计算机被植入未知的特种木马和孤本病毒的事件时有发生。尽管军工单位的涉密信息系统与 Internet 网物理隔离，但由于科研生产和技术交流的需要，涉密信息系统与 Internet 间接的信息交换依然大量存在。虽然各单位采取了相应的技术和管理措施，但涉密信息系统内计算机感染已知和未知病毒及木马的事件依然频发，涉密信息被轮渡木马及特种木马带出涉密网的隐患也依然存在[1]。

为提升涉密信息系统对未知病毒和木马的防御能力，解决传统的安全防御产品很难有效抵御未知新型恶意代码的攻击和入侵问题，不少军工单位已经率先在涉密信息系统中部署了主动防御系统，对已知和未知的恶意攻击行为均起到良好事前防御作用，并取得了较好的效果[2-3]。但现有的主动防御系统的告警数据却只能在特定的环境中被特定的人员查看，使得告警数据未能发挥出应有的作用[4]。特别是在具有多级结构的军工单位中，下级单位的告警数据无法及时反馈给上级单位，从而使得告警不能在病毒传播到其他单位之前被上级单位获知并提前采取措施阻止病毒和木马的扩散。另外，分级部署的涉密网络主动防御系统可视化展示平台目前已被大量应用[5]，但离军工单位的要求仍有差距[6]。

笔者针对当前主动防御系统展示平台在多级联动可视化展示的不足，结合分级保护标准，设计并实现一种分级部署的主动防御系统可视化展示平台。该平台具备严格的“三员”权限控制功能，支持分级部署，使得告警数据能被上级单位及时获知并提前向其所属单位发送策略，从而有效遏制病毒和木马的广泛传播。同时，该系统为管理者提供专门的视图，使得管理者能够及时了解单位的病毒防御工作状况，一旦发现病毒便能立即作出应变决策。

1　分级部署可视化展示平台的设计

1.1　平台概述

主动防御系统可视化展示平台以主动防御系统的安全数据的受控可视化为目标。既要完成对主动

收稿日期：2016-03-11；修回日期：2016-04-14
作者简介：张建平(1986—)，男，四川人，工程师，硕士，从事信息安全研究。

防御系统安全告警数据的分级可视化展示，为主动防御系统管理员、安全保密管理员、安全审计员和单位的管理者等多种角色提供相应的视图，又要考虑将告警数据在分级展示过程中的访问控制与主动防御系统管理员权限进行分离，实现主动防御系统告警数据的访问控制和数据价值的最大化。

1.2　平台总体设计

主动防御系统采用 C/S(Client/Server)结构进行系统设计，通过数据访问层实现平台数据在各级服务器和客户端的传输，通过业务逻辑层实现数据访问层到表示层数据的封装和业务逻辑的转换，通过可视化展示平台客户端程序实现主动防御系统数据的展示。展示平台通过以上三层体系实现可视化平台中数据的有效展示和授权访问功能。图 1 展示了可视化展示平台的系统框架。

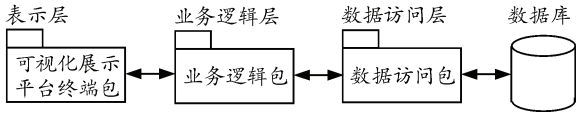

图 1　平台系统框架

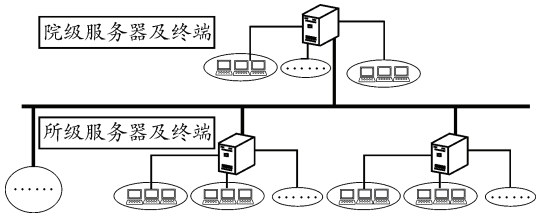

图 2　系统两级部署架构

主动防御系统可视化展示平台是在现有主动防御技术基础上，设计为可支持多级部署的可视化展示平台。为便于阐述，笔者以支持两级部署的可视化展示平台为例，阐述分级部署的主动防御系统可视化展示平台的设计与实现。图 2 展示了典型的支持两级部署的系统架构。主动防御系统两级的服务端分别负责各级的病毒、木马监控和处理，同一级中支持多安全域同级部署，二级服务器负责向一级服务器上报病毒、木马的攻击情况。

