广西科学院学报
Journal of Guangxi Academy of Sciences

2008,24(4):370~372
Vol. 24,No. 4 November 2008

涉密网物理隔离后的安全威胁及防范措施
Security Threat and Protection Measures on Confidential Network

刘孟全
LIU Meng-quan

(桂林空军学院,广西桂林 541003)
(Guilin Airforce Academy, Guilin, Guangxi, 541003,China)

摘要:分析涉密网与国际互联网或其它公共信息网物理隔离后所面临的主要安全威胁,认为涉密网物理隔离后主要存在内部攻击、"摆渡"攻击、非法外联和非法接入4种安全隐患,并针对这4种安全隐患提出相应的技术防范措施。

关键词:涉密网络 物理隔离 网络安全 威胁
中图法分类号:T309.2 **文献标识码**:A **文章编号**:1002-7378(2008)04-0370-03

Abstract: Four primary threats to security which contain internal attacking, ferry attacking, Illegal External Link and illegal connection between confidential network and Internet are analyzed. Kinds of technique defense ways against these threats are put forward.

Key words: secret network, physical isolation, network security, threat

目前,随着网络应用的普及深入,网络入侵和攻击日益猖獗,网络安全遭受到严重威胁,为防止涉及国家秘密的计算机及信息系统受到来自互联网等公共信息网络的攻击,确保国家秘密信息的安全,党和国家多次强调要求涉密计算机及信息系统要与互联网等公共信息网实行物理隔离,2000年1月1日起实施的《计算机信息系统国际联网保密管理规定》第二章保密制度第六条明确规定:"涉及国家秘密的计算机信息系统,不得直接或间接地与国际互联网或其它公共信息网络相连接,必须实行物理隔离"。众所周知,国际互联网是以国际化、开放和互联为特点的,而安全度和开放度永远是一对矛盾。虽然,目前可以利用防火墙、代理服务器、入侵监测等技术手段来抵御来自互联网的非法入侵,但是这些技术手段都还存在许多漏洞,还不能彻底保证涉密网信息的绝对安全[1]。物理隔离作为一种安全管理的技术手段,能够比较有效地防范来自外界对网络和信息系统的安全威胁。只有使涉密网和公共网"物理隔离",才能保证涉密信息网络不受来自互联网的黑客攻击,保证涉密网的信息不被泄漏和破坏[2,3]。实施物理隔离可以最大限度地阻止来自于国际互联网的直接攻击,但是物理隔离并不能彻底解决涉密计算机网络的安全问题。本文分析涉密网与国际互联网或其它公共信息网物理隔离后所面临主要安全威胁,并提出相应的技术防范手段。

收稿日期:2008-10-12

作者简介:刘孟全(1968-),男,高级实验师,主要从事园区网安全研究工作。

1 涉密网物理隔离后的安全隐患

物理隔离的涉密计算机网络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4种安全隐患。

1.1 内部攻击

美国CSI/FBI(计算机安全协会/联邦调查局)在1999至2003连续5年的《计算机犯罪与安全调查报告》中指出,有超过85%的安全威胁来自组织内部[4]。内部网络易受到攻击的主要原因有:(1)内部网络网速快,百兆甚至千兆的速度,能让黑客工具大显身手。(2)目前针对内部网络安全的重视程度不够,大量有漏洞的系统没有打上补丁。内部网络拥有更多的应用和不同的系统平台,自然有更多的系统漏洞。(3)为了简单和易用,在内网传输的数据往往是不加密的,这为别有用心者提供了窃取机密数据的可能性。(4)内网的用户往往直接面对数据库、直

接对服务器进行操作,利用内网的高网速,可对关键数据进行窃取或者破坏。(5)众多的使用者拥有不同的权限,管理更困难,系统更容易遭到口令和越权操作的攻击。服务器对使用者的管理也不是很严格,对于那些如记录键盘敲击的黑客工具比较容易得逞。(6)涉密信息不仅仅限于服务器,同时也分布于各个工作计算机中,目前对个人硬盘上的涉密信息缺乏有效的控制和监督管理办法。(7)由于人们对口令的不重视,弱口令很容易产生,很多人用诸如生日、姓名等作为口令,在内网中,黑客的口令破解程序更易奏效。

