学校编码：10384　　分类号＿＿＿＿密级＿＿＿＿

学号：X2011230229　　UDC ＿＿＿＿

工　程　硕　士　学　位　论　文

检察工作信息化安全保障系统的分析与设计

Analysis and Design of Informatization Security Protection System in Procuratorial Work

何　涛

指 导 教 师:　王备战教授

专 业 名 称:　软件工程

论文提交日期:　2013 年　月

论文答辩日期:　2013 年 5 月

学位授予日期:　　年　月

指　导　教　师：＿＿＿＿＿＿

答辩委员会主席：＿＿＿＿＿＿

2013 年 4 月

厦门大学学位论文原创性声明

本人呈交的学位论文是本人在导师指导下，独立完成的研究成果。本人在论文写作中参考其他个人或集体已经发表的研究成果，均在文中以适当方式明确标明，并符合法律规范和《厦门大学研究生学术活动规范（试行）》。

另外，该学位论文为（　　）课题（组）的研究成果，获得（　　）课题（组）经费或实验室的资助，在（　　）实验室完成。（请在以上括号内填写课题或课题组负责人或实验室名称，未有此项声明内容的，可以不作特别声明。）

声明人（签名）：

年　　月　　日

厦门大学学位论文著作权使用声明

本人同意厦门大学根据《中华人民共和国学位条例暂行实施办法》等规定保留和使用此学位论文，并向主管部门或其指定机构送交学位论文（包括纸质版和电子版），允许学位论文进入厦门大学图书馆及其数据库被查阅、借阅。本人同意厦门大学将学位论文加入全国博士、硕士学位论文共建单位数据库进行检索，将学位论文的标题和摘要汇编出版，采用影印、缩印或者其它方式合理复制学位论文。

本学位论文属于：

（　　）1.经厦门大学保密委员会审查核定的保密学位论文，于　　年　　月　　日解密，解密后适用上述授权。

（　　）2.不保密，适用上述授权。

（请在以上相应括号内打“√”或填上相应内容。保密学位论文应是已经厦门大学保密委员会审定过的学位论文，未经厦门大学保密委员会审定的学位论文均为公开学位论文。此声明栏不填写的，默认为公开学位论文，均适用上述授权。）

声明人（签名）：

年　　月　　日

摘要

随着全国各级检察机关基础网络平台建设的基本完成，信息化为检察机关提升司法水平、增强法律监督能力提供了很大的帮助。然而，事物往往是伴随矛盾而至的，信息系统暴露出越来越多的漏洞，信息安全问题日显严峻。检察机关作为国家的法律监督机关，平时工作涉及各种国家秘密、检察工作秘密，又产生国家秘密和检察秘密。因此，检察工作信息安全保障体系的建设显得尤为紧迫，建设一个可靠的检察系统信息安全保障体系日益重要。

本文着眼于检察工作信息化的不断发展，围绕检察工作信息安全保障体系建设的紧迫要求，在简要介绍国内外信息安全发展的现状后，分析了检察机关信息系统面临的安全问题及需求，讨论了信息安全的几个基本的威胁种类，也介绍了目前应对这些威胁的一些较常用的技术，如 ACL 技术、防火墙、入侵防御技术、PKI 技术以及 RSA 算法的加解密原理等。

在对检察信息化安全保障系统的保密需求、业务需求、非功能性需求进行认真分析的基础上，围绕检察内网、政务内网和外网的需求对安全系统进行综合全面的框架设计，涵盖了物理环境安全、网络安全防护、系统安全防护、应用安全、安全管理等信息系统安全各个层面。而由于检察专网的安全防范在检察工作中更加重要，因此本文着重研究并尝试搭建全国统一的检察系统专用身份证书管理系统，对证书管理系统的 CA、RA 以及 CRL 进行了一一设计和部署，并通过 RSA 算法制作了检察系统的身份证书。此外，还试图建立一套严格的检察系统信息网络安全管理机制，明确的安全管理人员和安全管理体系，作为检察信息安全保障系统的保障。

最后，本文探讨了此安全保障系统将来还需进一步完善的地方，展望了检察工作信息化建设的未来。

关键词：检察工作；信息化；安全保障系统

Abstract

As the basic completion of the fundamental network platform construction in the Procuratorial organs, information has a great role in enhancing the judicial level and strengthening the legal supervision ability. However, things are often accompanied with the conflicts, information system exposes more and more loopholes, information security problem become more and more serious. Procuratorial organs are the legal supervision organs of the state, it's daily work involves state secrets and Procuratorial secrets, again produces new state and Procuratorial secrets. Therefore, the construction of Procuratorial information security assurance system is particularly urgent, the construction of a reliable Procuratorial system information security assurance system is also becoming more and more important.

This dissertation focuses on the continuous development of information technology in Procuratorial work, and around the urgent requires of the security assurance system, introduces the present development situation of information security in domestic and foreign, after that, it analyzes the problems and needs of the Procuratorial information system security, then it discusses a few basic types of threat to information security and the commonly used technology to deal with these threats, such as the ACL technology, firewall, intrusion prevention technology, PKI technology, and decryption principle of RSA algorithm and so on.

