Xx 项目安全保密解决方案

第一章 网络安全结构分析和设计

1.1 网络情况概述和安全状况

本章我们将从内部网的网络拓扑以及网络内部包含的资产进行描述和分析
，

并了解目前内部涉密网络的安全保密现状。

1.1.1 内部网络拓扑结构

单位内部网络拓扑结构从密级和区域,应用三个因素上可以分为绝密隔离内

网区域,机密内网区域和310
专网三个区域,以下为三个区域的网络结构介绍.

绝密隔离内网(物理隔离,独立与其他网络)

绝密网

物理隔离

绝密隔离内网

单位绝密隔离内网应用主要是涉及绝密信息的数据处理,为单独一个隔离的

内部环境,区域内部所有的计算机均不联网,同时各台涉及绝密信息的计算机均

有人员独立操作物理空间,能够有效防止人为窥探行为.区域机房有效实现了电

磁辐射屏蔽和物理安全措施.

机密内网(包含机密和秘密级应用,最高密级为机密)

机密级内网网络拓扑结构

正在建设拟定建设的单位骨干网络内部采用千兆以太网结构,通过骨干交换

设备的 VLAN
划分,将不同应用和职能的部门划分为逻辑子网形式,除分布在北京

的计算所,55
所和技术局子网通过光纤远程与单位骨干网络连接外,其它子网均

与骨干网络在一个物理可控区域范围内各个部门子网内部均有机密级数据应用,

客户端通过端到端加密卡访问这些服务器.

单位网络中的动向情报子网中的动向库系统要求密级很高,但在业务上必须

和 310
专网互联,完成数据传输,但鉴于安全保密措施尚未解决,故没有进行实际

网络连接.

专网连接区域

310 专网连接区域

310 专网目前是一个单独的网络,结果比较简单,主要是通过路由设备与 310

网连接,然后提供一些发布的mail,web,dns 服务器.

从业务上讲,310
专网连接区域与机密内网中的动向子网是存在业务数据交

互的,目前的手段是工作人员使用软盘等设备进行数据交换传输,很难满足用户

的业务需求,在将来的安全规划设计后,将动向子网和 310
专网进行有效结合是

一个解决业务苦难的办法.

1.1.2 网络安全基本情况

目前的网络正在建设中，安全只考虑了机密级内网用户和机密服务器之间的

通信加密连接。

网络攻击

主要体现在机密内网,各个子网间目前没有做网络层安全防范和监控工作。

病毒防治

体现在机密内网和绝密内网的两个目前没有考虑应用层的病毒防范工作

应用需求:行为、身份不可抵赖等

机密级内网用户访问机密级数据库应用仅依靠 IC 卡加密连接无法判断身

份，无法做到抗抵赖和身份认证。

加密传输

机密骨干网络中有几个子网不在骨干网络所处物理可控区域中,其中的计算

所子网,55
所子网,技术局子网分布在外地,通过光纤与骨干网络连接,存在数据

泄密的隐患.

1.2 网络脆弱和风险性分析

单位内部网络是涉密网络，根据以上要求我们从以下几个方面对网络资产风

险性分析。

物理层安全脆弱性: 物理设备的脆弱性分析

物理设备和线路的泄漏分析

环境因素的脆弱性分析

网络层安全脆弱性:网络资源的访问控制脆弱性分析

可能存在的入侵脆弱性分析

政务可能存在攻击分析

非法访问分析

假冒攻击

网络设备安全隐患分析

系统层安全脆弱性:操作系统本身的脆弱性分析

对操作系统本身的安全配置脆弱性分析

桌面安全的脆弱性分析

应用层安全脆弱性:应用系统自身脆弱性分析

抵赖性分析

取证分析

应用系统的认证分析

应用系统的审计分析

管理层安全脆弱性:操作失误

人为故意攻击

人员安全意识薄弱

有待增强的安全管理意识

1.2.1 物理层脆弱和风险性分析

电磁泄漏

内网几个区域的电磁泄漏问题可以从以下几个角度上考虑(环境电磁泄漏,

设备电磁泄漏和线路电磁泄漏)

