ISSN 1009-3044
Computer Knowledge and Technology 电脑知识与技术
Vol.11, No.16, June2015

E-mail: jslt@dnzs.net.cn
http://www.dnzs.net.cn
Tel:+86-551-65690963 65690964

军用信息安全标准探析

江山[1],康洪晶[1],苏肖[2]

(1.海军工程大学,湖北 武汉 430033;2.92608部队,上海 20000)

摘要: 简述了国内外民用信息安全标准发展和研究的现状,介绍了我军信息安全标准建设,并对最常用的GJB2646-96《军用计算机安全评估准则》做了详细分析,对军用信息安全标准从完善体系建设和加强信息安全管理标准建设等方面提出改进建议。

关键词: 军用信息安全;信息安全标准;GJB2646-96;管理标准

中图分类号:G350 **文献标识码:A** **文章编号:1009-3044(2015)16-0016-03**
DOI:10.14004/j.cnki.ckt.2015.1167

Analysis on Information Security Standard of Army

JIANG Shan[1], KANG Hong-jing[1], SU Xiao[2]
(1.Naval University of Engineering, Wuhan 430033, China; 2.92608 PLA Troops, Shanghai 20000, China)

Abstract: The paper introduce the situation 0f the development and research on the information security standard in-country and oversea, also as the PLA in detail. The paper analyses the standard of GJB 2646-96 detailedly, and table a proposal about the information security standard of army on perfecting the system and enhancing the manager.

Key words: information security of army; information security standard; GJB 2646-96; management standard

为实现我军新时期新阶段的打赢局部战争和完成非传统任务的目标,我军的信息化程度不断提升,信息安全也正逐步重视。近年,国内外敌特分子对我军涉密信息的窃取越加疯狂,由于我军信息安全领域出现的失泄密事故对我军的建设和发展带来不小影响。分析和研究我军当前的信息安全标准,从体制和标准的高度遏制失泄密事故,从而进一步提高军用信息安全性和可靠性。

1 国内外信息安全标准建设发展情况

随着信息化建设的发展,各行业领域的信息化应用和建设越加广泛和深入。信息安全标准是指导信息安全产品和系统的开发设计指南,是评价或评定软件产品或系统的安全性的基本依据,是信息安全保障体系建设的全局性、长远性、基础性和规范性工作,应用于信息安全产品和系统的设计、研发、生产、建设、使用、测评的生命周期全过程,是提高软件或系统安全性的基本技术规范。[1]

安全标准是信息化建设的基础工程,是提高信息化安全体系构建质量的重要保证和科学控制手段,对提高软件整体安全质量和水平发挥重要作用。

1.1 信息安全标准的发展

国际上针对信息安全制定了多个标准,但是总的来说主要是从两个方面,即:侧重于系统和产品的技术指标和侧重于信息的日常管理标准,简单来说就是技术流和管理流。

1.1.1 侧重于系统和产品的技术指标的信息安全标准发展流

上世纪70年代,随着计算机、网络等信息技术在国家重点行业和领域的广泛应用,由于软件失效故障以及安全体系管理存在的漏洞导致的问题愈发严重,甚至造成了严重的经济损失及人员伤亡。美国国防科学委员会基于此在1970推动了第一部信息安全标准,即可信计算机系统评价标准(TCSEC,Trusted Computer System Evaluation Criteria)的诞生。该标准是世界范围信息安全领域第一个全面的信息安全技术标准,对信息安全相关要求做了严格规范,特别是首次提出了安全分级评级概念,将软件产品或系统的安全划分为A、B、C、D,4个等级、7个级别,针对文件和用户提供安全保护,操作系统保护,审记保护,强制性保护以及最高级别安全保护。美国国防部1985年12月公布该标准,起初在军队广泛应用,并向民用领域推广应用,逐渐成为具备广泛指导性的评价和建设标准。

