ISSN 1009-3044
Computer Knowledge and Technology 电脑知识与技术
Vol.9, No.1, January 2013.
E-mail: info@dnzs.net.cn
http://www.dnzs.net.cn
Tel:+86-551-65690963 65690964

基于网格的LINUX文件完整性校验工具的原理

赵 斐

(北京华大智宝电子系统有限公司,北京 100015)

摘要:文件完整性校验是一种基于主机的入侵检测技术,可以检测出入侵者对主机文件的非法修改。针对目前文件系统完整性校验中存在的运算复杂性问题,结合网格技术的应用背景,提出一种基于网格的文件系统完整性校验的应用模型,并对其产生的原因、特点、应用平台、工作流程进行了详细的阐述。目的是实现网格虚拟环境下提高文件完整性校验的速度。

关键词:文件系统;完整性校验;网格;入侵检测

中图分类号:TP309 文献标识码:A 文章编号:1009-3044(2013)01-0041-03

The Principle of an Integrity Checker for LUNIX Host Files Based on Grid

ZHAO Fei

(Beijing Huada Zhibao Electronic System Co., Ltd., Beijing 100015,China)

Abstract: The file system integrity verifying is one of the intrusion detection technology, being able to check the alert of files producing when it has an invader. This paper is aimed at arithmetic complexity problem at present in file system integrity verifying. In this paper, the file system's integrity verifying model is created based on grid applying. And the paper carried out a detailed exposition of its causes, characteristics, application platform, workflow. Purpose is to improve the speed of file integrity verifying under grid suppositional environment.

Key words: file system; integrity verifying; grid; intrusion detection

文件完整性是LINUX系统安全的一个重要特性。文件完整性校验是对入侵前后的系统状态进行比较,通过状态的变动来判断系统是否受到入侵。入侵发生一定为引起系统文件的改动。在确定了初始系统状态后,文件完整性校验程序定期检查当前系统状态并与初始系统状态进行比对,发现可疑或非法的修改时触发警报。文件完整性校验工具工作原理如下:在数据库中保存待检测系统文件的特征码。每次校验时重新计算每个文件的特征码并与数据库中的相应特征码进行比对,如果相同则说明文件正常;如果不同则说明文件已经被修改,触发警报并向系统管理者报告该文件的异常改动。因为校验工具无法区分被检测文件的变动是由于正常修改引起的还是由于入侵引起的,所以在正常修改了被监测文件后应当立即更新特征码数据库内的数据,从而避免校验时产生误报。

文件完整性校验的优点:发现入侵行为很重要的一个方面就是保证数据和系统的完整性。一旦入侵者成功入侵,为逃避检测和方便下次入侵,一般会通过更改系统中的相关文件来隐藏他的活动;同时做一些改动,例如植入后门程序,保证下次能够继续入侵。这两种活动都能够被文件完整性校验系统检测出。同时,文件完整性校验系统又具有相当的灵活性,可以为系统中的所有文件或某些重要文件进行单独配置。

文件完整性校验的弱点:文件完整性校验的结论依赖于本地的数据库,而这些数据是可以被入侵者修改的。当入侵者取得管理员权限后篡改文件完整性校验系统,更新数据库,那么文件完整性校验系统就会失效。同时,文件完整性校验不能实时监控,无法第一时间发现攻击行为并采取防御措施。因为文件完整性校验时需要处理的数据量非常大(如果检测全面文件的话),所有进行一次针对所有文件的文件完整性校验是一件非常耗时的工作。

而本文主要解决的问题就是如何提高文件完整性校验的速度。

1 关键技术及特点

1.1 文件完整性校验

用密码学的方法来检验文件的完整性是大多数软件的共同考虑。文件的特征码,也称校验和、数字文摘或数字签名,由文件内容通过Hash函数计算得出。不同的文件几乎不可能得到相同的Hash结果;同时Hash算法是一个单向函数,无法进行逆推。所以

