论信息系统的安全性设计

摘要：

2011 年我有幸参加了某单位遥感卫星测控系统项目的研制，我在系统中担任软件分系统负责人，主要负责软件开发的管理工作、软件需求分析，软件设计方面的工作。遥感卫星测控系统主要完成对遥感成像卫星的遥测，遥控和数传任务，软件分系统作为整个系统的分系统之一，主要完成系统硬件设备工作参数设置，系统运行状态监视和遥感图像数据的管理功能。由于卫星测控系统的操作牵涉到卫星资源的控制和遥感影像产品的管理，系统的安全性设计变得十分重要。在项目的需求分析阶段，项目组对系统的安全性进行了分析，得出的结论是系统可能存在物理安全隐患，网络通信安全隐患，和系统安全隐患，在项目的设计阶段项目组针对系统安全风险分析报告中提到的系统安全隐患做了相应的设计方案。主要采用异地备份来解决可能发生的自然灾害对系统造成的不可恢复的损坏。采用防火墙技术和入侵检测系统对网络访问加以控制，采用非对称加密技术和数字签名技术保证重要数据的安全性和可靠性。本文对系统的安全性设计进行了详细介绍，最后总结了系统运行的效果和不足之处，以及针对不知之处采取的补救措施。

正文：

2011 年我参加了某单位遥感卫星测控系统项目的开发工作，我在系统任命中担任软件分系统负责人，主要负责软件开发小组的管理和对系统进行软件需求分析和设计。遥感卫星测控系统由发射分系统，接收分系统，测试标校分系统，天伺馈分系统和软件分系统组成，系统的五个分系统各施其职，协调工作，完成对遥感卫星的跟踪，遥测，遥控和数传任务。软件分系统在系统中扮演指挥者的角色，主要负责对系统工作状态的监视，工作参数的设置，执行卫星跟踪任务计划和管理遥感影像数据。软件系统也是整个系统的人机接口，工作人员在执行任务时对设备的大部分操作都要通过软件分系统完成，系统对防误操作方面的要求比较高，软件分系统承担了卫星遥控计划的执行和卫星遥感数据的管理，因此，系统对安全保密性要求比较高。 软件分系统采用 C/A/S 三层体系结构，数据库服务器主要完成对系统的任务计划，遥感数据和系统日志信息进行存储管理；业务服务器主要完成系统的业务处理，主要包括与上级指挥中心的网络通信功能，与其他硬件分系统的嵌入式软件之间的串口通信功能，对系统工作参数的设置和工作状态的监视功能，执行上级指挥中心下发的任务计划，对遥感影像数据进行管理等功能。系统包括多个客户端软件，主要完成人机接口功能。系统的数据库服务器，业务服务器，多个嵌入式监控软件和部分客户端处于同一个局域网内，部分客户端部署在指挥中心，通过光纤网络与业务服务器通信。系统与指挥中心的网络接口是系统与外界的唯一一个外部接口。 项目组在分析了系统的网络结构和组成后，我们发现系统在物理方面，网络通信方面，系统安全性方面都存在安全隐患。物理方面，由于系统由多个服务器和大量磁盘阵列组成，系统保存了大量的中药数据，尽管系统本地也采取的备份措施，但是如果发生火灾，洪灾，地震等不可抗击的自然灾害，将可能永久性损坏系统服务器和存储设备，导致大量的宝贵数据丢失；在网络传输方面系统对外有一个网络接口与指挥中心进行通信，这个非法访问者提供了机会，可能存在外部的非法入侵行为。在网络上传输的数据会被非法获取，导致重要信息的泄密，或者外部非法入侵者冒出指挥中心给系统发送错误的任务计划，导致系统执行错误的遥控指令，这将会导致严重的后果。在系统内部，应用服务器和其他硬件设备的嵌入式软件通过串口传输控制命令和设备状态，有少部分设备由于设备

位置离系统机房比较远，并且要经常移动位置，所以不得不采用无线通信的方式，这也给非法入侵者提供了机会。可能通过截获无线信号获取设备控制命令，或者伪造设备命令导致设置执行错误的指令。所以网络通信将是系统实施安全防护的重点部分。在系统访问控制方面，系统的服务器采用 windows server2008 操作系统，客户端采用 windows xp 操作系统，虽然操作系统提供了比较安全的用户身份认证和访问控制权限控制，基本上满足了系统安全性要求，但是也有可能因为系统的漏洞或者系统感染病毒或木马程序导致非法入侵者可以访问系统资源。在应用系统层面，主要存在工作人员误操作的隐患。 经过需求阶段的系统安全分析，项目组得出了系统安全风险报告，项目组根据报告中提到的问题进行了系统安全性方案设计，物理方面的安全问题主要是自然灾害导致的，并且一旦发生也是不可抗拒的，我们采取将系统重要数据定时进行异地备份，在指挥中心建立一个重要数据备份库。予解决系统物理方面的安全问题。 在网络通信方面，我们采取了两方面的解决措施，一方面是在系统外网入口处安装应用防火墙，控制外部用户对系统内的资源访问，通过设置访问 ip 端口号限制，已经通信服务方面的限制，阻止非法用户通过网络进入系统，同时安装入侵检测系统，达到及时发现网络访问异常告警的目的，根据入侵检测系统报告的网络情况，及时修改防火墙设置。另一方面是对系统与中心传输的数据进行加密和合法性验证，主要采用了非对称加密技术 RSA 和数字签名技术。有效防止数据被窃取，也保证了数据源的合法性，同时也防止双方的抵赖性。对于系统内部的无线传输，我们采用具有加密功能的无线数传模块，发送方在发送数据之前进行数据加密，接收方接收到数据后先进行解密即可得到正确的命令。防止了无线通信可能造成的数据泄密。 在操作系统级，我们关闭了很多没用的网络通信服务，设置了用户访问权限、策略。对用户的访问权限进行控制，同时安装杀毒软件定期进行病毒扫描，防止系统被病毒感染或者木马程序入侵。及时安装系统补丁，定期更新病毒库。定期更新用户密码。对重要的数据采用加密软件进行加密存储。在应用软件方面，我们主要采取用户身份认真和访问权限控制，将用户等级分为管理员，操作用户和监视用户；管理员可以创建用户和执行一切操作，操作用户可以控制设备，执行任务计划，监视用户只能对系统工作状态进行监视。这样可以防止卫星测控系统软件被不相干人员随意操作。 系统经过一年多的运行，目前运行稳定，没有发现非法访问和泄密事件发生，说明我们的系统安全性设计方案是成功的，但是在系统运行中也发现一些考虑不周全的地方，用户可以通过 PE 光盘启动系统，绕过已经安装的操作系统直接访问系统硬盘，这相当于操作系统设置的用户名和密码，用户访问权限没有用了。我们发现这个问题后，封闭了所有设备的光驱和 USB 接口，并加强了安全管理方面的工作，对系统机房实行二十四小时监控，防止非法人员接近系统主机，经过这个项目，我们总结出信息系统的安全工作必须从技术上和安全管理制度以及工作人员的思想上全面考虑。单从技术上无法保证系统绝对的安全性，系统安全任重道远，我们时刻准备对系统不足之处进行改进。