北京交通大学

实验报告

中 文 题 目： 保 密 检 查 技 术

学　　院：计算机学院

专　　业：信息安全

姓　　名：张 向 宇

学　　号：**18281059**

指导教师：

2020 年 **7** 月 **3** 日

目录

一、实验目的

（1）通过亲身实践深入理解并掌握保密技术检查的相关工具和技能
（2）通过理解并掌握保密技术检查来深入理解保密工作的流程和重要性
（3）学习编写设计保密检查用表，掌握保密检查工作能力

二、实验环境

1、软件环境：

操作系统：Microsoft　Windows7 Professional 64bit
软件环境：智华计算机终端保密检查系统 涉密单机版 V1.0 3161

2、硬件环境：

平台：X86_64 兼容 PC 机
CPU：AMD Ryzen 4800HS
GPU：NVIDIA RTX2060 MAX-Q
RAM：16GB DDR4 RAM

三、实验工具简介

计算机终端保密检查系统是在安全保密检查类软件研发的基础上，严格按照国家对计算机安全保密检查的技术要求，针对各级保密局和各级党政机关、科研院所、大中型企业、军工企业等，进行安全保密检查和防范工作的安全产品，该产品均已通过国家保密科技测评中心测评。

该系统从使用场景上分为单机版、网络版。单机版用于单机检查，网络版则基于机关、单位的网络，实现保密检查网络化和常态化，提高保密检查效率，降低检查成本。

检查对象主要包括文件对象检查、计算机使用痕迹、安全策略配置、系统安全等。检查装备结合国家现行标准和技术要求，对涉密和非涉密计算机的安全保密状况给出准确、全面、有效的评价。

计算机终端保密检查系统为保密管理部门和党政机关单位计算机信息系统进行日常的安全保密检查提供了强大的技术手段，及时发现违规行为、失泄密漏洞和安全隐患，加强防护措施，做到及时有效的防止失泄密事件的发生，保障了国家秘密的安全。

主要功能：

◆ 对被检查计算机的本机信息进行采集，其中包括被检主机的主机名、IP 地址、操作系统的型号、用户列表、MAC 地址等；
◆ 能够收集调出该机的相关上网信息；
◆ 恢复被删除的上网记录，支持硬盘分区的所有格式；
◆ 收集最近用户使用过的文档信息，包括用户已删除的文档；
◆ 通过文件名或者文件内容查找被检计算机现存的文件；

◆ 通过内容关键字查找已被删除的文件在扇区中的文字碎片信息，快捷判定是否处理过违规或敏感内容；
◆ 发现 MSN、网络蚂蚁、QQ 等互联网常用工具的最后登陆时间，辅助确认违规上网行为的发生；
◆ 发现 Modem 的最后启动时间，当时的用户信息；
◆ 可以调出被检查电脑的移动存储介质的使用记录；
◆ 收集系统安装的补丁信息、安装时间等；
◆ 软件自身具有硬件绑定保护，防止不法人员非法复制利用；
◆ 软件所有模块为完全自主开发，预留了二次开发接口；
◆ 可以收集违规用户的违规信息，并生成报表；
◆ 可为具有执法资格的检查部门提供违规痕迹擦除模块。
系统特性描述
◆ 设计灵活、使用简单、用户界面友好；
◆ 搜集信息全面、高效、准确；
◆ 稳定性好，自身安全性高；
◆ 预留接口，方便二次开发；
◆ 对被检测主机使用旁路检测技术，不会对被检计算机造成危害。

计算机终端保密检查系统使用形态：

使用时直接将装有本系统程序的移动存储介质载体接入被检查计算机，运行程序即可获得检查报告。

常见问题和注意事项：

（1）在 WIN_PE 系统下，由于检查软件获取的是 PE 系统的相关信息，因此，会有一些服务项、进程项、操作项检查不到信息，所以请在正常系统下运行涉密计算机安全保密检查软件

（2）在 Windows Vista 和 Win7 系统下运行程序时，若 UAC（User Account Control：用户帐户控制）开启，请选中程序点击鼠标右击，选择其中的“以管理员身份运行”。若系统中 UAC 未开启，则可以直接运行程序。

