技术方法

国土资源涉密计算机泄密隐患分析与防范

——以费县国土资源局为例

姜泉[1]，邢兆波[1]，密长林[2]

（1.费县国土资源局，山东 费县　273400；2.临沂市国土资源局，山东 临沂　276000）

摘要：依据信息安全等级保护有关政策和标准，结合费县国土资源局信息化建设中涉密计算机管理工作实际，探讨如何从计算机信息输入和输出 2 个方面有效预防计算机失窃密。从计算机身份认证与访问控制、网口、UBS 口电磁辐射，办公设备 5 个方面分析泄密隐患，并提出相应的应对措施，强调了在国土资源系统涉密计算机管理方面要加强保密意识，提高防范技能。

关键词：国土资源；信息安全；摆渡木马；电磁泄漏

中图分类号：P218　　**文献标识码**：B

国土资源信息化建设发展迅速，基础设施与业务应用逐步完善，与此同时，网络与信息安全体系也逐步建立和发展[1]。但与日益增加的业务应用对信息安全的需求相比，网络与信息安全系统尚缺乏统一的规划、安排、组织与实施，现有安全应用还比较单一，缺乏系统性和整体性，存在较大安全风险，远不能达到国家对信息系统安全防护的相关要求。从窃密的角度看，自动攻击工具越来越多、攻击技巧越来越强，但知识门槛却越来越低；从失密角度讲，主要是当事人严重违反保密有关规定。泄密事件危害极大，如不及时解决，将严重影响信息化的进一步发展。依据国家信息系统等级保护相关标准及其他信息安全标准规范[2]，结合费县国土资源局信息化建设实际经验，对国土资源计算机系统失窃密进行研究。从计算机信息输入和输出 2 个方面，分析计算机失窃密原因，落实安全防护技术措施，建立健全安全管理制度，进一步提高国土资源网络与信息系统的安全保障能力和防护水平，确保网络与信息系统的安全运行，推进国土资源信息化的安全、健康、协调发展[3,4]。

1　身份认证与访问控制

1.1　相关规定

（1）处理秘密级信息的系统口令长度不得少于 8 个字符，口令更换周期不得长于 1 个月；处理机密级信息的系统，口令长度不得少于 10 个字符，口令更换周期不得长于 1 周；处理绝密级信息的系统，应当采用一次性口令或生理特征等强认证措施；口令必须加密存储，并且保证口令存放载体的物理安全。

（2）涉密计算机原则上专人专用，特殊情况需要多人使用的必须指定专人管理，采用技术手段使相互不可访问。

1.2　分析

身份认证就是指证实主体的真实身份与其所声称的身份是否相符的过程。而这一过程是通过特定的协议和算法来实现的。如果非授权的系统使用者通过非法的途径进入了系统，那就一定会给涉密系统带来极大的安全隐患，因此身份认证是给非法入侵者设置的第一道防线。

访问控制技术是对用户访问计算机信息系统的权限分别进行控制的技术。它具有兼顾一般用户共享信息资源的方便和确保涉密信息安全的功能，是防范非法入侵者窃取涉密信息的第二道防线。实际工作中主要采用强制访问控制技术，防止非法入侵者在系统中进行超出权限范围的操作。访问控制技

* **收稿日期**：2012－02－08；**修订日期**：2012－05－03；**编辑**：王秀元

作者简介：姜泉（1981—），男，山东费县人，助理工程师，主要从事国土资源信息化管理与研究工作；E－mail：76369@126.com。

术会依据一定的原则决定能否让用户访问这些涉密信息。高密级的信息必须受到强制访问控制双重保护。目前主要做法是根据涉密人员的等级来决定他能够访问的信息的密级，低涉密等级的人员不能够知悉高密级的涉密信息。

1.3 应对措施

目前费县国土资源局的管理办法是涉密计算机专人专用，利用专门的涉密计算机防护系统，合法用户除输入口令外，还要将自己的密钥盘插入到涉密计算机上才能进入系统，人机分离时，必须将密钥盘锁入密码柜。

