文章编号：1005-8451(2007)09-0024-03

企业安全管理系统的设计

徐 斌
(南京铁道职业技术学院，南京 210015)

摘 要：各种单一的安全解决策略已不能应付现在复杂的网络安全环境，企业安全管理（ESM）系统集中管理各种不同的安全系统，如防火墙、入侵检测系统、虚拟专用网等，形成一个完整的安全系统。分析现有的ESM系统，并针对缺乏内网安全性的问题提出一个新的ESM系统结构，并进行模拟验证。

关键词：网络安全；企业安全管理系统（ESM）；入侵检测系统；内网安全
中图分类号：TP39 文献标识码：A

Design of Enterprise Security Management System

XU Bin
(Nanjing Institute of Railway Technology, Nanjing 210015, China)

Abstract: Various single security solution couldn' t cope with more and more complex network security environment. Enterprise Security Management (ESM) was centralized integrated management of heterogeneous security solutions, such as firewall, IDS, VPN. It was analyzed existing ESM System and, based on the results, proposed a new structure of ESM System with reinforced internal security and tested it..

Key words: network security; Enterprise Security Management System; IDS; internal security

网络上各种各样服务如电子商务、电子银行等日益普及。网络的普及给人们生活和工作带来各种便利的同时也带来了安全问题，如不健康信息的传播、信息犯罪等。为了建立企业安全管理系统，提出并设计了一个强化内部网络安全的企业安全管理（ESM）系统。

1 企业安全管理系统的结构设计

1.1 企业安全管理系统概念

企业安全管理是将不同的安全解决策略，如入侵检测系统、入侵切断系统以及虚拟专用网等安全技术集中统一管理，使之成为一个整体。目前的企业安全管理（ESM）系统一般仅是对同种类型的产品实现监控功能，为了监控使用不同种类型的安全产品的安全系统，分析它们所收集的数据，报告安全事件，管理每个安全系统的具体策略，ESM更多考虑安全协议标准。比较通用的ESM的安全标准协议是OPSEC。安全性开放式平台（OPSEC）可提供业界企业级策略管理和策略执行框架。构成OPSEC联盟的300多家公司采用OPSEC框架，为客户提供了企业级网络安全各方面的解决方案。

1.2 设计高内部安全性的ESM

现在采用一种安全产品对系统进行安全保护，检测异常行为，阻止入侵是不足以保证信息安全的，复杂的网络环境需要使用多种安全解决方案。事实上现在并不缺少安全的专业解决方案，如有防火墙，入侵检测系统，虚拟专用网和防病毒软件等。

在各种电子商务活动中，信息系统暴露在内外网络上。因此，信息系统的安全，特别是可靠性和可用性受到较大威胁。

随着安全管理的重要性的增加，越来越多的公司采用ESM的解决方案。这些ESM的目标是集中管理各种不同的安全系统，通过分析相互的信息，发现尽可能多的安全问题。ESM与非集中管理的安全系统相比，具有减少资源消耗，提高安全管理的效率的优点。

这些ESM系统有一个树型结构，安全措施应该在内网和外网都要实施，然而，目前的ESM在内网都比较脆弱，安全防护不高。为了提高内网的安全，内部的服务器不得不安装其他的安全系统，增加了系统的负担。如果一个系统只注重外网的入侵，而对内网的入侵没有采取什么措施，那么一个内部成员的攻击或者是失误可能造成系统的崩溃。

收稿日期：2007-02-08
作者简介：徐 斌，工程师。

由于建立一个如公司的真实环境的网络，成本太高。我们建立了一个小型网络，测试所建立的ESM的性能。

1.2.1　Web日志分析

在图1中，Web服务器日志中记录了大量有用信息，如访问日志中记录了连接到系统的IP地址、时间和被访问的文件等，在错误日志中记录诸如文件不存在的错误等。日志在实际的Web系统中有很多的用途，比较典型的是进行网站的流量统计和安全分析。我们这里利用“日志分析模型”对服务器存储Web日志和非法用户或行为数据库进行分析，检测非法入侵行为。

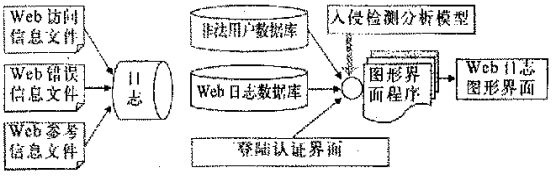

图1　Http协议日志分析模型

1.2.2　Telnet日志分析

在图2中，这个Wtmp文件有用户日志的信息。它包含用户的登陆信息和离开的信息，系统关闭和重新启动等。

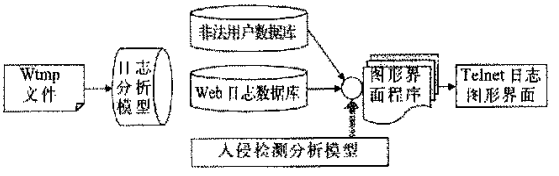

图2　Telnet日志分析模型

我们采用Web日志分析入侵检测模型和Telnet日志分析入侵检测模型以及一个切断模型，建立一个入侵检测系统，建立如图3所示的物理连接。用A系统和B系统分别模拟没有内网安全性的ESM和有内网安全性的ESM系统的安全性能。

