doi: 10.3969/j.issn.1006-1576.2011.01.017

涉密网络信息安全保密

李刚，雷艾，张弦弦
（中国兵器工业第 58 研究所 信息中心 四川 绵阳 621000）

摘要：针对军工单位涉密网络的安全保密要求，对涉密网络信息安全保密技术进行研究。分析了网络信息安全的安全防范措施及其实现方法，将入侵检测技术与防火墙技术、身份鉴别技术等增强协作，以增加其自身的动态灵活反应及免疫能力，保障涉密网络的信息安全。网络信息保密技术的发展趋势表明，必须要不断追踪新的信息技术，及时升级更新、完善信息系统的安全防御措施。

关键词：信息系统；信息安全；身份鉴别；入侵检测
中图分类号：TP393.08　　**文献标志码**：A

Secrecy Network Information Security

Li Gang, Lei Ai, Zhang Xianxian
(Information Center, No. 58 Research Institute of China Ordnance Industries, Mianyang 621000, China)

Abstract: Aiming at the security requirements of secrecy network, research the information security technology. Analyze the security of network information safety precautions and its implementation will be detected, the technology and the technology and capacity to identify technologies for enhanced coordination to increase their own dynamics flexible response and immunity ability to guarantee the network security of secret information. Network information confidential the technological development trend that must keep track of new information technology to upgrade and update and improve information systems security precautions.

Keywords: information systems; information security; authentication; IDS

0　引言

在军工单位中，需要处理、存储国家秘密的计算机称为涉密计算机，由涉密计算机构成的网络系统称为涉密网。网络信息安全是指防止网络本身及其采集、加工、存储、传输的信息数据被故意或偶然的非授权泄露、更改、破坏或使信息被非法辨认、控制。目前，军工单位普遍使用计算机网络进行产品设计和生产经营管理，通过计算机造成的失泄密事件日益增多。为了确保国家秘密的安全，国家对从事军工科研和生产的单位实行保密资格审查认证制度，并对军工单位的涉密网络建设和使用提出相应的要求。故针对军工单位如何达到涉密网络的安全保密要求进行探讨。

1　涉密网络信息安全的要求及其特点

1.1　涉密网络的技术防范要求

国家在对军工单位的保密资格审查认证中，要求军工单位的涉密网络必须由具备涉密系统建设资质的单位进行设计和建设，并遵循《涉及国家秘密的信息系统分级保护技术要求》（BMB17-2006）、《涉及国家秘密的信息系统分级保护方案设计指南》（BMB23-2008）。其中，明确提出涉密网络必须具备以下技术措施：备份与恢复、病毒防范、身份鉴别、访问控制、信息加密、安全审计、入侵检测、漏洞扫描等。并要求对涉密网络中的信息输入输出接口进行控制。

1.2　涉密网络的技术防范特点

1) 对于国家秘密，需要划分不同的级别，每个级别中又划分为若干类，每类涉密信息的知悉范围是确定的。这种控制秘密信息的知悉范围是强制的，不得超越。在涉密网络中需要确定每台计算机操作者的身份，并能对网络中涉密信息的传递行为进行控制。

2) 身份假冒包括：非法使用人员通过私自使用涉密计算机仿冒合法使用人；合法使用人员通过伪造盗用它人 IP 地址仿冒其他合法使用人员。为了防止身份假冒，在网络的登陆使用中需要将现实中的人与网络中的虚拟身份地址关联起来，且确保其身份地址不能被盗用。

3) 在计算机使用过程中，需要对涉密信息的创建、打开、更名、复制、编辑等行为进行识别和控

收稿日期：2010-10-12；修回日期：2010-10-27
作者简介：李刚（1976-），男，重庆人，工程师，从事网络安全与集成研究。

制。同时，还需要将各种日志信息的格式进行统一，以便于在发生失泄密事件后进行审计追查。

4) 计算机信息输入输出接口（USB 接口、光驱、软驱等）是计算机失泄密事件的主要通道。需要对计算机的所有接口能进行控制，主要通过内网安全管理、身份鉴别、访问控制、安全审计、信息加密技术来实现。