身份认证和访问控制技术的存在，只能保证非授权和非法用户很难进入到系统内部获取涉密信息。但是在实际工作中，一般是本着“防内大于防外”的原则，很多泄密事件的发生是由于涉密人员麻痹大意造成的。

2 网口

2.1 相关规定

(1)涉密计算机系统不得直接或者间接连接国际互联网。

(2)国家秘密信息不得在与国际互联网联网的计算机信息系统中存储、处理和传递。

2.2 分析

一是目前还没有可靠的技术手段，使与 Internet 连接的计算机信息系统得到安全保障；二是 Internet 是一个完全开放的网络空间，网络中的任何一个计算机信息系统随时都会受到来自 Internet 各个角落、出于各种目的的访问和攻击。因此一旦涉密计算机系统与 Internet 连接，将会使系统中的涉密信息受到严重威胁。

3 USB 口

3.1 相关规定

(1)禁止使用非涉密计算机和存储介质存储和处理涉密信息。

(2)涉密移动存储介质禁止连接国际互联网。

(3)非涉密存储介质禁止连接涉密计算机信息系统。

(4)涉密计算机与涉密存储介质应粘贴保密标识签。

总之，就是禁止各类移动存储介质交叉使用，其主要目的就是为了防止“木马”程序窃取涉密信息。

3.2 分析

计算机领域中所谓的“木马”是指那些冒充合法程序却以危害计算机安全为目的的非法程序。它是具有欺骗性的文件，是一种基于远程控制的黑客工具，具有隐蔽性和非授权性的特点。隐蔽性是指木马设计者为了防止木马被发现，会采用多种手段隐藏木马，这样用户即使发现感染了木马，也难以确定其具体位置；非授权性是指一旦木马控制端与服务器端连接后，控制端将获得服务器端很多操作权限，如操作文件、修改注册表、控制外设等。

针对上述情况，涉密计算机一般采用物理隔离的措施，即计算机系统不直接或间接地与互联网或者其他公共信息网络相连接。实施物理隔离可以最大限度地阻止来自于互联网的直接攻击，但物理隔离并不能彻底解决计算机系统的安全问题。

物理隔离的计算机面临的威胁主要有内部攻击、“摆渡”攻击、非法外联和非法接入等。这其中以“摆渡”攻击最为严重，且难于防范。这种方式甚至可以间接入侵既不接入互联网、也不接入内网的完全隔离的计算机。

“摆渡”攻击是利用木马和移动存储介质对计算机进行的攻击。主要包括：①攻击者控制连接到互联网的计算机，当发现移动存储介质接入时，就将“摆渡”木马植入其中；②该移动存储介质在涉密网络使用就会激活“摆渡”木马，自动收集涉密计算机上的涉密文档等信息，并进一步渗透涉密网；③木马将收集到的信息加密隐藏在移动存储介质上，当该移动存储介质再次接入互联网时，就会把收集的秘密文件发送给攻击者。

木马的启动是利用了 U 盘根目录下的 autorun.inf 文件，这个文件在 U 盘广泛使用之前一般是出现在光盘中，用于计算机插入光盘后的自动启动。例如：由于很多用户没有关闭计算机操作系统的“自动播放功能”，黑客将木马程序伪装成 autorun.inf 文件植入 U 盘中，当 U 盘在涉密机器上使用时就自动执行了木马程序，将资料复制到 U 盘中并隐藏起来，当 U 盘再次在上网机器上使用时就将资料通过网络发送出去，从而将涉密文件从没有任何网络连接的机器上窃走。

由于 autorun.inf 文件不仅存在于 U 盘上，而且在硬盘的每个分区下都有一个 autorun.inf 文件。带有木马的 U 盘一旦在某台计算机上使用，不仅会窃走资料，而且会在这台计算机中替换掉计算机硬盘中的 autorun.inf 文件，从而使得该计算机也被植入木马，进而使此后在这台机器上使用的 U 盘都被植入木马，当这些被植入木马的 U 盘在其他计算机中使用的时候就会感染其他的计算机，“摆渡”攻击就是通过这种方式实现木马的扩散。