与美国的TCSEC标准强调信息保密性不同,欧洲四国(英、法、德、荷)为了全面衡量软件或系统的信息安全保密性以及完整性、可用性整体安全性提出了新的评价标准,这也是目前信息安全性的划分指标的基础和雏形。欧洲四国根据多年来在军队,政务,商务等重要部门和领域信息安全要求发展的需要,建立了信息技术安全评价准则(ITSEC,Information Technology Security Evaluation Criteria)。ITSEC标准将信息安全从基本功能和评价方法两个角度提供基本规范和具体指南,其中基本功能准则划分为10级F1~F10,其中,前5级F1-F5对应于TCSEC

收稿日期:2015-05-10
作者简介:江山(1977—),男,上海人,工程师,硕士,研究方向为信息技术;康洪晶(1984—),男,黑龙江延寿县人,工程师,硕士,研究方向为计算机应用技术;苏肖(1985—),男,安徽人,工程师,硕士,研究方向为计算机应用技术。

的五级评价标准，后6级F6-F10重点针对程序及数据，操作系统可用以及针对网络的广泛应用建立的数据通信保密性、完整性、可用性提出具体要求和评价方法。同事，ITSEC对建立软件或系统的形式和非形式化描述，以及安全策略的基本形式模型和硬件结构设计要求。与TCSEC对应的是，ITSEC不把信息安全列入软件和系统本身之中，而将信息安全性作为软件或系统的重要评价标准之一，是衡量评价软件或系统的重要方面和依据。

美国连同加拿大以及ITSEC的欧洲四国为代表的欧联体等六个国家七个标准组织于1993年6月起草并推出了信息技术安全评价通用准则(The Common Criteria for Information Technology security Evaluation，CC)，并作为将其作为重要参考和依据推动了信息安全国际标准的诞生。CC标准综合了之前相关已有信息安全标准，结合信息安全控制最新技术和方法，以安全功能和评价为主，推出了以安全审计、通信、密码保护、用户数据保护、标识与鉴别等为主的11个安全功能，以及以功能测试、结构测试、系统测试和检查以及半形式化和形式化的设计和测试为主的7个评估保证级别。目前，CC标准已成为国际信息安全通用规范和安全认证标准。

1.1.2 侧重于信息系统安全日常管理标准发展流

随着信息技术在商业领域的广泛深入应用，应英国广大商业公司及部门要求，英国贸易工业部于1993年着手研究信息安全管理方法，并进行研究立项，在1995年推出了BS7799-1：1995《信息安全管理实施规则》，标准为大、中、小各型工商业信息系统综合已有安全管理惯例方法提供了具备可参考、可操作的安全实施规则，明确了信息系统设计中安全保证的流程方法，设定了信息安全控制范围基准。在此基础上，随后在1998年推出了BS 7799-2：1998《信息安全管理体系规范》，主要规范了信息安全控制范围基本要求，对信息系统的部分或全部信息安全提供了系统性的评估基础，也可视为对已有信息系统进行信息安全体系评估的可靠规范。信息安全管理体系BS7799由信息安全管理规则和信息安全管理体系两个基本部分组成，主要从具体信息系统实施方法规范和信息系统评价建设信息安全体系两个角度对信息安全进行控制。1999年对安全管理标准BS7799-1和BS7799-2进行了修订，新版本明确和强调了组织或单位在信息安全管理和体系建设中承担的责任。

进入21世纪，随着计算机网络广泛推广，信息安全得到世界范围充分重视。BS7799-1，BS7799—2逐渐被广泛应用和认可，分别在2000年和2005年被国际标准组织(International Organization for Standardization ，ISO)采纳为国际标准，即BS7799-1成为国际标准ISO / IEC l7799：2000《信息技术——信息安全管理实施规则》；以BS7799—2为基础修订完成ISO / IEC 27001：2005《信息安全管理体系规范》。

1.2 我国的信息安全标准建设情况

我国积极引进国际标准，同时结合我国信息安全的实际情况，研发和制定了一系列的信息安全标准，其中大部分是借鉴和引用了国际公认较为成功的安全标准[2]。

表1　我国信息安全标准的引用情况

我国标准	引用的国际/国外标准
GB/T 18336-2001 《信息技术安全性评估准则》	ISO/IEC 15408
GB 17859-1999 《计算机信息系统安全保护等级划分则》	TCSEC
GB/T 22080-2008 《信息安全管理体系要求》	ISO / IEC 27001：2005

