高性能计算机群的信息安全

Technical Implementation of Security Defence in HPC Cluster

中航工业信息技术中心　杨如峰　孔垂岗

杨如峰

中航工业信息技术中心（金航数码）系统集成部项目经理、数据中心工程师，致力于信息系统数据中心的规划、建设和IT基础设施体系研究工作，先后承担了中航工业大型高性能计算中心项目基础设施部分建设现场技术管理、中航直升机公司信息系统IT基础规划等工作，具有丰富的IT基础设施建设与规划经验。

目前国内外针对高性能计算机群技术的科研，主要集中在机群自身的性能和并行算法的研究上，对机群整体的安全性研究却相对较少。此外，目前我国还没有一套完整的高性能计算安全标准体系，标准的缺失带来的种种弊端日益凸显。

随着应用的不断深入以及模式多样化、并行化和系统开源化的高速发展，高性能计算机群平台更加趋于开放性和普遍性。这种模式带来便利的同时也增加了网络的风险性，越来越多的恶意攻击者将目光投向高性能计算机群系统，通过非法入侵，从中获取大量信息。因此，在建设高性能计算机群系统之初，制定一套行之有效的高性能计算机群系统安全解决方案已迫在眉睫。

现状及设计目标

1　安全现状

目前国内外针对高性能计算机群技术的科研，主要集中在机群自身的性能和并行算法的研究上，对机群整体的安全性研究却相对较少。此外，目前我国还没有一套完整的高性能计算安全标准体系。标准的缺失带来的种种弊端日益凸显。

以航空制造业常见的CFD流体计算为例，在整个流程中，安全隐患主要存在于以下环节。

（1）在数值建模前处理和后处理过程中会面临以下安全隐患：

· 提交的作业夹带病毒文件或恶意程序；

· 用户提交作业过程中，访问控制存在缺陷；

· 用户终端自身安全性无法验证，处于非健康状态接入网络；

· 作业数据以明文形式传输，可能被非法用户窃取，造成数据泄密。

（2）在计算求解或大网格生成过程中会面临以下安全隐患：

· 作业提交后，作业进程无合法性验证；

· 高级用户利用SSH漏洞获取系统高级权限，进行系统关机、程序卸载等破坏性动作。

（3）在机群系统进行并行计算过程中面临以下安全隐患：

·用户获取对全局共享目录的控制权限，其他用户的数据将面临被非授权查看、获取、篡改的风险；

·全局共享目录一旦出现故障将导致数据丢失或无法读取。

综上，设计生产过程中的安全隐患，包括以下几类。

（1）内部攻击和内部人员误操作。凭借对内部网络结构和配置的充分了解，以网络嗅探、暴力破解等手段，访问非授权资源，破坏系统。

（2）系统漏洞攻击。利用系统服务等软件设计缺陷，通过破解和注入攻击，获取更高级的权限，导致服务无法响应，甚至出现数据丢失。

（3）恶意代码攻击。通过恶意蠕虫、病毒、缓冲溢出代码和木马后门在网络中泛滥，导致网络堵塞，爆发时可能导致系统崩溃。

（4）环境破坏。大量的计算成果存储在高性能计算机群中，由于环境因素带来的损害，引起数据丢失。

2 建设目标

高性能计算机群是计算资源配置技术、存储资源配置技术和操作系统技术等多种技术的集成体。本文利用信息安全技术与基础资源关系，架设一套符合高性能计算机群系统需要的安全防线，最终要实现如下目标。

（1）系统可用：利用安全技术手段，保证系统不被恶意入侵和恶意攻击，保证系统的可用性。

（2）数据合法：对数据的保护是整个系统保护的核心。保证数据传输过程中不被非法拦截、窃取，存储数据不被非授权用户查看、篡改等。

（3）过程可控：按照最小授权原则，控制授权用户仅能在合法范围内使用，防止非授权用户使用系统，保证系统在完全可控的环境下运转。

（4）行为可查：日志审计工作是预判风险、分析风险和事后追查的重要依据，对于网络内用户所有操作行为进行日志记录，可以在事前进行处置、在事后进行追查。

（5）系统可管：在密集型计算环境下，用户类型众多，加强对用户的集中管控，能有效提高系统的可靠性和运行效率。

3 安全设计模型

高性能计算机群系统不能完全单独采用一种安全防护技术，在设计中必须充分利用 LINUX 平台开放性的特点，通过与传统的安全防护技术相融合，来提升系统的安全性。结合信息安全技术体系及基础资源关系，通过对内采用身份鉴别、认证与授权，病毒与恶意代码的防治，系统层安全防范，网络管理，监控与审计，漏洞扫描，数据传输加密与压缩，运行安全；对外采用准入控制、入侵行为检测、边界防护和运行安全等措施（如图 1 所示）为系统建设一套可靠的安全屏障。

