电子政务安全与主机系统设计

Electron Government Affair Security and Host System Project

高峰 （临安浙江林学院现代教育技术中心 311300） 卢尚琼 （临安浙江林学院图书馆 311300）

摘要：本文首先讨论电子政务系统的安全隐患及其特点，在此基础上提出了一种基于安全考虑的主机系统方案。实践表明，本文作者为某市所设计的电子政务主机系统方案具有比较好的安全性能：一方面，它能够有效地抵御来自网络外部的攻击行为；另一方面，它能够有效地防止来自网络内部的攻击行为。

关键词：电子政务　安全漏洞　外部攻击　内部威胁　主机系统

1 电子政务的安全漏洞及其特点

电子政务是依赖于计算机和网络技术而存在的，这就意味着电子政务应用不可避免地存在着由Internet的自由、开放所带来的信息安全漏洞。电子政务的信息安全涉及技术的安全和管理的安全，这些信息安全漏洞主要表现在以下几个方面[2] [3] [4]：

1.1 身份认证

由于非法用户可以伪造、假冒政府网站、社会团体、企业和个人身份，因此登录到网上政务站点的政府内部人员、社会团体、企业、个人无法知道他们所登录的网站是否是可信的政府网站，政府网站也无法验证登录到网站上的客户是否是经过政府部门认证的合法用户，非法用户可以借机进行破坏。"用户名＋口令"的传统认证方式安全性较弱，用户口令易被窃取而导致损失。

1.2 信息的机密性

传输在各政府部门间、政府与企业间、外出的领导与办公室之间的敏感、机密信息和数据有可能在传输过程中被非法用户截取。

1.3 信息的完整性

敏感、机密信息和数据在传输过程中有可能被恶意篡改。

1.4 信息的不可抵赖性

网上行为一旦被否认，政府部门、机构或个人没有已签名的记录可作为仲裁的依据。

电子政务系统的安全漏洞具有自身显著的特点：

(1) 电子政务最终目标是建设政府办公自动化、面向决策支持、面向公众服务的综合平台。因此电子政务系统一方面要求考虑政府内部网络的安全，另一方面要求考虑面向公众服务的网络安全。

(2) 电子政务行使政府职能的特点导致来自外部或内部的各种攻击，包括黑客组织、犯罪集团或信息战期间信息对抗等国家行为的攻击。攻击包括基于侦听、截获、窃取、破译、业务流量分析、电磁信息提取等技术的被动攻击和基于修改、伪造、破坏、冒充、病毒扩散等技术的主动攻击。

(3) 信息网络的可腐败性是电子政务必须考虑的另一问题。信息系统要求有相应的安全环

的要求都较为严格。Windows 2000 Server配合IIS和ASP.NET环境所提供的这一PC机上的低成本解决方案可基本满足这些要求。此原型系统完成后，还要经过广泛的测试和修改，才能逐步进入实用阶段。

参考文献

1 秦鑫等.NET框架数据访问结构，计算机系统应用 [J]，2002年第12期。

2 Chris Payne，ASP.NET从入门到精通，人民邮电出版社，2002。

3 蔡连成等，专家系统基础与实现，天津大学出版社，1990。

4 李志伟，基于Web的飞机故障远程诊断专家系统的设计，计算机应用与软件 [J]，2002年第12期。

境。目前，大部分电子政务选用的系统本身存在着安全弱点或隐患. 网络硬件系统的弱点和漏洞将危害网络的可靠性和可用性; 网络软件系统的弱点和漏洞则可能构成系统隐患。

(4) 网络威胁包括来自内部与外部的威胁、主动攻击与被动攻击带来的威胁。网络威胁的隐蔽性、边界模糊性、突发性以及易被忽视等特点要求我们引起高度重视。据统计：11%的安全问题导致网络数据破坏，14%的安全问题导致数据失密。

(5) 由于电子政务的特殊性环境，安全性的破坏来自于内、外两方，要防止外部的破坏，更要防止内部的安全问题。从恶意攻击的特点来看，FBI统计的结果是65%的攻击来自网络系统内部，如来自内部的非法窃取或非授权访问。实际上，对信息安全保障的威胁，从来就来自"内"、"外"两个方面，而且外因通过内因起作用，堡垒最容易从内部攻破；随着内部人员威胁的加剧，内部人员犯罪已经体现出了"危害大、难抵御、难发现"的特点。

2 电子政务系统的安全性架构设计

电子政务提供科学决策、监管控制、大众服务的功能，信息安全是其成功的保证。电子政务安全建设要求保护网络中信息存放、传输的安全，提高网络防护、检测、响应恢复和对抗攻击的能力，保证网络的保密性、鉴别性、完整性、可用性和可控性。其核心是保证系统数据的安全和系统的可用性，网络安全是基础环节。在安全设计时，要求技术、管理、法制、教育并举，有机综合多种安全技术，构建整体安全保障体系。