2 涉密网络的信息安全原则与措施

2.1 涉密网络的信息安全原则

1) 制度体系、流程管理与技术手段相结合的原则

军工保密安全以管人为主，安全策略要以完整的制度体系、规范合理的工作流程为主，结合技术防范手段来实现，不能将保密安全策略完全建立在技术手段上。

2) 公众产品与涉密产品相结合的原则

保密安全体系首先应建立在一个相对完整的网络基础上，对基础的网络和非核心的部分应采用成熟的公众产品，如交换机、备份恢复系统、网络防病毒系统等，在关键部分采用专用的涉密安全产品，如身份鉴别、防火墙、入侵检测、漏洞扫描等。

3) 全面预防与重点防范相结合的原则

由于产品设计和生产经营管理的实际需要，军工单位的信息安全应建立在全面预防措施的基础上，对重点的信息安全方面采用技术手段进行自动监控，优先解决身份鉴别问题，其次是信息输入输出接口的控制，最后解决访问控制。

4) 最小授权原则

军工单位涉密人员各自的涉密范围不同，在对人员进行权限设置时，只针对需要访问的模块或信息授权，尽量控制涉密人员的访问范围最小化。

5) 选用成熟技术与兼顾技术发展相结合的原则

军工单位涉密网络处理的是国家秘密，应优先选择成熟可靠的保密安全产品。

2.2 采取的技术措施

结合上述原则和军工单位涉密网络的技术防范要求，采取分级控制与加密存储相结合的措施对涉密信息档案，特别是涉密文件加以保护。

在制度上明确由单位统一管理，并为每位在涉密网中的员工固定一个 IP 地址（与 MAC 地址和交换机端口进行绑定），IP 地址所产生的所有行为视为该员工的行为。

采用硬件钥匙结合口令的方式对操作系统的登陆进行完善，通过硬件钥匙进行身份验证的方式将具体员工与虚拟 IP 对应关联起来。

对涉密信息进行知悉范围控制。在对涉密信息分类的基础上控制涉密信息的打开、编辑等操作行为，将对涉密信息的管理控制变成对操作权限的分配和管理。

对网络服务器的访问进行控制，对网络中受限终端的对外信息输出渠道进行控制。网络服务器的访问控制可以采用防火墙与交换机 VLAN 技术相结合的方式来解决。对于终端信息输出渠道的控制，可以采用基于网络的设备集中控制系统，即固定一个输出口，其余端口全部封闭。

军工单位涉密网络的保密安全措施及其实施在单位中始终是动态变化的，其引起改变的时机和方法取决于安全审计的结果。因此，还应对涉密信息审计及安全策略进行动态调整。

3 信息安全产品的关键技术

3.1 身份认证与自主加密保护相结合

在军工单位涉密网络的日常应用中，需要对各种涉密文件进行大量处理，应该为每位使用者提供对自己处理的涉密文件进行加密保护的功能，其加密密钥可以用同一个硬件钥匙来保存。对硬件钥匙中的密钥进行管理（写入、修改、读出、存储），使之符合密品管理的要求。通常使用 USB 接口设备，通过硬件钥匙进行身份认证。

3.2 涉密资料的分类管理、操作行为与访问控制相结合

涉密网络中的涉密信息要控制其知悉范围，必须对涉密信息及其使用人员进行分类，建立一种相对固定的关联规则。

国家秘密信息在军工单位涉密网络中主要表现为文字和图形，为了防止无关人员接触秘密信息和通过更名等方式改变国家秘密的表现形式而造成秘密泄露，必须对使用人员的计算机操作行为（打开、创建、更名、复制、编辑）进行控制。

要在涉密网络上实现访问控制，使涉密信息只被授权的人员知悉，必须建立涉密信息与授权人员的对应关系规则，确定其可以进行的操作类型。可采取下列方式：

1) 将涉密信息按使用类型进行分类，确定每类

涉密信息的知悉对象；对涉密信息进行分类，比如，对军工产品的设计、工艺、生产等过程产生的涉密信息按项目管理的方式进行分类，对经营过程中产生的涉密信息按计划、财务、质量、试验等使用属性进行分类等。这样，每类涉密信息的知悉人员是相对确定的，为避免使用人员频繁变化带来的设计困难，可以引入相对固定的人员类别表述——角色。这时，对知悉范围的管理就转变为对涉密信息类别与角色之间的关系集合的管理。