技术实现

针对以上现状，本文提出一套行之有效的方法，来加强高性能计算机群的安全性。

1 鉴别、认证和授权技术应用

在高性能计算机群系统环境下，利用身份鉴别、认证和授权技术对高性能计算机群的用户进行统一、集中的管理，确认操作者身份，防止非授权用户使用系统或授权用户非法使用资源。

（1）基于 PKI/CA 的统一身份认证技术，取代传统的用户名认证方式，与用户作业提交子系统、接入边界子系统等进行集成，以数字证书作为用户身份鉴别的凭据，使用户在访问全过程中始终只有一个身份。

（2）利用安全认证网关等设备，将基于 B/S 访问的资源置于后台，由安全网关进行服务的双向请求，建立起安全访问通道和身份鉴别机制，减少用户对资源的攻击和非授权访问。

（3）利用 LINUX 平台自身的安全特性对访问的角色进行权限限制，配置最小访问范围和运行权限，减少对系统自身的破坏。

（4）对直接为用户提供服务的子系统提出开发要求，如必须具备身份鉴别强度、重鉴别和系统内部权限控制等功能。

2 访问控制技术应用

结合高性能计算机群平台特点，通过访问控制技术防止非授权用户使用系统和划分系统安全边界，加强系统内、外部资源双向的访问控制。

（1）利用网络隔离和控制技术，提升网络层面的安全控制。通过交换机层面端口隔离技术，控制本地端口之间的通信，减少内部安全隐患；利用端口安全技术，实现 MAC 地址绑定、802.1X 认证和广播风暴的抑制，减少网络层面的欺骗攻击。

（2）利用 LINUX 平台下 SELinux 技术，实现用户细粒度强制控制策略。用户提交的作业不立即运行，而是交由系统进行权限评估，避免用户信息在过程丢失后作业信息不被非授权用户使用。

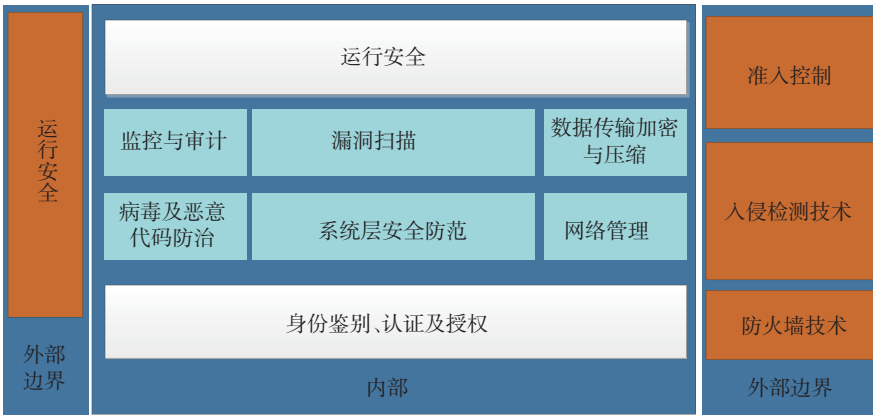

图1 高性能计算机群防护要点

（3）利用传统的防火墙技术来划分高性能计算机群平台的边界，配置基于端口级别的访问控制策略，控制用户所能访问的端口，控制高性能计算机群自身对外部资源的访问。

（4）利用网络行为的准入控制技术，对用户的准入行为进行监控和检查。

（5）对于操作过程，分析应用系统中需要处理数据的类型、格式和长度，在安全设计中进行参数检查，使程序在错误发生的最初阶段中止，防止参数的入口欺骗和溢出攻击。

3 监控和审计技术应用

监控和审计分为两方面：其一，需要监控和审计用户本地化的操作行为，其二需要监控和审计用户网络过程中的行为。高性能计算机群平台要实现前台和后台的集中审计，从目前的技术发展看，在现阶段需要多种方式结合，对过程行为进行审计定位来加强其安全性。