3.3　应对措施

以费县国土资源局信息化建设经验为基础，建议：

(1)涉密介质专人管理，秘密信息在移动介质中必须加密存储，禁止用非涉密存储介质来存储和处理涉密信息。

(2)禁止在接入互联网的计算机上使用涉密存储介质。

(3)禁止接入互联网的存储介质接入涉密网计算机上，如果一定要从互联网向接入涉密网的计算机传送资料，必须使用刻录光盘的方法传送。

(4)当反病毒软件发出木马警告或怀疑系统有木马时，尽快进行杀毒和木马清除处理。

4　防电磁泄露

4.1　相关规定

(1)处理国家秘密信息的计算机信息系统必须采取防电磁辐射的防范措施。

(2)应当使用低辐射计算机设备或者采取屏蔽或干扰等防辐射的技术措施。

(3)涉密计算机系统摆放必须距离金属导体(暖气管、水管等)1 m 以上。

4.2　分析

计算机是靠高频脉冲电路工作的，由于电磁场的变化，必然要向外界辐射电磁波。这些电磁波会把计算机中的信息带出去，只要具有相应的接收设备，就可以将电磁波接收，从而窃取秘密信息。例如：①主机中各种数字电路电流的电磁泄漏；②显示器视频信号的电磁泄漏；③键盘开关引起的电磁泄漏；④打印机的低频泄漏等。

4.3　应对措施

使用低辐射计算机设备，如：红黑电源；计算机电磁屏蔽技术，如：屏蔽箱；计算机电磁辐射干扰技术等。

距离金属导体 1 m 以上主要是因为计算机使用高频信号，因此电磁波可以借助计算机系统的电源线、数据连接线、机房内的电话线，甚至暖气管道及地线等金属导体进行传播，特别是这些管线都有弯曲部分，这就更有利于窃密者的接收，如果电磁波走直道是靠电磁波自身能量辐射，而弯道则相当于带有信息的辐射电子飞出了金属导体，也就把这些信号给传到外边了。

目前费县国土资源局规定机密级计算机必须安装视频电磁干扰仪，以防止上述事件的发生。另外，对于打印机、刻录机等输出设备来说，最主要的还是管理问题。在费县国土资源局规定涉密办公自动化设备依照“谁使用，谁负责”的原则进行管理，除进行设备台账管理，明确领导责任和使用人责任以外，为每台涉密设备建立使用登记表，凡是利用涉密办公自动化设备输出、制作、产生的各类涉密载体必须履行审批、登记等手续，其目的就是对所有涉密设备都做到使用行为可查、可追朔，防止非法输出。

5　办公设备

5.1　相关规定

(1)每台涉密设备均须建立使用登记表。利用涉密办公自动化设备输出、制作、产生的各类涉密载体必须按《国家秘密载体管理办法》履行审批、登记等手续。

(2)维修一般在单位内进行，由单位工作人员完成或全程旁站陪同。

(3)需要外出维修的，应当拆除所有可能存储过涉密信息的硬件和固件，与维修单位和维修人员签订保密协议。

(4)如涉密设备中存储过涉密信息的硬件和固件不能拆除，应当按照涉密载体销毁要求予以销毁。

(5)涉密设备的存储硬件禁止降低密级使用。

(6)不再使用或无法继续使用的涉密设备需要报废前，使用人应拆除存储过涉密信息的硬件和固件，履行销毁审批手续。

(7)经审批后，将存储过涉密信息的硬件和固件送保密部门统一进行销毁。

5.2　分析

硒鼓作为激光打印机的核心部件，它的工作原

理是:当文字或图像的激光信息逐行照射在有机光导鼓(OPC)上时,会在鼓芯表面形成静电潜像,同时将墨粉吸附在鼓的表面上,进而转印到纸上,即完成打印。如果想窃取打印机打印的信息,可以把扫描棒安装在硒鼓上的某个部位,比如:硒鼓的废粉仓内,硒鼓的充电辊下方,或有机光导鼓的鼓仓上。当打印文稿经过扫描棒时,文稿内容就会全部被扫描并存贮下来。如果扫描棒中配有无线发射装置或者在维修、报废环节中内容被读取,涉密信息就会泄漏。