解决好信息共享与保密性、完整性的关系、开放性与保护隐私的关系、互联性与局部隔离的关系，是实现"安全的"电子政务的前提。因此，在建设电子政务系统平台时以下几个方面的问题必须慎重考虑：

2.1 网络安全结构规划

对电子政务系统按照不同安全级别划分安全域。内部网络进行虚拟子网络隔离，边界接入网络分别采用物理隔离或隔离技术实现。

2.2 网络实体安全建设

包括电子政务关键主机物理安全保障和机房安全建设，安全物理保证和信息存储介质安全保证等内容，保证网络实体运行环境的安全。这里涉及到两个方面：网络操作平台的安全建设和网络安全防护措施。

2.3 建立安全管理体系

由于网络新漏洞的出现与新威胁的增长，必须通过网络安全管理实现系统审计信息的综合分析，不断在运行中调整安全策略、完善安全设计，使安全策略更符合实际（如网络防护安全规则、入侵检测规则）、安全设计更趋合理。另一方面，要求建立各项应急响应措施与应急制度，提高系统抗攻击或抗灾难响应能力，通过网络安全管理体系的建设，保障网络安全体系的动态性和自适应性。

基于上述电子政务系统的安全和服务特点，我们在设计某市电子政务系统的主机系统时主要考虑以下三个方面的问题（如图1）：

2.3.1 高可用性设计

电子政务系统的可靠性主要由两种途径来保证：(1) 主干链路扩展为两条，平时使用Ether Channel技术可以利用多条链路的带宽，当一条链路发生物理故障时，另外一条链路可以作为主干链路的备份; (2) 为网络控制中心的设备提供尽可能多的备品备件，以便在发生由硬件引起的故障时可以尽快的恢复网络运行。

2.3.2 扩展性设计

在设计电子政务系统时，我们选择模块化的网络设备，这样网络的扩充和升级都非常容易：

在网络扩充或升级时，只需要添加或更换模块便可以完成; 而设备也可以通过软件或硬件升级，以便于支持未来的新的网络标准。这样可以保证网络设备的最高效率的运行。

2.3.3 安全性设计

对信息安全产生威胁的原因归纳起来有两点：一是外部原因，如黑客的侵袭；另一个是内部原因，这是最主要也是最危险的攻击行为。

在进行电子政务系统的安全性设计时，我们主要考虑三个方面：

(1) 与Internet互联的安全性

在本方案设计中，把与INTERNET相连的服

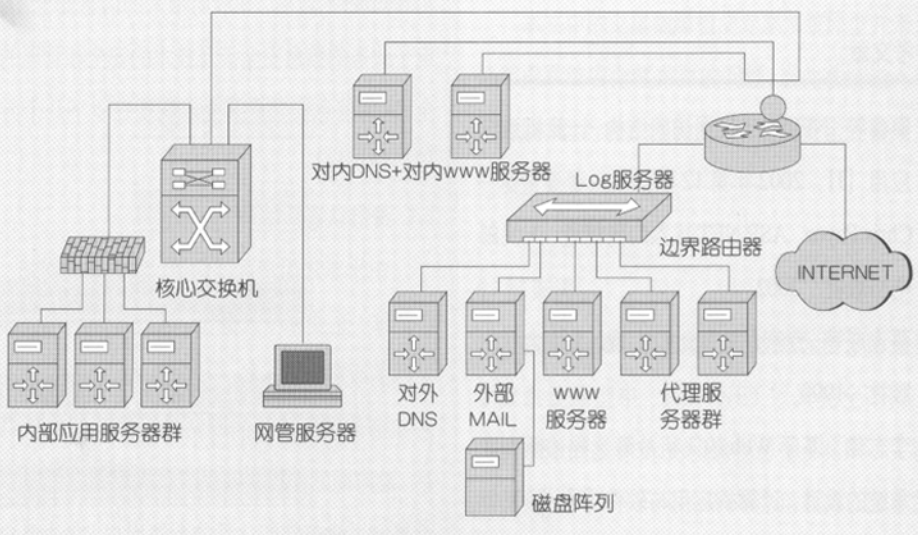

图1 电子政务系统的主机系统示意图

务器的安全性集中在服务器自身以及路由器的安全功能上。

作为面向INTERNET的服务器，其安全隐患在于服务器提供的各项服务本身具有的BUG，黑客往往利用某项服务的漏洞进入服务器或者从事其他危害。所以在我们的设计中，采用如下策略：① 服务器采用UNIX操作系统，该操作系统的BUG比起源码保密的WINDOWS操作系统和开发维护组织松散的LINUX少很多；② 每台服务器只开启一项服务。由于每台服务器开启尽可能少的端口，这就大大减少了系统的安全隐患；③ 使用高性能的线性路由器，使得我们既可以在路由器上实施较为复杂的安全策略，同时又不影响INTERNET的接入速度。