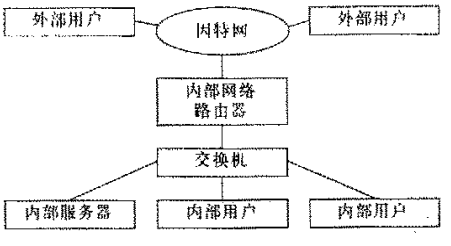

图3　入侵检测系统物理连接图

由于实验条件的限制，我们不可能用各种安全解决方案来建立我们的ESM，但我们仍就采用入侵检测系统（IDS）和防火墙这两种最常用的安全系统。

2　结果分析

我们在真实入侵环境下实验了A系统和B系统的反馈结果如下。

表1显示了在A系统下7台计算机试图通过Web服务入侵的次数和6台计算机试图通过Telnet进行连接的次数。当一个具有指定ID的用户试图访问，数据连接的数量、数据传送量以及平均数据传送量发生变化，ESM针对这些信息进行分析，一旦检测到有一个入侵，这个用户的连接就被切断。

表1　A系统测试表

Host	Web log	ID	Telnet log
210.28.168.21	183	Root	32
210.28.168.22	55	Test1	26
210.28.168.21	9	Test2	42
210.28.168.21	7	Test3	20
210.28.168.21	3	Test4	15
192.168.0.4	17	Test5	21
192.168.0.6	11		
服务器	285	服务器	156

表2显示了在B系统下7台计算机试图通过Web服务入侵的次数和6台计算机试图通过Telnet进行连接的次数。

表2　B系统测试表

Host	Web log	ID	Telnet log
210.28.168.21	253	Root	47
210.28.168.22	46	Test1	29
210.28.168.21	13	Test2	51
210.28.168.21	23	Test3	21
210.28.168.21	32	Test4	18
192.168.0.4	5	Test5	24
192.168.0.6	3		
服务器	375	服务器	190

3　结束语

本文提出了一个具有高内部安全性的ESM的结构。建立并测试了ESM，试验结果表明，网络的内部安全性确实提高了。但是，新的结构并不完善，例如，造成系统的成本上升，网络速度下降。其次对于安全系统来说更重要的是实时阻止黑客攻击和

文章编号：1005-8451(2007)09-0026-03

智能网络视频监控系统在铁路工程建设管理中的应用

王辉麟，蒋秋华，史天运，王富章
（铁道科学研究院 电子计算技术研究所，北京 100081）

摘 要：着重阐述视频监控技术的发展现状。详细介绍智能网络视频监控系统的典型组成结构和功能特点，并对其在铁路工程建设管理信息化中的应用和重要作用进行论述。

关键词：智能网络视频监控系统；铁路工程建设；管理信息系统；应用
中图分类号：U2：TP39 文献标识码：A

Application of Intelligent Network Video Monitoring System to railway engineering construction

WANG Hui-lin, JIANG Qiu-hua, SHI Tian-yun, WANG Fu-zhang
(Institute of Computing Technology, China Academy of Railway Sciences, Beijing 100081, China)

Abstract: It was elaborated the actual situations of network video monitoring technology emphatically, introduced the model and the functions and characteristics of the Intelligent Network Video Monitoring System in the railway engineering construction management in detail, in addition, the effect and trend of it in the Railway Engineering Construction Management Information System was discussed.

Key words: Intelligent Network Video Monitoring System; railway engineering construction; Management Information System; application

随着铁路的快速发展，大型铁路工程建设的现代化、科学化和信息化管理的要求越来越高。一方面，由于目前在铁路工程建设项目中（尤其是车站、桥梁和隧道等重点建设区域和施工现场），工程施工现场地点分散，现场环境复杂，成为日常施工管理和质量监控工作的主要障碍，工程建设指挥部门对施工现场的施工安全情况、施工人员的操作规范、工程施工进度的监控管理缺乏有效、直观和合理的管理手段；另一方面，施工现场重要施工材料的看管，往往力不从心，人员配置多少都是不够用的。

智能网络视频监控系统采用基于B/S结构的软件架构、基于MPEG2/4的转码流技术、以及基于帧差法和改进性高斯模型背景减法算法相结合的视频图像分析技术，实现了具有非法侵入和货物看管功能的智能视频分析和监控功能，自动对属于监控范围内的施工现场进行实时视频分析，对铁路建设施工现场安全生产的威胁提供实时侦测和报警联动，包括施工重要区域的非法闯入者；监测施工现场的安全出入口及消防路线；防止重要施工材料设备的丢失等。

工程建设管理人员在工程建设指挥部、调度中心或者其他工程建设相关部门办公室实现对全部工程施工现场和工程施工环境的监控，大大减轻日常管理人员现场巡视的工作量，便于及时发现危险隐患，保障安全生产，提高铁路工程建设的管理信息化和科学化。

收稿日期：2007-02-05
作者简介：王辉麟，助理研究员；蒋秋华，副研究员。

病毒破坏。有待于设计更合理的入侵切断方法来处理非法的流量，避免大量非法的流量阻塞网络。

参考文献：

[1] 朱 敏，朱之平. 网络入侵检测技术[J]. 计算机应用与软件，2004 (6)：95-98.
[2] 杨 苇，刘振华. 入侵检测系统的比较[J]. 计算机工程，2004 (3)：137-138.
[3] 孟晓明. 网络信息的入侵检测技术与方法研究[J]. 网络资源与建设，2004 (2)：131-133.
[4] 宿 洁，袁军鹏. 防火墙技术及其进展[J]. 计算机工程与应用，2004 (9)：147-151.