1.3　用户权限分离设计

系统权限分离方面，参照分级保护和现有的安全产品的设计，按照权限分离原则，在两级展示平台分别设计了“三员”和操作员用户功能。其中，展示平台的系统管理员可完成组织架构的创建、用户的创建、终端健康状态的查看、报表的查看和导出等功能；安全管理员可完成用户角色的分配，可为普通用户配置可查看的范围；安全审计员可完成对“三员”操作日志的审计；普通的操作用户可查看在授权范围内的终端的健康状态数据和报表数据；系统还设计了相关主管领导的账号类型，为主管领导提供单位内病毒和木马防御态势的报表等数据，为主管领导决策提供依据。表 1 展示了系统在权限分离方面的设计。

表 1　系统权限设计

用户类型	用户权限
系统管理员	创建、编辑、删除组织机构 创建、编辑、删除用户 编辑终端所属组织结构 查看、分析和导出各类报表数据
安全保密管理员	修改用户的角色 修改操作员查看数据的范围
系统审计员	审计用户的操作日志
普通操作用户	查看授权范围内的数据 查看授权范围内的终端的监控状态数据
相关主管领导	查看单位内病毒和木马数据报表 查看单位内病毒和木马防御态势

1.4　平台功能模块设计

分级部署的主动防御系统可视化展示平台核心功能是完成对多种角色用户展示主动防御系统告警数据。为此需实现各级展示平台间数据的通信和多级服务端数据的有效级联，即实现在一级平台展示各二级单位的总体防病毒态势，能在二级平台展示各二级单位信息系统对病毒和木马、恶意代码等防御态势并能精确跟踪到单个计算机的健康状况。

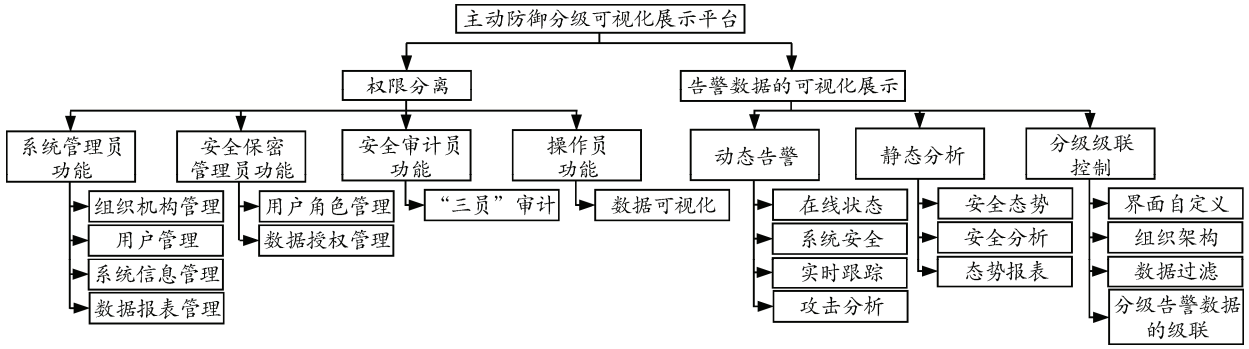

图 3　平台功能模块设计

在主控制台界面，笔者设计了攻击分析、系统安全、实时跟踪、组织架构、态势报表等功能导航，

可以从不同的视角对安全数据进行分析。另外在实时和历史数据展示方面，笔者设计了安全态势(终端安全分数段比例构成图)、安全分析(一个月内受攻击计算机终端的统计数量走势)、威胁实时感知(实时受攻击的 IP 及告警信息)等指示器[7]。图 3 展示了该平台的功能模块设计。

2　可视化展示平台的实现

根据上述可视化展示平台的设计思路，笔者在可视化展示平台实现过程中，采用了 flash 编程、数据库编程、网络通信编程、Windows 控件自绘技术和 VC++进行设计实现。

图 4 展示了作为二级单位的“D 部”受到某种攻击时，可视化展示平台呈现的主界面；图 5 展示了“D 部”受到攻击的同时，“D 部”所在的“B 所”在一级展示平台上出现的告警信息。