(2) 电子政务系统自身的安全性

根据IDC的统计报告，信息网络所受到的攻击有70%来自于网络内部，因此我们设计电子政务系统的安全性，主要为了防止系统内部人员的非法操作或者不合理操作，保证系统的安全可靠性。

在整个网络架构上，首先，我们将公共服务区单独划分出来，使其受到路由器的路由策略的保护，所有的内部访问数据全部都在A点被过滤拦截，从根本上保证公网服务器群不会受到来自内部网的攻击。其次，利用交换机内置的软硬件功能对局域网内所有访问进行验证，不但包括管理和配置交换机的访问，还包括通过交换机访问网络体系架构的所有内容。最后，我们在主机系统的操作系统级别进行设置，可以提供基于每个用户的身份验证、授权、加密等，也可以提供基于应用的存取权限过滤。

(3) 防火墙设计

作为一般性安全性架构设计，将网络分成三个部分，即：在边界路由器后放置一台防火墙，通过防火墙将网络分成外部网络、内部网络和DMZ（停火区），见图2。把服务器放在DMZ区，并通过相关的安全性设置，以便内部、外部用户都能访问服务器，又能对服务器进行安全性保护。

但这种设计对电子政务系统不是很合适，主要缺陷是：对网络管理来说，复杂的内部用户所带来的安全性问题并没有解决。由于网络内部用户数多、较分散及用户网络行为差异等特点，一般我们还应通过3层交换机划分成不同的VLAN进行分类和联通及控制，比如将用户分成部门内可访问、国内外都可访问权限等，使用户的网络行为相对可控，提高可管理性。这时，在路由器或者3层交换机上将产生大量的包交换过程，从而成为电子政务系统信息流通的瓶颈。

为了克服上述缺陷，我们设计的防火墙构架如图3所示。采用该防火墙构架的主要优点是：

① 采用4层交换路由器来完成边界路由和安全性检查、限制功能；据此，将电子政务网络的内、外隔离。② 在电子政务网络内部，通过3层交换机与边界路由器之间建立1个公共网段，电子政务系统内部的其他网段的用户只能通过位于公共网段的服务器，间接地访问外部网络，而外部网络的信息只能受限制地到达公共网段（如图1所示）。其好处是投资相对减少，信息流通的瓶颈相对消除，安全性却大大提高。③ 不管如何设置防火规则，内外的进出完全隔离应该是最高等级了。④ 由于公共网段的相对自由化，可引入多种的出口带宽资源，使出口的配制相对自由，可以实现按需配制不同的出口资源，有可能促使低费用出口带宽运行方式的实现。

4 结束语

实践表明：我们所设计的主机系统方案具有比较好的安全性能：一方面，它能够有效地抵御来自网络外部的攻击行为；另一方面，它能够有效地防止来自网络内部的攻击行为。

当然由于网络新漏洞的出现与新威胁的增长，要保证电子政务的永久绝对安全是不太现实的。这就要求网络系统管理人员在技术上必须主动适应网络动态变化，建立自适应的安全保障体系。

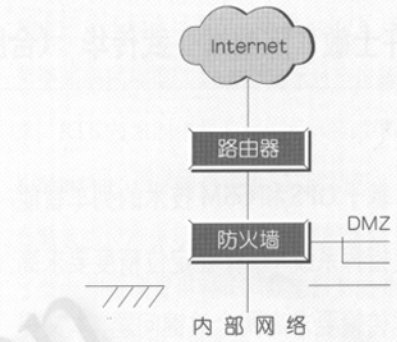

图2 防火墙的一般模式

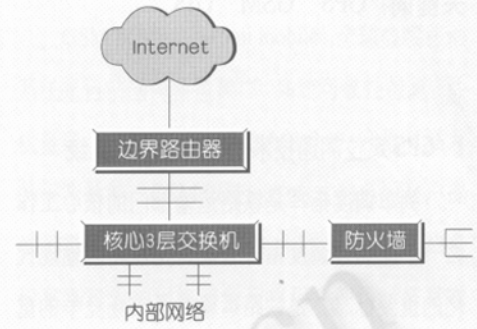

图3 改进的防火墙构架

参考文献

1 北京启明星辰信息技术有限公司，网络信息安全技术基础[M]，电子工业出版社，2002。
2 唐勇、胡华平、陈海涛、等，基于代理的网络入侵检测系统的研制[J]，计算机工程与科学，2002，24(1):9-13。
3 苗青、宣蕾、苏金树，网络安全战略预警系统的攻击检测技术研究[J]，计算机工程与科学，2002，24(1):14-17。
4 闵君、龚晶莹，入侵检测技术的研究[J]，2002，计算机应用研究，19(2):1-4。