收稿日期:2012-11-28
作者简介:赵斐,男,河南洛阳人,硕士学位,助理工程师,主要研究方向为入侵检测。
本栏目责任编辑:冯蕾

通过特征码进行文件完整性校验是一种非常成熟的方法。当文件一被修改,就可检测出来。因此,利用文件的特征码可方便地检测出入侵者对文件的修改。

1.2 网格技术的特点及其模型

网格是一种高性能计算平台,由分布在Internet 上的各类资源组成。网格将所有资源虚拟为一台超级计算机,在这个虚拟环境下进行资源共享和协同工作,为用户提供一体化信息和计算、存储、访问等应用服务[1]。组成网格系统的资源是动态变化的,所有资源由网格统一管理。网格能够动态监视和管理网格资源,实现任务的动态迁移,从可利用的资源中选取最佳资源服务。

Ian Foster于2001年提出了网格计算协议体系结构,将网格技术的核心定义为标准化的协议与服务,并与互联网协议进行类比(如图1)。该结构主要包括以下五个层次[2]:

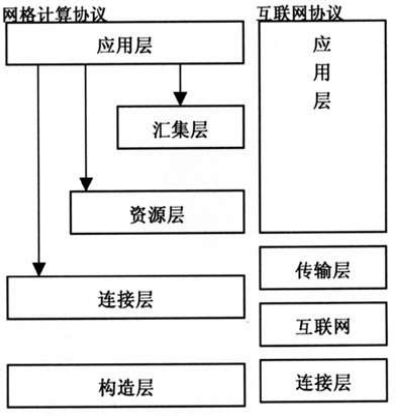

图1 网格系统五层协议结构

(1) 构造层(Fabric)

构造层的基本功能是向上提供网格中可共享的资源。常用的构造层资源包括处理能力、存储系统、网络资源、分布式文件系统、分布式计算机池、计算机集群等。构造层资源提供的功能越丰富,则可以支持的高级共享操作就越多。

(2) 连接层(Connectivity)

连接层的基本功能是实现网格共享资源间便利安全的通信。它定义了核心的安全通信、网络资源处理与认证授权控制等协议。通信协议允许在构造层资源之间通过传输、路由及名字解析等机制进行数据交换和授权认证、安全控制。

(3) 资源层(Resource)

资源层的主要功能是实现单一资源共享。资源层主要定义了资源共享间的安全握手、资源初始化、资源运行状况、统计与付费等使用数据。该层建立在连接层的安全通信和认证授权控制协议之上,通过调用构造层函数来访问和控制局部资源。

(4) 汇集层(Collective)

汇集层的主要功能是协调各种资源。该层将资源层提交的受控资源汇集在一起,供虚拟组织的应用程序共享和调用。汇聚层对来自应用的共享进行管理和控制,提供资源代理、资源监测诊断、网格启动、账户管理、协同分配管理、数据复制服务、负载管理控制、软件发现服务等多种功能。

(5) 应用层(Application)

应用层是是网格上用户的应用程序,在虚拟组织环境中存在的。应用程序通过各层的应用程序编程接口调用相应的服务,再通过服务调动网格上的资源来完成任务。应用程序的开发涉及大量的库函数,需要构建支持网格计算的大型函数库。

2 基于网格的文件完整性校验的特点

目前在文件系统校验建模方面的研究很少.Shlomo Hershkop等人曾采用PAD(Probabilistic Anomaly Detection)算法开发了基于Unix的文件系统的异常检测器FWRAP,但是他将文件系统作为一个整体进行建模,由于文件系统的数据量较大,数据的存贮和运算带来较大的系统负荷,因此它不能处理大容量的训练数据[4]。而数据的存贮和运算恰恰是网格的优势所在。

网格是一个异构、动态的计算平台,目标是实现资源共享和分布式协同工作。在网格环境中所有的组件都是虚拟的,通过定义一组核心接口来动态的调用网格中的各种资源,实现所有的服务。在进行具体服务时以底层资源组成为基础直接对虚拟组织进行资源管理。因此基于网格的文件完整性校验具有如下特点[3]:

