论计算机网络的安全与监控

摘要

文章首先分析了本单位的网络安全现状，指出了存在的问题，接着结合各应用系统的安全需求提出了建立网络安全系统的几项措施：一．变平面网络结构为层次网络结构，实现网络的纵深防御；二．建立统一的访问认证系统，采用分级授权和基于角色的授权相结合的机制，能够快速完成对所有用户的授权工作，强化网络安全；三．建立各应用系统的安全边际保护措施，对于核心系统通过划分安全边际，加强接口的监控来完善保护措施；四．实现内外网的动态隔离，不仅可以实现信息资源的共享，也能够保证企业核心系统的安全；五．建立防病毒网关，防止病毒的攻击。另外，文章还介绍了如何防范用户私自接入互联网的技术措施，最后指出做好网络安全工作，应该做到管理和技术相结合。

正文

我单位是一家大型的铁路局，管辖着三省一市的铁路运营工作，经过多年的建设信息系统生产、安全、管理、办公、财务、人事等各个领域，成为企业不可或缺的重要平台。

随着信息化的发展，铁路的信息系统必须由服务内部转向社会公众开放，为旅客和货主提供信息查询和车皮计划申报等网上服务。那么如何在开放的环境下保证现有各系统的安全运行，就成为一个不能回避的首要问题。另外由于原先我们的网络安全防范功能也仅限于用户名和口令等简单的措施，为此建设一个完善的网络安全系统，提高整个网络的安全性和可靠性，成为我局信息化建设的必然选择。

我们铁路局的企业网是个庞大的广域网系统，它连接着铁道部、铁路局、站段和车站四级单位，在网络上运行着列车调度指挥系统、车站现车管理系统、客票系统、货票系统、办公系统等几十个应用系统。目前的联网点有近万个，要确保这个庞大系统的安全，必须在统一规划分布实施的原则下进行。

2008 年 4 月至 12 月，我们进行了网络安全系统的建设工作，我作为项目经理负责项目的规划和实施，下面详细介绍网络安全系统的经过和措施。

1．变平面网络结构为层次网络结构，实现网络的纵深防御。

以前我们的网络是平面结构的，即办公网和生产网是互连互通的，通过办公网可以随意访问生产网，这样的网络结构容易造成一点突破全局失防的结果，因为以前企业网和互连网是物理隔离的，所以这种结构的弊端还不明显，但是如果和互连网连接后，这样的结构是显然不能满足安全要求的。

为此，我们进行了网络的层次划分，将企业的网络划分为三层：外部网、办公网、生产网。在外部网和生产网之间建立缓冲接待区，外网用户不能直接访问办公网的信息，必须通过接待区进行地址的代理转换。另外，在办公网和生产网之间安装防火墙，对未授权的办公网用户进行隔离。

这样的立体防御体系的最大好处就是解决了网络的分层保护问题，变单层防护为多级防御，提高了网络的安全及。

2．建立统一的访问认证系统。

由于企业网内部用户众多，要进行有效的管理，就必须建立统一的认证系统，通过认证来进行用户的身份识别和访问权限控制。因每个用户可能要访问不同的应用系统，为减少用户重复登陆，我们使用了单点登陆技术，用户一次登陆后，即可获得授权 TICKET，然后各应用系统根据 TICKET 来确定是否允许访问。

由于企业内部用户有近 8 万人，每个人的权限都可能不一样，要给每个用户授权工作量巨大，为此在认证服务器上我们实行分级管理和基于角色授权相结合的机制，首先由局信息中心对二级单位的网络管理员进行授权，然后二级单位的网络管理员再对本单位的员工进行角色授权。这里的角色是指对各应用系统访问权限的组合。例如：售票员角色的权限只能进入售票系统，站长角色的权限则可进入办公、货运、客运等各个系统。基于分级的角色授权机制极大地减轻了我们的工作量。

3．建立各应用系统的安全边际保护措施。

虽然设计了网络的分层保护，但各应用系统间也必须采取相应的保护措施。例如列车调度系统是一个需要保证绝对安全的应用系统，因为它关系到列车的运行安全，如果出现差错的话就可能造成运输秩序的混乱，引起列车的大面积晚点；客票系统也是面向旅客的，车站

不能售票，将会给旅客的程降组织工作带来严重的影响，它的安全性也非常重要。

因此，对这些核心的生产系统，必须强化安全防范措施。我们的防范策略是首先划分清楚网络的安全便界，保证每个系统只有一个接口对外进行信息交换，然后再根据每个系统的不同特点对网络接口采取相应的技术措施。例如对于列车调度系统，我们规定信息只能向外读（用于查询列车时刻），外界的信息不能向内写，同时还规定了数据只能按照规定的径路流动，另外还进行流量的监控，一旦出现异常就可发出警报。通过采取多种措施，可以说极大地提高了核心系统的安全性。

4. 实现内外网的动态隔离。

在社会的信息化程度越来越高的情况下，实现企业网和互连网的连通是必然的趋势。虽然物理隔离能提高系统的安全性，但是也极大地阻碍了信息资源的充分利用，向社会提供运输信息也是铁路企业应有的职责。

要实现企业网和互联网的互通，必须有一个安全可靠的技术防案来保证，否则管理者很难作出这样的决策，因为一旦影响生产系统的运行，带来的结果将是灾难性的。

在实现和互联网的连接中我们采取的是动态隔离的措施。首先是建立一个网络访问接待区，互联网的用户只能到达接待区，其访问请求均由接待区进行代理和转换后，再访问办公网，同时还规定互联网用户的数据访问路径，即只能访问办公网，不能访问生产网，同时对接待区也进行流量监控。企业网用户要访问互联网也必须通过接待区完成权限检查和地址转换。

目前，通过接待区用户可以查询列车的票额信息和运行时刻以及货运计划信息，同时授权用户还可以通过互联网提报车皮计划，网上订票系统也在建设中，应该说只能是在一定程度上，为旅客和货主提供了方便。

5. 建立防病毒网关，防止病毒的攻击。

病毒和木马层出不穷，对信息系统的安全构成了了极大威胁，病毒的防范也成为信息安全的一个重要内容。

我们的防病毒措施就是建立防病毒的网关来实现对病毒的查杀。具体的做法就是在企业网和互联网的连接处建立防病毒网关，在重要的应用系统的出口也加装防病毒网关，对流入的数据进行分析和监控，及时查杀病毒。

通过以上措施，可以说我们初步建立了企业网络的安全防护体系，使企业网的安全性得到了极大的提高，尤其是这些措施整体使用，其安全防护效果更加明显。

当然，网络安全系统建立后，也不就是万事无忧了，例如在对信息系统的运行检查中我们发现有的用户私自开通互联网，通过 ADSL 上网，这样就使我们企业网有多个出口，也使我们采取的技术防范措施毫无作用，是个极大安全隐患。为此我们在路局统一部署了桌面安全系统，收集用户数据流中的 IP 地址情况，发现非法 IP 地址时及时报警，这样我们就很容易发现问题，及时采取措施果断处理。

应该说网络安全不仅仅靠技术防范，更需要加强安全管理，只有两者相辅相成，才能保证网络更加安全可靠。