2) 通过组织结构树来管理使用成员，通过硬件钥匙转换成对应的 IP 地址，使用人员对某类涉密信息的知悉权利就可以用是否属于某个角色来表述。这时，对使用人员的管理就转变为对角色组中成员的管理。

通过引入相对固定的角色概念，访问控制的实现就转变为对信息类别与角色、角色与使用人员之间的关系的管理。

在确定上述关系的同时，还必须要有对网络入侵进行检测监控的能力，以实现对知悉范围的控制。

3.3　控制高密级信息的安全流向

怎样控制高密级安全区域的涉密信息不能流向低密级安全区域，而高密级安全区域的非涉密信息流向低密级安全区域又不受影响，是现在军工单位迫切需要解决的一个问题。

可以通过 OA 或邮件系统，在文件进行传输的时候，首先读取文件的属性，由文件的属性来判定该文件是否涉密，如果该文件涉密，则不允许发送。

3.4　日志与审计相结合

如何解决计算机中不同操作系统所产生的日志信息格式的统一，在不占用大量的网络带宽资源的情况下，如何保证日志信息在产生和传输过程中不会被旁路、篡改、丢失，在审计中如何结合访问控制的规则自动对违规的日志信息进行高效过滤并自动报警。

需要进行审计分析的主要设备包括：路由器、防火墙等网络和网络安全设备以及通用的操作系统等，对这些的日志进行日志过滤、可疑的活动进行综合分析；根据确定的安全策略和实施情况的差距进行有效的审计，根据审计结果和日志内容抵御和清除病毒、蠕虫和木马，修补系统的漏洞。升级已有的和不安全的服务，加强网络审核，加强反病毒扫描，增加建设审计报告库，总结每次出现的问题和解决的方法。

4　涉密网络信息安全技术发展趋势

4.1　分布式入侵检测

分布式入侵检测系统是现代 IDS 主要发展方向之一，主要包括 2 层含义：1) 针对分布式网络攻击的检测方法；2) 使用分布式的方法来检测分布式的攻击，其中的关键技术为检测信息的协同处理与入侵攻击的全局信息的提取。分布式入侵检测系统能在数据收集、入侵分析和自动响应方面最大限度地发挥系统资源优势，其设计模型具有很大的灵活性。

4.2　智能化入侵检测

现阶段常用的智能化方法有神经网络、遗传算法、模糊技术、免疫原理等方法，这些方法常用于入侵检测的辨别与泛化，利用专家系统的实现来构建 IDS 也是常用的方法之一。

4.3　网络安全技术相结合

结合防火墙、PKI（Public Key Infrastructure，公开密钥基础设施）、安全电子交易等网络安全技术与电子商务技术，提供完善的网络安全保障。

4.4　建立系统的测试评估体系

设计通用的入侵检测测试评估方法和平台，实现对多种入侵检测系统的检测，已成为当前入侵检测系统的一个重要研究与发展领域。评估入侵检测系统可从检测范围、系统资源占用、自身的可靠性等方面进行。评价指标有：能否保证自身的安全、运行与维护系统的开销、报警准确率、负载能力以及可以支持的网络类型、支持的入侵特征、是否支持 IP 碎片重组、是否支持 TCP 流重组等。

5　总结

目前，信息系统技术正处于蓬勃发展的阶段，新技术层出不穷，也不可避免地存在一些漏洞。因此，要不断追踪新技术的应用情况，及时升级更新、完善信息系统的安全防御措施。

参考文献：

[1] 谢希仁. 计算机网络[M]. 电子工业出版社, 2003.
[2] 蔡立军. 计算机网络安全技术[M]. 中国水利水电出版社, 2005.
[3] 杨波. 网络安全理论与应用[M]. 北京电子工业出版社, 2002.