共享性:网格将多个结点的资源集成起来,提供动态、跨结点的资源环境,解决大容量数据的存贮问题。各种资源通过网格技术有效的提供给网格中的任意合法结点。各个结点通过资源共享,完成用户提交的各种任务。

协同性:网格提供一个协同管理的环境,能够在动态组成的系统中解决大容量数据的运算问题。网格将来自不同管理域、不同管理平台、具有不同能力的结点集成在一起,成为一个有机的整体。用户不仅可以使用单个结点提供的功能,而且能够使用多个结点的聚合资源。网格资源结点根据不同的任务,动态组成不同的服务,通过彼此间合作,共同完成任务。

动态性:网格具有高度的可扩展性,支持结点的动态加入和退出。网格对这些结点进行有效管理和分配,以保证结点退出时不影响系统的正常工作,结点加入时立即被系统发现并且可用。

3 基于网格的文件完整性校验平台框架

框架模型见图2。

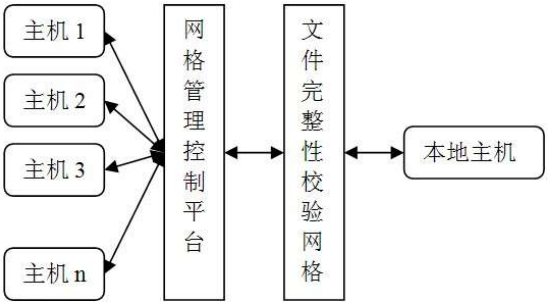

图2 基于网格的文件完整性校验平台框架

基于网格的LINUX文件完整性校验平台主要由2部分组成：

网格管理控制平台：它是基于网格的文件完整性校验平台的集中控制管理单元，通过该平台的集中统一控制，使得新建的文件完整性校验平台子系统通过统一的规范，与原有子系统实现互通、互联和互操作，在网格管理控制平台的统一协调控制下发挥出系统的最优化效用。

文件完整性校验网格：在基于网格的文件完整性校验系统下，可用的存储空间和计算能力是无限的。该网格为本地文件完整性校验系统提供透明的数据计算和存储接口，使本地主机能够容易的实现网格中的资源共享。该网格通过动态的利用整个网格中强大的计算资源，为本地主机用户提供远远强于自身的运算能力，最大限度的缩短文件完整性校验所需的时间。

4 结论

本文提出了一种基于网格技术的LINUX文件完整性校验模型,该模型通过利用网格技术强大的资源共享能力，借助不同网段不同平台主机的整合计算能力，极大的缩减单机进行文件完整性校验时所需要的时间。该模型具有以下特点：

(1) 该模型不需要源文件、大规模训练数据，通用性和易用性好；

(2) 该模型能大大缩短文件完整性校验所花费的时间，提升工作效率；

(3) 抵抗攻击的能力更强，漏报率更低。

参考文献：

[1] 徐志伟,冯百明,李伟.网格计算技术[M].北京:电子工业出版,2004,2,23.

[2] Ian Foster,Carl Kesselman.The Grid:Blueprint for a New Computing Infrastructure[M].北京:机械工业出版社，2005.

[3] Foster I,Kesselman C,Nick JM,etal.Grid Services for Distributed System Integration[J]. Computer,2002,35(6).

[4] Shlomo Hersbkop，Ryan Ferster，Linh H.Bui，Ke Wang and Salvatore J.Stolfo.“Host—based Anomaly Detection Using Wrapping File Systems”.CU Tech Report April,2004.

[5] Eleazar Eskin.Probabilistic anomaly detection over discrete records using inconsistency checks.Technical report,Columbia University Computer Science Technical Report,2002.

[6] Sufat rio , Roland H. C. Yap . Improving host based IDS with argument abstraction to prevent mimicry attacks. Proceedings of RAID 2005, Springer,Germany,2006

[7] Adam G.Pennington,etc.Storage2based Intrusion Detection: Watching storage activity for suspicious behavior,Washington DC,Proceedings of the 12th USEN IX Security Symposium,2003.