对于用户网络化的操作，用户数据传输过程和平台操作过程进行行为动作的审计，要借助应用平台的自身细粒度审计，并且实现不同管理员角色的相互制约，防止审计信息被非法篡改。同时通过 LINUX 本地审计功能，配置审计守护进程，添加审计规则和观察器收集所需要的数据，定期生成设计报表和搜索日志来周期性地分析数据。

4 恶意代码防护技术应用

从高性能计算平台所采用的底层平台系统看，计算软件对底层操作系统依赖性相对较高，而国内现有 LINUX 平台下主机层面的安全防护手段较少，因此，对高性能计算机群平台的恶意代码及病毒的防护需要做到以下几点。

（1）利用网络层面的病毒防治及恶意代码查杀技术，在用户提交作业传输过程中进行数据包的检查和过滤，使合法信息正常传输，对非法信息进行直接阻断并形成查杀记录，对传输过程进行唯一性基本信息记录，便于事后审计和审查。

（2）对用户本地化的病毒定期查杀，减少本地病毒对程序的感染。利用本地化的监控控制手段，禁止常见的木马及恶意程序在本地运行。

（3）由于高性能计算机群平台所接受的计算网格格式比较特殊，通过对平台可接受的文件格式及运行内容进行限制，过滤掉非合法格式文件。

（4）通过利用 LINUX 平台下 SELinux 技术及用户细粒度强制控制策略，控制病毒和恶意代码对系统核心文件的破坏，降低系统风险。

5 运行安全技术应用

高性能计算机群系统运行过程中参与人数多，系统稳定性高且设计复杂，在运行过程中需要从操作安全、系统安全、数据安全、应急处置等多角度入手。

（1）通过 LINUX 下 SElinux 技术配置细粒度的内部访问机制，控制各操作人员的操作行为，相互制约，并对操作行为进行审计记录。

（2）对于系统自身安全，通过对系统自身进行安全加固修补系统及软件漏洞，调整核心服务参数，关闭非关键服务，配置系统服务范围，配置本地防火墙策略，配置系统核心文件的访问权限，对系统文件和应用系统配置文件进行全局备份，加强系统自身的安全性。

（3）对于数据安全，既需要考虑本地数据的安全，也需要考虑传输过程中数据的安全。用户通过作业调度子系统或机群 SSH 远程访问子系统进行数据访问，要保证其安全性可以通过机群本地文件夹权限进行控制，以及通过作业调度系统进行远程目录的访问限制。同时借助于专有的文件传输系统对传输的数据进行加密和压缩处理，且在传输过程中采取加密措施，保护数据的安全性。

（4）对于数据自身的保护，一般高性能计算过程中的数据和结果数据是临时性的，结果数据也会在用户本地留有备份，针对这些数据可以执行周期性备份，但保留时间可以不用过长。对于系统数据，进行系统完整性备份，过程中进行差异的周期性备份，以保证系统在出现故障后能恢复到正确配置的可用状态。

（5）在运行维护过程中，制定好机群每个组件的应急处置预案和操作规程，可以有效减少由于疏忽、不按规程进行操作所带来的损失。

6 攻防及安全验证技术应用

高性能计算机群系统的安全防护是循序渐进的，各种网络威胁无处不在，在进行了行之有效的安全防护后也需要对防护内容进行安全验证，及时发现未知的安全隐患。

（1）利用传统的入侵检测技术对数据流异常、网络访问行为异常和网络事件异常等行为进行及时的检测，提高边界的安全性。利用漏洞扫描技术，日常性对系统安全性分析，减少由于系统漏洞引起的恶意攻击事件发生。

（2）日常运行维护工作中，跟踪机群各组件的安全状态和市场动态，制定计划，定期进行攻防试验，来验证平台的设计安全性，及时发现漏洞并弥补。

结束语

本文提出的基于高性能计算机群平台的信息安全防范方法，能够实现对平台可靠性和安全性的提升。然而由于高性能计算机群系统自身的特殊性和复杂性，部分安全性问题目前仍没有得到很好的解决。因此，未来加大对 Linux 平台下安全技术和高性能计算机群平台特性的研究，将是推动高性能计算机群系统安全技术的有力保障；同时，随着国产化的推动，针对这两方面的研究，必将为高性能计算平台安全防护增添新动力。 （责编 谷雨）