2 军用信息安全标准建设

通过多年的建设，我军已经形成了一定规模的信息安全标准，从计算机安全，网络体系建设，涉密信息系统等许多信息领域都制定了相应的安全评估准则、安全要求及安全体系结构，通用技术，保密要求等。具体制定的部分标准如下：

- GJB 2255-95《军用计算机安全术语》
- GJB 2646-96《军用计算机安全评估标准》
- GJB 3395-98《军用网络安全评估标准》
- GJB 5023-2001《军用数据库安全评估标准》
- GJB 3343-98《军用计算机网络安全体系结构》
- GJB 5095-2002《信息技术安全通用技术》
- GJB 4603-93《军队涉密信息系统安全保密要求》
- GJB 1281-91《军队指挥自动化计算机网络安全要求》

这些信息安全标准已经形成了初步的我军信息安全标准体系，主要从基础标准，技术和机制标准，评估标准和具体安全要求四个方面建设和发展信息安全标准的。

表2　我军信息安全标准体系

基础标准	技术和机制标准	评估标准	具体安全要求标准
GJB 2255-95	GJB 5095-2002	GJB 2646-96	GJB 4603-93
		GJB 3395-98	GJB 1281-91
		GJB 5023-2001	

信息安全标准体系的作用主要在两个方面。一是确保了信息安全产品的整体信息保密性，完整性和可用性，严格分层的安全体系架构推动了各层次信息安全产品的互联互通，提高信息安全产品适用性；二是建立了信息产品或系统的控制和评价体系，主要集中在准入和评价两个方面，设定信息产品或系统的信息安全最低要求，严格信息安全最低要求，同时倡导信息安全评价，推动高安全产品的推广使用，提高整体信息安全保证，也有助于信息安全国家战略实施。[3]

针对上述最重要的信息安全标准GJB 2646-96《军用计算机安全评估标准》，主要从美国的TCSEC标准为蓝本制定的，主要针对的是军用计算机的安全评估，主要面向操作系统，也可以作为其他需要作安全评估的标准[4]，基于GJB 2646之上的还包括数据库安全评估标准和网络的安全评估标准。

GJB 2646按照处理的信息等级和采取的相应措施将系统安全分为四等八级别[4]：

D级为最低级别；

C级为自主保护，又分为C1自主安全保护，C2可控访问保护；

B级为强制保护，又分为B1具有标号的安全保护，B2结构化保护，B3安全域；

A级为验证保护，又分为A1验证设计，超A1最高标准。

同时强制规定军用软件设计应当达到B2以上，同时也对软件的等级评定做了严格操作规定。

3 军用信息安全标准改进建议

在分析国内外信息安全标准和我军信息标准基础上，我们

应当清楚地认识到,我军的信息安全标准的建设,从体系完整性,及时更新,独立创新等很多方面存在不小差距,具体说来,有以下几点:

1)标准制定落后于信息安全的发展需求

我军现行的信息安全标准大多是上个世纪90年代制定的,而近十年是信息化高度发展的十年,也是信息安全标准高速发展的十年,我们的很多标准已经落后于时代发展。如我军当前广泛推行的GJB2646标准以1985年的TCSEC标准为蓝本制定。

2)标准体系亟待完善

分析我军的信息安全体系,对比我国当前的信息安全体系,存在两个主要的问题:

一是缺乏信息安全管理的标准。在现实信息社会中,80%的信息安全事故来自人们对网络安全知识的缺乏和内部管理的漏洞[5],如果只是从技术角度加强信息安全,是不足够的。针对我军信息结构和保密特点,吸收已有信息安全优秀案例成果建立建设信息安全管理方法,规范信息安全管理过程方法,形成一套行之有效的实施标准是我军信息安全建设当务之急。