On the basis of serious analysis of confidentiality requirements, professional requirements and non-functional requirements of Procuratorial information security system, the dissertation comprehensively design the system's framework around the needs of Procuratorial Intranet, government intranet and external network, the framework covers all kinds of levels include the physical environmental security, network security, system security, application security and security management. Due to the Procuratorial intranet security is more important in the Procuratorial work, so this dissertation try to set up the national united special identity certificate management module, design and deploy the CA, RA, and the CRL of the certificate management module respectively, and made the identity certificate of the Procuratorial module through the RSA algorithm. In addition, this dissertation try to establish a set of strict Procuratorial security management mechanism system, to explicit safety manager and safety management system, so as to guarantee Procuratorial information security system.

Finally, this dissertation discusses the problem about how to further perfect the

security system in the future and the prospect of the Procuratorial information system construction.

Keywords: Procuratorial work; Informatization; Security Guarentee System

目录

Contents

第一章 绪 论

1.1 选题背景及研究意义

随着信息技术的飞速发展，信息化时代的到来，信息资源日益成为重要生产要素、无形资产和社会财富，信息和信息技术在社会经济文化发展中的作用越来越大，已经渗透到人类社会活动的各个方面、各个领域。这是当今最先进和强大的生产力，成为推动经济社会变革的重要力量，也将极大地推进人类文明的进程，把人类带入一个崭新的信息化时代。

21 世纪的检察事业需要现代化，而检察事业的现代化最主要的是实现检察信息的现代化。向科技要战斗力，依靠检察科技进步和提高检察干警素质已成为检察工作的发展方向。而今各级检察机关正在进行的科技强检工作就是检察工作与现代信息技术的有机结合，即以信息网络技术为基础，以电子检务为形式，以公平正义为目标，不断改革完善检察决策机制和工作机制，构建现代检察工作模式。

可以说检察工作的方方面面均与信息化建设息息相关，发现犯罪离不开信息，证明犯罪离不开信息，进行法制宣传、预防犯罪离不开信息，检察决策、行政办公同样离不开信息。随着全国各级检察机关基础网络平台建设的基本完成，信息化为检察机关提升司法水平、增强法律监督能力提供了很大的帮助。然而，事物往往是伴随矛盾而至的，信息系统暴露出越来越多的漏洞，信息安全问题日显严峻，网站木马、黑客入侵和篡改网站的安全事件频繁发生，严重影响了信息化建设的正常运转。而检察机关作为国家的法律监督机关，平时工作涉及各种国家秘密、检察工作秘密，又产生国家秘密和检察秘密。因此，对于检察机关来说，信息安全保障体系的建设显得尤为紧迫，信息安全因此也日益成为检察机关上下愈加关注的问题，建设一个可靠的检察系统信息安全保障体系日益重要。

1.2 研究现状

1.2.1 国外研究现状

80 年代中期，美国国防部为适应军事计算机的保密要求，在 70 年代的基础理论研究成果计算机保密模型的基础上，制定了“可信计算机系统安全评价准则”（TCSEC），其后又对网络系统、数据库等方面做出了系列安全解释，形成了安全信息系统体系结构的最早原则。至今美国已研制出的符合可信计算机系统安全评价准则要求的安全系统（包括安全操作系统、安全数据库、安全网络部件）多达 100 多种。90 年代初，英、法、德、荷四国针对 TCSEC 准则口令保密性的局限，提出了包括保密性、完整性、可用性概念的“信息技术安全评价标准”（ITSEC）。其后由美国国家安全局和国家技术标准研究所以及加、英、法、德、荷五国共同提出了“信息技术安全评价通用标准”（CC），确立了国际标准，该标准对安全的内容和鉴别给予了更完整的规范，为用户对安全需求的选取提供了充分的灵活性[1]。

1.2.2 国内研究现状

我国在系统安全的研究与应用方面与先进国家和地区存在很大差距。近年来，在我国进行了安全操作系统、安全数据库、多级安全机制的研究，但由于自主安全内核受控于人，难以保证没有漏洞。而且大部分工作都以美国 1985 年的 TCSEC 标准为主要参照，所开发的防火墙、安全网关、黑客入侵检测系统、安全路由器等产品和技术，主要集中在系统应用环境的较高层次上，在完善性、规范性、实用性上仍存在许多不足，特别是在多平台的兼容性、多协议的适用性、多接口的满足性方面存在很大距离，其理论基础和自主的技术手段也有待发展和强化。尽管如此，我国的系统安全的研究与应用已经起步，具备了一定的基础和条件。1999 年 10 月发布的“计算机信息系统安全保护等级划分准则”，为安全产品的研制提供了技术支持，也为安全系统的建设和管理提供了技术指导。2007 年全国重要信息系统安全等级保护定级工作电视电话会议召开之后，国家重要信息系统的运营使用单位及其主管部门认真组织积极落实等级保护工作，目前基本完成了全国重要信息系统的定级工作任务。围绕着国家颁布的文件和标准，各重点行业也加强了对等级保护工作的研究力度，颁布了一些行业文件和标准。在制定各项标准的同时，国内也有不少学者在研究各项安全防护技术，但大多数都限于将国外的各项技术应用于国内的实践环境当中。