1.2 "摆渡"攻击

"摆渡"是指在物理隔离的两个网络间所进行的信息交换,"摆渡"攻击就是在"摆渡"过程中发生的对物理隔离网络所实施的攻击。应用最新的攻击技术,攻击者可以利用移动存储介质对物理隔离的网络实施"摆渡"攻击。攻击者首先攻击控制连接到互联网的计算机,当发现移动存储介质接入时,就会将"摆渡"木马植入其中。该移动存储介质一旦在内网使用就会激活"摆渡"木马,自动收集内网计算机上的涉密文档等信息,甚至可以进一步向内网渗透,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在接入互联网的计算机上使用时,木马就会自动把收集的秘密文件交给攻击者。移动存储介质的广泛使用和管理不善,使得移动存储介质成为"摆渡"攻击中的一艘艘"渡船"。

1.3 非法外联

非法外联是指涉密信息系统非法接入互联网,其表现形式主要有两种:一是私自将计算机同时连接涉密网和互联网,使涉密网和互联网相互联通;二是将涉密计算机接入互联网。

按照相关规定,涉密信息系统不能与互联网相连,但是有人为了便利,可能把计算机一边接入涉密网,一边又通过拨号、宽带、无线等方式接入互联网,破坏涉密网的物理隔离。由于这条接入互联网的线路几乎没有网络安全防御措施,外部攻击者很容易通过这条线路获取计算机的控制权,进而渗透到涉密内部网络,窃取涉密网的秘密信息。即使当事人员没有恶意,给涉密网带来的危害和后果也是非常严重的。

除了要防止一台计算机同时接入涉密网与互联网的现象,还要严防私自将涉密计算机特别是涉密便携式计算机带回家中接入互联网的行为。有些工作人员在办公时将便携式计算机接入涉密计算机网络处理涉密信息,回家后又将便携式计算机接入互联网,查阅资料、处理电子邮件。从表面上看,只要接入互联网前把机器上的涉密信息清除掉,这种行为的危害不大。然而,计算机一旦接入互联网就有可能遭受攻击。如果攻击者入侵并控制计算机,就可以利用磁盘恢复技术将清除的涉密信息还原出来。同时,入侵者还可以通过对机器上信息的分析,判断出该主机是否曾接入涉密网,并在其中植入特殊的木马。计算机回到涉密网后,这种木马就会自动收集涉密网内的信息,并且加密存储起来,等到计算机再次上互联网时,主动把收集的信息加密发送到事先指定的邮箱地址,达到窃取秘密的目的。

1.4 非法接入

非法接入是指外部信息系统非法接入涉密计算机网络。对涉密内部网络而言,随着计算机网络应用的普及,综合布线时在各个可能联网的位置都预留了网络接口,加上工作人员和工作环境的变化,一些网络接口可能出现失控。这些失控的接口被人非法使用,就会导致外部计算机进入内部网络。另外,涉密内部计算机网络中的主机如果对外提供拨号接入服务,也有可能被非法用户使用,使得外部计算机进入内部网络。恶意用户非法接入涉密网,会对涉密内部网络进行攻击,窃取秘密情报。即便没有恶意的用户接入涉密网,也会使涉密用计算机网络内部出现使用非法软件、使用未受控的存储介质存储秘密、进行非法外联等现象,导致严重的泄密事件。

2 涉密网物理隔离后的防范措施

针对涉密网面临的安全威胁,必须在管理和技术手段两方面采取相应的防范措施。首先,在管理上要制定规章制度和奖惩措施,明确哪些行为是禁止的,即使这些行为没有造成危害也要受到处罚(如网络扫描行为),将攻击行为消灭在萌芽状态。其次,在技术手段上针对不同的安全隐患,采取不同的技术措施[5]。

2.1 防范内部攻击

采用符合可信计算组织 TCG 推出的可信任网络连接 TNC 标准规范的安全解决方案是涉密网络防范内部攻击的最有效措施[6]。TNC 从操作环境的硬件组件和软件接口两方面制定可信计算的相关标准与规范,主要目的是通过使用可信主机提供的终端技术,实现网络访问控制的协同工作。TNC 网络构架结合已存在的网络访问控制策略(例如 802.1x、IKE、Radius 协议)来实现访问控制功能,通过提