二是对于具体信息系统的安全要求多,缺乏严格的统一安全标准。没有统一的安全标准,当不同的信息系统在互联互通时,增加了网络安全认证等问题。

3)标准制定缺乏自主性

我军标准制定主要是根据国际或国家的相应标准,对我军实际情况分析不够。例如我军的GJB3433-98《军用计算机网络安全体系结构标准》就是和ISO的OSI的7层协议结构完全相同。

总之,随着计算机技术的深入发展,"互联网+"国家战略的不断推进,信息安全在我国重要领域特别在军队越来越当引起重视。信息安全标准的建设是信息安全的整体性,基础性工作,在研究国内外信息安全相关标准及其发展历程基础上,研究了现行我军信息安全特点,对后期我军信息安全标准建设发展重点提出了合理化建议。

参考文献:

[1] 曾海雷.信息安全评估标准比较的研究和比较[J].计算机与信息技术,2007(5):1228-1230.
[2] 向天荣.GB 17859标准的等级评定[J].计算机工程,2005,11(4):57-60.
[3] 周楠.网络与信息安全评估标准综述[J].电脑知识与技术,2007(9).
[4] GJB 2646-96 ,军用计算机安全评估标准[S].
[5] 但丽云.ISO27001:2005标准的实施步骤与控制重点[J].中国认证认可,2008,42(3):43-45.

(上接第15页)

运行过程中,电脑会自动将信息资料传输到存储设备中,然后计算机系统会分析这些信息所运行的环境是否安全,如果存在安全隐患,系统会自动将信息反馈到操作端,从而保护数据信息不被更改。所以,数据加密对于系统内外部的安全管理具有重要的保护作用,网络数据库用户应当通过访问权限或设定口令字等方式对关键数据进行加密保护。

2.2 加密软件中应用数据加密技术

在计算机运行过程中,数据加密技术也是防范黑客攻击与病毒的有效措施。人们在使用计算机过程中,病毒或黑客随时会发动攻击,而该项技术能够阻断病毒或黑客进攻的路径。当技术人员对文件进行加密过程中,一旦发现存在病毒,就会迅速采取措施,实施隔断,阻止病毒扩散。由此可知,若想使计算机软件良好运行,必须要注意运用数据加密技术。

2.3 电子商务中的数据加密技术

随着以阿里巴巴为首的网上购物的风行,电子商务与网络已成为不可分割的整体,而网络的开放性又给电子商务带来了不可估量的影响,甚至是安全威胁。为更好地促进电子商务与网络之间的协调、良性发展,本文重点关注电子商务中的数据加密技术,尤其是SST和SSL安全协议,要进一步论证这两个协议的科学性和合理性。

2.4 专用虚拟网络中应用数据加密技术

在当前,数据加密技术的运用范围很广,甚至将触角伸进一些企事业单位的局域网中。而不同单位的局域网,需要的数据加密技术专业路线却大致相同,即充分路由器在虚拟网络中保存各种数据,再经路由器中的硬件采取加密措施,再通过网络将加密后的数据传递出去,其他路由器接收后,其中的硬件会自动实施解密步骤,保证接收者能够阅读加密数据内容。

3 结语

计算机网络技术的快速发展,给人们的生活、学习和工作都带来了很多的便利,我们在享受计算机网络系统的便捷高效时,也要充分认识到计算机网络系统面临的安全问题。而信息加密技术对于网络信息安全性的保护已经越来越重要,因此在实际应用中,应根据用户的需求进行不断的研发、革新,来满足人们对信息安全的需求,有效维护网络环境的安全。

参考文献:

[1] 潘珊珊. 浅析计算机网络信息加密技术[J]. 科技资讯, 2013(33).
[2] 杨建才. 对计算机网络安全中应用信息加密技术的研究[J]. 计算机光盘软件与应用, 2012(3).
[3] 庞治年, 邹德金. 关于计算机网络信息加密技术的探讨[J]. 信息安全与技术, 2012(3).
[4] 王蕾, 孙红江, 赵静. 数据加密技术在计算机网络安全领域中的应用[J]. 通信电源技术, 2013(2).
[5] 李红丽. 计算机网络安全隐患分析和数据加密技术的应用[J]. 九江学院学报:自然科学版, 2012(4).