除了辐射泄密外,目前市场上主流复印机、打印机、以及传真机等都有存储或临时存储数据的硬盘。这些硬盘存储的数据像电脑硬盘一样即使删除也能恢复。因此,打印机、复印机等维修、报废时,如果硬盘不进行严格脱密处理,就容易出现泄密问题。同理,如果将涉密资料拿到地方商家进行喷绘、复印,即使亲眼所见对方没有存储自己的资料,但商家的硬件设备已经记录了所处理的数据,同样有泄密可能。

5.3　应对措施

针对目前办公自动化领域存在的泄密漏洞和隐患,切实加强涉密单位打印机硒鼓的保密管理工作已迫在眉睫,这就要求必须从硒鼓的生产、供货、使用和回收 4 个环节上强化管理,以确保生产单位可靠、供货渠道安全、使用管理规范、回收环节严格。

6　结语

在国土资源涉密计算机管理方面,费县国土资源局制定了 4 项举措强化管理:

(1)完善制度,加强培训。规范机关计算机安全使用,确保局机关网络信息安全工作有效顺利开展。

(2)落实措施,着眼防范。对全局所有计算机全部安装了防病毒、防火墙软件,及时查杀木马等病毒,对重要岗位计算机组织专人定期进行全面检查,并研究制定了信息安全应急预案,进一步提高了全局预防和控制网络突发事件的能力和水平。

(3)加强管理,严防泄密。对涉密文件以及与此有关的计算机进行全面清理,并按要求在局办公室设立 1 台涉密专用计算机,专门存储全局重要文件和档案,并指派专人管理维护使用,严禁接入互联网,严禁与非涉密移动存储介质交叉使用,确保国家秘密的安全。

(4)严格追究,违规必惩。本着谁主管谁负责、谁使用谁负责、谁运行谁负责的原则,规定各股长为股室计算机管理第一责任人,所长为各中心所计算机管理第一责任人,按照国家有关法律、法规、规定使用,严格执行机关制定的计算机网络管理工作制度,违反机关计算机网络管理制度,造成损害的,依照有关规定进行坚决处理。

保密工作“三分技术,七分管理”,只要在工作中不断加强保密意识,提高对泄密隐患的防范技能,并在工作中落实执行各项保密工作的要求,从细节做起,预防与改进并重,做到“想保密,会保密,干保密”,形成扎实系统的个人保密素养,就一定能在保密工作中做到“万无一失”。

参考文献:

[1] 王建兵. 国土资源信息系统安全建设整改需求探讨[J]. 国土资源信息化,2010,(4):3-6.

[2] 徐世亮. 江西省国土资源网络安全防护体系建设探讨[J]. 国土资源信息化,2011,(4):45-48.

[3] 尹建国,曲党政,张英. 浅谈“数字城市”建设与城市规划[J]. 山东国土资源,2011,27(5):63-64.

[4] 密长林,孙景广,姜莉,等. 临沂市国土资源数字执法系统的设计与实现[J]. 山东国土资源,2011,27(4):47-49.

Analysis And Prevention of Computer Leak Risks in Land and Resources Line

JIANG Quan[1], XING Zhaobo[1], MI Changlin[2]

(1. Feixian Bureau of Land and Resources, Shandong Feixian 273400, China; 2. Linyi Bureau of Land and Resources, Shandong Linyi 276001, China)

Abstract: According to policies and standards of information security levels, combining with the practices of computer management information construction in Feixian Bureau of Land and Resources, countermeasures for preventing computer theft secret in computer input and output have been studied.

Key words: Land and resources; information security; ferry horse enforcement; electro-magnetic leakage