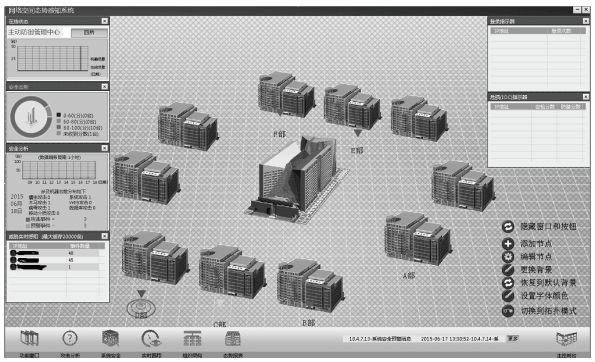

图 4　视化展示平台二级主界面

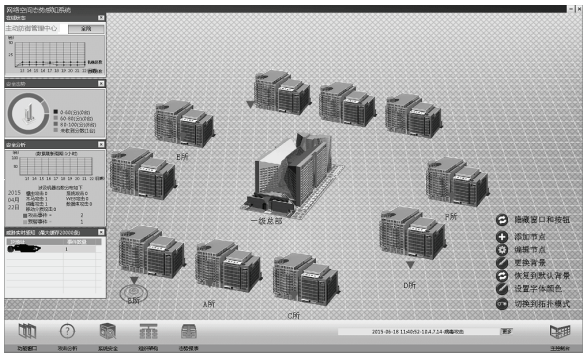

图 5　可视化展示平台一级主界面

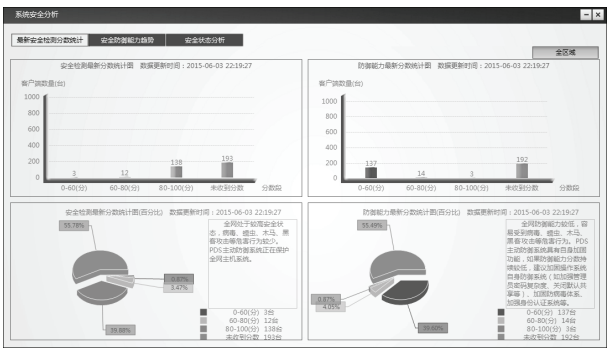

图 6　安全检测评分统计界面

图 6 和图 7 分别展示了安全检测评分统计情况和最一个月安全检测平均分数和防御能力平均分数的趋势。

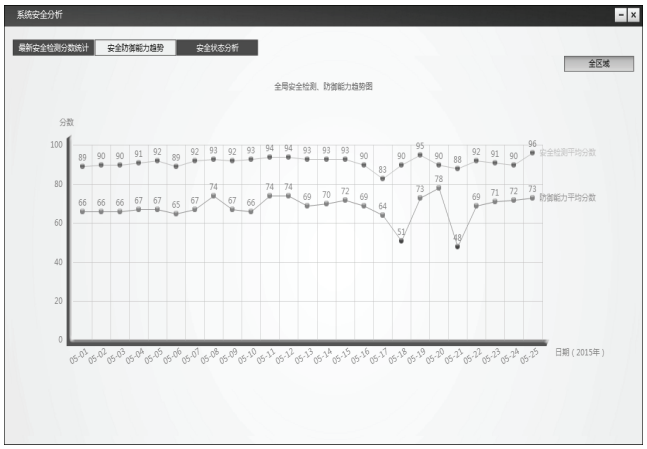

图 7　防御能力趋势界面

3　结束语

笔者设计并实现一种分级部署的主动防御系统可视化展示平台。通过告警数据可视化和系统权限分离的设计，实现在一级平台展示本级单位和各二级单位的总体防病毒态势，在二级平台展示本级单位信息系统对病毒和木马、恶意代码等的防御态势并能精确跟踪到单个计算机的健康状况。通过安全态势和安全分析功能模块的设计，实现对历史告警数据的分析和展示；通过威胁实时感知和实时跟踪等功能模块，实现对告警数据的实时监控，并能将实时数据及时上报给上一级展示平台，避免病毒和木马在大范围内的传播。

参考文献：

[1] 李洪敏, 李宇明, 张建平, 等. 基于局域网的主动防御技术应用[J]. 兵工自动化, 2013, 32(12): 20-22.

[2] 陈超, 妙全兴. 蜜罐技术研究[J]. 计算机安全, 2009(8): 33-34.

[3] 杨闯朝. 主动防御及其反制技术研究[C]. 厦门: 中国社会科学出版社, 1994.

[4] Lu Wenlian, Xu Shouhuai, Yi Xinlei. Optimizing Active Cyber Defense[J]. Lecture Notes in Computer Science, 2013, 8252(1): 226-245.

[5] 李琳琳, 曹凯滨, 谢伟秋. 可视化监理平台的研究与实现[J]. 测绘与空间地理信息, 2014, 37(1): 115-117.

[6] 罗晓波, 王开建, 徐良华. 基于行为分析的主动防御技术及其脆弱性研究[J]. 计算机应用与软件, 2009, 26(7): 269-271.

[7] 方小卫, 黄旭荭, 李涛, 等. 软性材料制造业服务平台研究[J]. 机电工程, 2015, 32(8): 1027-1032.