1.2.3 存在的问题

检察机关计算机信息网络从 2000 年开始规划建设，至今已建立了从最高人民检察院、省检察院、市检察院、县（市、区）检察院的检察机关三级专线网络。最高检至省院的网络为第一级网，各省院之间的互联则通过最高检中转；省院与各市级院之间相连的网络为第二级网，各市院之间的互联则通过省一级院中转；市级院至县级院的网络为第三级网，各县院之间的互联则通过市一级院中转。全国检察机关专线业务网络在性质上属于涉密业务专网，整个网络和 Internet 等非涉密网络实现物理隔离。而在原有二、三级网络系统的建设过程中，基于分步建设、不断完善的总体建设方针，高检院并未对整个网络的安全保密系统建设做统一规划和考虑，随着二、三级网络中应用系统的逐步推广使用，如何有效保障整个网络中涉密信息的生成、传输、存储、访问的安全保密性，就成为现阶段整个系统建设中急需解决的首要问题。

总体来说，当前检察网络信息系统的信息安全比较薄弱，主要表现在以下几个方面：

1、宏观上国家信息安全的法律法规不健全，国家信息安全基础产业和基础设施自主性差，缺少自已的核心技术。

一方面，国家在信息安全方面法律缺乏，现有法律法规体系存在诸多不完善的地方。如：在涉及网络安全、电子合同、电子证据、计算机犯罪等方面，法律法规已然跟不上信息技术发展的需要。另一方面，国家信息安全基础产业和基础设施建设的自主性差。目前，我国计算机硬件、通信设备制造业的基础集成电路芯片主要依靠进口，系统软件、支撑软件基本上是国外产品。长期缺乏自主技术和产业，导致中国目前在互联网核心控制水平上没有起码的自卫能力，即所谓“制网权”。

2、检察机关自身信息安全管理问题突出。

信息安全管理包括三个层次的内容：组织建设、制度建设和人员意识。目前检察机关信息系统的安全管理归检察技术部门负责，但全国大部分基层检察院建立的规章制度可落实性差，甚至没有规章制度；领导对信息安全也还不够重视，没有形成群防群治的意识。信息安全的管理人员上还存在多人负责、责任到人、任期有限等诸多问题。同时，信息安全意识的教育和培训也还远远不够。

如形同虚设的简单口令问题。在检察系统中，有近 60%的电脑未设置开机密码、系统用户名密码或电子邮箱密码等等，同时即使在设置了密码口令的电脑中，绝大部分还是原始密码或仅由几位简单的阿拉伯数字或字母构成，设置的口令过短，口令使用周期过长等。这就为窃密者提供了一条通过建立一个空连接，悄悄进入远程计算机的技术便利。lockdown.com 曾公布了一份采用“暴力字母破解”方式获取密码的“时间列表”，分析显示：如果用一台双核电脑破解密码，瞬间就能搞定 6 位数字密码(如银行密码)，8 位需 348 分钟，10 位需 163 天，如果混合使用数字和大小写字母以及标点等，6 位耗时 22 小时，8 位需 23 年。再如防不胜防的泄密载体。随着信息科技的高速发展，移动存储介质的种类日趋多样，软盘、优盘、移动硬盘、MP3、MP4 等在工作中的应用十分广泛。特别是优盘，由于其便于携带、方便存取，在我们的工作中随处可见，检察工作信息均可以存储在一个小小的优盘中。不少人用它私自下载和保存涉密文件，还有的人将工作优盘带回到家庭电脑中进行检察工作信息处理，甚至带着涉密的优盘逛街、聚会、出游，一旦丢失，后果不堪设想。除了这些泄密隐患外，优盘一旦被植入病毒，特别是“木马”病毒后，如果接入检察涉密计算机，涉密文件就会在不知不觉中被别有用心者窃取。

3、重安全技术，轻安全管理，缺乏系统管理的思想。

有些干警对信息安全工作缺乏必要的网络安全知识和概念，片面强调检察信息网是检察系统的专用网，只要不与互联网联通或不将涉密信息放在互联网上就不存在网络安全问题；有的单位对网络安全的认识有偏差，认为即使有网络安全问题，只要买一些防火墙、杀毒软件装到电脑上，从技术上堵住安全漏洞，防止外来攻击，网络就安全了，完全忽略内部自身的信息安全管理；还有些单位对信息安全是一个动态的持续改进过程认识不足，仍采取传统的静态管理办法，出了问题才去想补救的办法。这些问题不仅严重影响检察机关的信息安全防范能力，而且会影响整个检察机关的信息化进程。

如有机可乘的系统漏洞问题。应用软件或操作系统软件在逻辑设计上的缺陷或在编写时产生的错误，这些缺陷或错误如果被他人利用，可以获取远程计算机的控制权，轻易窃取远程计算机中的检察工作中相关重要资料。尽管通过打补丁的方式可以缓解由漏洞引起的问题，但是大多数干警没有及时打补丁的意识，或者根本不会打补丁，造成计算机系统长期存在系统漏洞，这就给了一些别有用心人的可乘之机。