环境电磁泄漏:从拓扑结构图上可以看出，某单位内部网所处物理环境为

内部可控安全区域，环境电磁泄漏的威胁系数较低。

设备电磁泄漏:各个区域(服务器和工作机房内)都还没有配备抗设备电

磁泄漏的设备,解决不了设备诸如服务器，主机产生的电磁泄密问题。

1.2.2 网络层脆弱和风险性分析

非法访问

内网使用的数据库的日常用户安全意识如果不强，口令设置缺乏科学性，

易猜测，且更换频率低，个别人甚至半年更换一次。这位非法用户盗取数据库资

源提供了可能，并且在内部局域网络中这种经常会出现的口令探测也同样缺乏有

效的技术监管。

部分 UNIX 或 Windows NT/2000
的命令可以实时检测网络数据包的传输情

况，对于 telnet ,rlogin
这些不加密的网络应用，用户登陆口令很容易被发现

和窃取。

主机操作系统漏洞和错误的系统设置也能导致非法访问的出现。

假冒攻击

在系统的内部局域网内，居心叵测的攻击者可以将自己的 ip
地址改为他人

的地址发起攻击，这种做法往往会让管理人员转移调查目标，难以发现真正发起

攻击的人。

攻击者也可将自己的网卡换掉，修改mac 地址和ip
地址向服务器发起攻击，

攻击完后再回到以前的设置，这些问题是目前中心的安全手段所解决不了的。

互连设备的安全隐患

内网使用的交换和路由设备都支持 SNMP
简单网管协议，这些设备都维护

着一个有着设备运行状态，接口等信息的 MIBS 库，运行着 SNMP
的主机或设

备可以称为 SNMP AGENT.SNMP
管理端和代理端的通信验证问题仅仅取决于

两个Community 值，一个是Read Only(RO)值，另一个是Read /Write (RW) 值，

拥有 RO 值的管理端可以查看设备的一些信息包括名称，接口，ip 地址等;拥

有RW值的管理端则可以完全管理该设备。令人担忧的是大多支持snmp 的互连

设备都是处于运行模式，至少有一个RO
的默认值为PUBLIC，会泄漏很多信息。

拥有RW默认值的设备在互联网上也是很多。加之SNMPV2
版本本身的安全验

证能力很低，所以极易收到攻击，从而导致互连设备的瘫痪和流量不正常，如果

没有冗余设备，那样整个内部网络就会瘫痪。

互连设备的弱管理口令，IOS
版本太低也会使交换设备受到入侵和拒绝服

务攻击，导致不能正常工作，影响信息中心的工作。

安全旁路的隐患

绝密级区域和机密机区域内网均是与其他区域物理隔离，而且绝密级区域

的计算机均不联网，但依然存在安全旁路问题，随着技术的发展，安全旁路已经

不局限与使用电话线拨号上网，而是指通过其他的数据通信设备比如 usb 存储

器，红外线口，网卡(笔记本用户)等设备进行数据泄密，这个就算计算机不联

网也是无法解决的问题。

安全旁路问题已经成为涉密单位比较严重的泄密隐患。

访问失控隐患(专网区域和机密级网络区域)

主要集中在机密级数据内网，集中机密级数据应用的内网服务器均配备的

加密卡，需要访问这些服务器的用户配备加密卡和 IC 卡与服务器建立加密连接

才可以访问服务器，但普通用户还是可以通过网络底层协议访问这些服务器和访

问机密服务器的客户机，网络窃取数据还是存在很大的可能性，缺乏必要的网络

层访问控制手段。

广域专网的一个区域也存在这个问题，广域专网用户通过拨号等手段与专

网区域的一台计算机交互数据，但网络连通后确没有访问控制手段，这台数据交

换计算机连接的专网内部网络中有一台重要的服务器，一旦存在攻击行为将数据

交换机器作为跳板，窃取重要服务器就简单化了。

1.2.3 系统层脆弱和风险性分析

操作系统 这些系统是数据库的主要运行平台。这些系统均达到C2 级

的安全标准，设置有严格的用户权限，防止数据被非法删改、查询和拷贝
.

系统仅具有D1 级的安全性，文件一旦在局域网上共享，根据系

统管理员日常考察，普通用户设置访问口令的情形不多，并常常是面向所有

用户共享。

系统和Unix 系统由于广泛的应用，存在的安全性问题比较多，几乎

每隔一段时间就有关于 windows 和 Unix
的漏洞信息发布在互联网上如针对

sun 系统的漏洞供给代码站点http://lsd-
pl.net;众多的攻击信息会使内网

的服务器面临很大的危险

桌面安全的脆弱性分析

各区域采用的工作平台是windows2000，但windows2000
的桌面安全则令人

担忧，传统的用户名和密码的验证方式已经经不起密码字典档的推敲，攻击者可

以从网络或本机针对目标机器发起验证试探，并且网络验证时(工作组或域验证)