供一个由多种协议规范组成的框架来实现一套多元的网络标准，其主要功能和目标有：(1)平台认证。用于验证网络访问请求者身份，以及平台的完整性状态。(2)终端策略授权。为终端的状态建立一个可信级别，例如：确认应用程序的存在性、状态、升级情况，升级防病毒软件和IDS规则库的版本，终端操作系统和应用程序的补丁级别等。从而使终端被给予一个可以登录网络的权限策略，进而获得在一定权限控制下的网络访问权。(3)访问策略。确认终端机器以及其用户的权限，并在其连接网络以前建立可信级别，平衡已存在的标准、产品及技术。(4)评估、隔离及补救。确认不符合可信策略需求的终端机能被隔离在可信网络之外，执行适合的补救措施。

软件和硬件相结合才能实现TCG/TNC标准规范，目前国内已有部分厂商的全局安全网络解决方案符合该标准规范，涉密网络应优先采用这些方案。在此基础上，结合网络行为审计系统，则可以有效防范内部攻击。

2.2 防范"摆渡"攻击

对于可采用移动存储介质管理系统来防范"摆渡"攻击。对移动存储介质从购买、使用到销毁全过程进行管理和控制。从密级设定、认证授权、访问控制、锁定自毁、违规监控、扇区加密、安全审计等方面对移动存储介质进行失泄密防护管理，实现：进不来(非涉密介质接入涉密计算机上不能使用)、拿不走(涉密介质接入非涉密计算机上不能使用)、读不懂(无使用者身份认证授权用户不能解密，涉密介质丢失不会造成泄密事故)和走不脱(详细的涉密介质使用日志，泄密事件可追踪)的管理目标。

2.3 防范非法外联

防止非法外联，应对涉密网内部计算机接入互联网的行为进行监管，使内部计算机只能访问涉密网IP地址，其余IP地址禁止访问。结合TNC标准规范中的用户入网认证客户端或移动存储介质管理系统可轻易实现此功能，从而防止涉密计算机非法接入互联网。

2.4 防范非法接入

防止非法接入，要严格控制接入涉密网的每台终端，防止未授权的计算机接入涉密网。网络管理员应该高度重视网络接入的安全，通过安全策略对内网计算机的身份进行认证，将MAC地址和交换机端口绑定，如果要达到更高的安全级别还可将IP地址、用户名和Vlan也同时绑定，关闭暂时不用的交换机端口，杜绝非法计算机接入[7]。

3 结束语

涉密网和公共互联网采用相同的技术构建，面临着许多相同的安全问题。由于涉密网和公共互联网是"物理隔离"的，且对网络安全有较高要求，其安全隐患有明显的特点。针对这些安全隐患，目前已经有成熟的技术手段进行防范，只要合理采用这些技术，就能基本保证涉密网的信息安全。

参考文献：

[1] 肖伟春. 内网安全建设规划方案探讨[J]. 计算机安全，2007(8)：94-95.
[2] 李敏，费耀平. 物理隔离技术的研究[J]. 计算机工程，2004，30(4)：104-106.
[3] 陈睿，田忠和. 物理隔离网闸数据交换技术的研究[J]. 计算机与数字工程，2005，33(2)：47-49.
[4] 于阳. CSI/FBI2003年计算机犯罪与安全调查(上)[J]. 信息网络安全，2003(9)：57-59.
[5] 石峰. 浅论公安边防部队内网安全体系建设[J]. 网络安全技术与应用，2007(5)：78-80.
[6] 李兴国，顾震苏. 基于可信网络连接的安全接入技术[J]. 微计算机信息，2007，23(15)：28-29，46.
[7] 范一鸣. 校园网接入控制技术应用研究[J]. 计算机应用，2003，23(s2)：28-30.

(责任编辑：韦廷宗)

西班牙科学家用头发培育出多能干细胞

诱导式多能干细胞具备人体胚胎细胞和成熟细胞两种干细胞在医学应用方面的优点，但是其培育过程却十分困难且低效。巴塞罗那再生医学中心的科学家采用新方法，用一根头发就可以获得诱导式多能干细胞，将这种细胞培育过程效率提高了100倍，而且这种多能干细胞的增殖能力和发育的多样性与胚胎细胞不相上下。另外，这种多能干细胞还具有胚胎细胞欠缺的一大优点，即从某个病人的头发培育出的诱导式多能干细胞的基因与这个病人的基因匹配，这样将来科学家有可能培育出能治疗特定疾病的干细胞。但是目前使用头发培育出的诱导式多能干细胞还不能真正用于治疗疾病，还需要通过多次病毒导入等研究，将其基因构型还原到"多能性"。

(据科学网)