时用户名和密码是以明文的形式传输，非常容易被窃取，使用更先进安全的认证

方式迫在眉睫。

系统身份认证的脆弱性分析

目前系统内部的大量windows 系统仍然使用windows
自身的身份认证方式，

这种认证方式首先在传输上存在被窃取的安全隐患;其次就是这种认证方式并不

公开，可能存在login
后门，也就是说有两种途径进入系统;再者就是仅以用户

名和密码作为验证方式，遭受crack
破解的几率很大，攻击者只需要一本字典档

和足够的攻击时间就可以完成破解工作。

1.2.4 应用层脆弱和风险性分析

恶意代码

恶意代码在windows
平台上主要是病毒和黑客软件问题，病毒主要是从诸如

internet,外部数据交换等环境引入;对于UNIX
系统恶意代码主要是黑客软件和

攻击代码。黑客软件和攻击代码对“系统”unix
服务器系统形成了威胁，这些

黑客软件和攻击代码的散布非常广泛且下载容易简单。

另一种恶意代码就是网络病毒，它构成威胁的层面非常广，目前系统内部还

没有相应的技术手段能够有效的处理这个隐患。

抵赖性

抵赖，在局内有好几种情况:网络攻击抵赖，破坏政务数据后的抵赖，破坏

机密数据的抵赖。网络攻击抵赖由于目前网络协议对安全性问题考虑得很少，所

以单单依靠协议地址或一些简单的通信标志来判定攻击者的身份是很难的，也是

证据不足的，高水平的攻击者在攻击时一定会掩饰自己的身份和标志，这样才不

会暴露自己的身份。

破坏数据的抵赖主要是因为现行系统平台的审计机制较弱和权限划分不清

造成的;并且局内目前针对成果数据的完整性校验工具和体系尚未建立，这类事

件在今后是极有可能发生的。

这类风险较多的存在与数据库的应用上面，对数据库的行为没有合适的审计

手段就很难做到抗抵赖。

入侵取证问题

攻击的手法和技术总是出现在针对该技术的防范之前，现有的防范体系都是

建立在已发现的手法的研究之上的，一旦入侵出现，攻击成功，如何发现攻击者

的身份和攻击的步骤，手段对及时调整网络安全设计和挽回损失会起到极其重要

的作用。

缺乏有效的网络安全审计手段，单单依靠入侵检测系统，入侵行为的取证会

显得比较困难。

应用系统自身的脆弱性

主要体现在notes 和oracle
数据库上，任何的应用软件都或多或少的存在

安全问题，一部分是软件设计上的安全bug;一部分是安全配置的问题。

针对 bug
和安全配置的漏洞采取的攻击手段和工具在互联网上流传的比较

广泛，如果没有进行合适的配置加固和安全修补，问题就会比较多，安全风险也

就比较大。

应用系统的身份认证缺陷

系统网内存在的主要应用方式是数据库系统，目前的认证方式和操作系统

平台一样都是用户名和口令，我们在系统层的认证脆弱性中进行过相应的分析，

这种用户名和口令的认证方式存在很大的隐患。

尤其是数据库系统更应该考虑这方面的问题。

应用安全审计的缺乏

应用的审计在系统网内部主要集中在数据库系统的审计上面，数据库保存

应用的重要涉密数据，任何对数据库的登陆，操作(添加，删除库表，字段等)

都应该被记录下来留以分析。

数据库的用户名和口令保存的不严密，被人窃取，那么对数据库的越权操

作也就会变的合法化，造成了损失也很难对原因进行定性。

1.2.5 管理层脆弱和风险性分析

操作失误

这是一个无法避免的问题，主要分为系统管理员和普通用户操作失误两种。

前者的影响往往是致命的，直接危害到系统和数据安全;后者主要影响用户数据

的完整性。

人为的故意攻击

来自系统内部人员的攻击是很难防范的，内部工作人员本身在重要应用系统

上都有一定的使用权限，并且对系统应用非常清楚，一次试探性的攻击演练都可

能会对应用造成瘫痪的影响，这种行为单单依靠工具的检测是很难彻底避免的，

还应该建立完善的管理制度

人员安全意识的薄弱

系统内能够接触到涉密数据的人员分布在好几个区域，其中的网管部门安全

意识较高，不会有太大的问题，但有一些终端用户如使用 Unix 数据服务器的，

这些用户也能接触到密级数据，但往往自身安全意识较差，所使用的工作平台不

是没打过安全补丁，就是口令过于简单。攻击者可以不需接触到数据服务器，只

需找一个薄弱的终端，就可以窃取或破坏数据。

有待增强的管理意识

系统内相应的安全产品一旦建立并不代表能够有效的解决安全问题，安全产品仅

是安全体系的一个方面，在整个安全体系中最为重要的实际上是管理。建立的安

全产品体系仅是一个技术上的保障，如果不配备相应的管理手段，管理策略策略，

这个安全体系依然是一个空架子，起不到任何作用。

1.3 安全保密设计思路和结构

1.3.1 安全保密设计模型

为了降低安全的风险和减少成本，根据信息安全的生命周期特征，提出了一

种按阶段实施的可操作的模型。

模型将信息安全的生命周期描述为下面各个阶段:

Policy Phase 策略制订阶段:制订系统的安全目标;

Assessment Phase
评估分析阶段:实现需求分析、风险分析、安全功能分析

和评估准则设计等，明确表述现时状态和目标之间的差距;

Design Phase
方案设计阶段:形成信息安全解决方案，为达到目标给出有效

的方法和步骤;

Implementation Phase
工程实施阶段:根据方案设计的框架，建设、调试并

将整个系统投入使用。

Management Phase 运行管理阶段:在管理阶段包括两种情况——
正常状态下

的维护和管理(Management
Status)，以及异常状态下的应急响应和异常处理

(Emergency Response Status)。

Education Phase
安全教育:是贯穿整个安全生命周期的工作，需要对企业

的决策层、技术管理层、分析设计人员、工作执行人员等所有相关人员进行教育。

?

信息安全问题且桓龇浅,从拥淖鄹衔侍猓畔?低秤卸喔丛樱畔踩
有多复杂。信息安全具有信息系统所具有的各种特性，同时也有自己的独特性。

分析某单位内部网络的信息安全需求，应该从信息安全的不同特性和不同角

度去分析，然后根据各方面分析的结果，形成综合的需求分析和解决方案设计。

信息安全最突出的特性包括:

相对性

动态性

潜在性

生命周期特性

分布性

层次性

业务相关特性

综合性、集成性

管理核心、策略核心等

安全的生命周期特性需要通过 SafeCycle
模型在信息安全体系的建立过程

以及今后的维护过程中体现。

1.3.2 安全保密设计结构

网络安全保密设计结构

物理安全 网络运行安全 信息安全保密 安全保密管理

环境安全 备份与恢复 身份鉴别 管理机构

设备安全 网络病毒防治 访问控制 管理制度

介质安全 电磁兼容 信息加密 管理技术

电磁泄漏发射防护 人员管理

信息完整性校验

抗抵赖

安全审计

入侵监控

操作系统安全

数据库安全

物理安全设计要求

为了网络设备，设施，介质和信息免遭自然灾害，环境事故以及人为物理操

作失误或错误及各种以暴力手段进行违法犯罪行为导致的破坏，丢失，涉密系统

需要具备环境安全，设备安全和介质安全等功能

网络运行安全设计要求

为保证网络功能的安全实现，涉密系统需要具备备份与恢复，计算机病毒

防治，电磁兼容等功能

信息安全保密设计要求

为了保证信息的保密性，完整性，可控性，可用性和抗抵赖性，涉密系统需

要采用多种安全保密技术，如身份鉴别，访问控制，信息加密，电磁泄漏发射防

护，信息完整性校验，抗抵赖，安全审计，安全保密性能检测，入侵监控，操作

系统安全，数据库安全等。

安全保密管理要求

系统必须加强安全保密管理，设置安全保密管理机构，制定严格的安全保密

管理制度，采用适当的安全保密管理技术将系统中的各种安全保密产品进行集

成，并加强对涉密人员的管理。

第二章 安全保密总体防护设计

依据 1.2
节对单位网络内部两个区域的安全分析结果,在本章节给出单位整

体安全保密总体防护设计措施

2.1 安全网络vlan 划分

机密级网络内部机密应用和普通密级应用没有从网络层分开，造成了网络通

信的不可控性，从涉密系统的安全设计上考虑，必须将两个不同密级的网络进行

有效的区分，配备网络访问控制才可以满足要求。

安全设计考虑在机密级网络内部使用三层骨干交换机将机密级网络中的机

密应用服务器以及客户终端和普通应用以及终端用户区分为两个
VLAN,配置三

层路由，同时设置accesslist 策略

机密级内网安全VLAN 划分解决措施:

在内网骨干交换机上按区域密级划分至少两个VLAN,配置三层路由，按

密级不同划分访问控制列表access-list，重点保护内网中重要的部门