四、实验内容

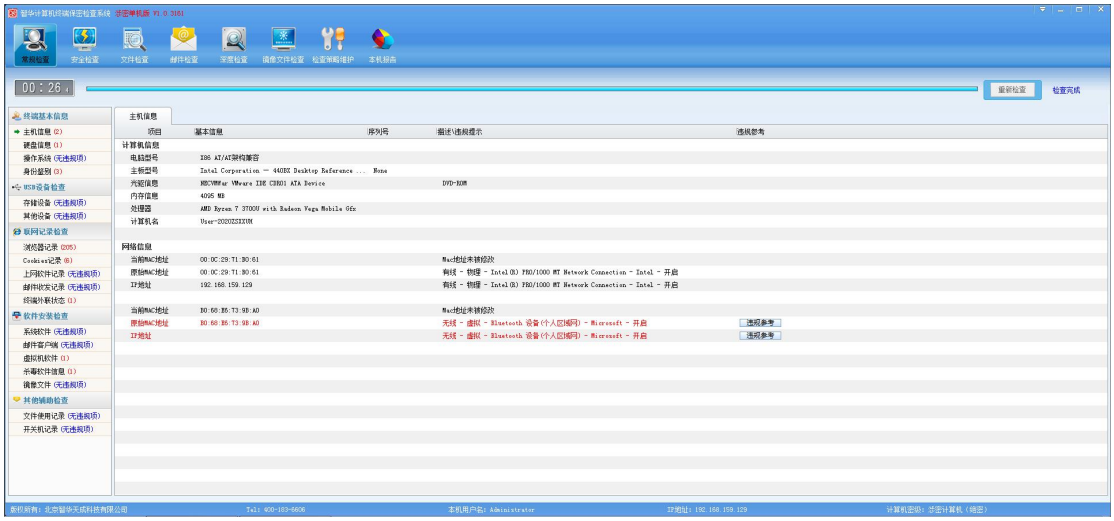
（1）常规检查
（2）安全检查
（3）文件检查
（4）邮件检查
（5）深度检查
（6）镜像文件检查
（7）检查策略维护
（8）本机报告

五、实验步骤

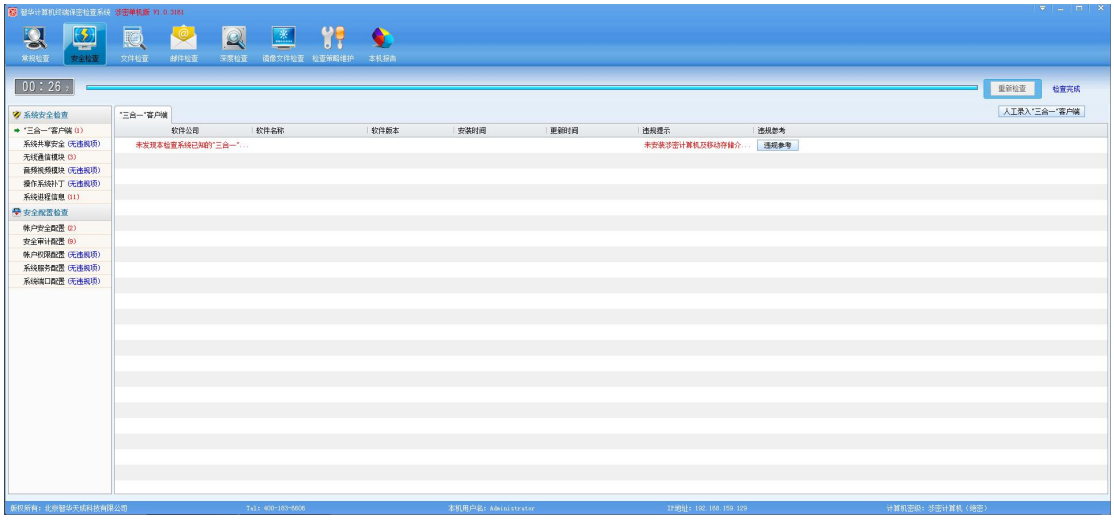
首先在计算机中运行终端保密检查软件，设定本机运行密级

（1）常规检查

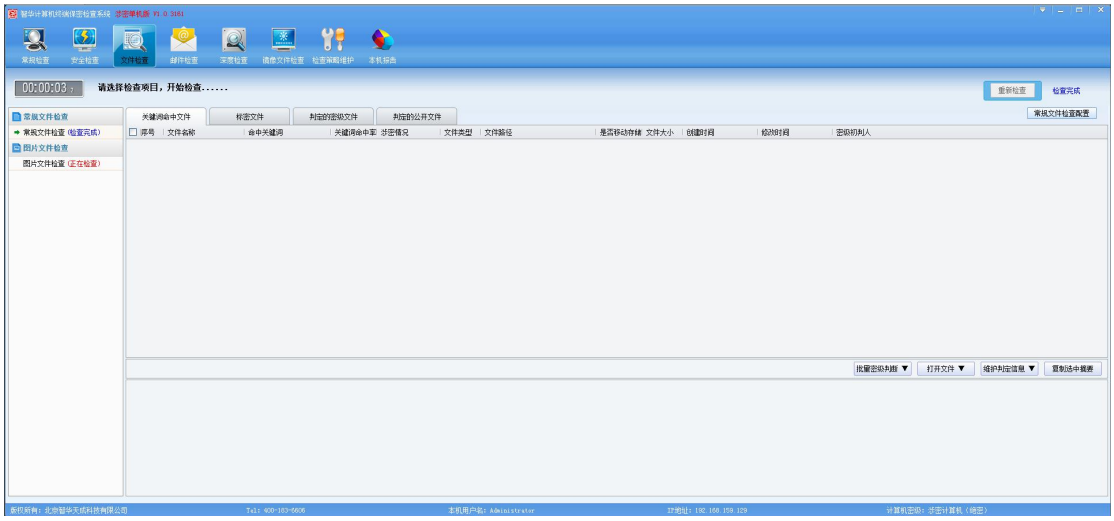
选择常规检查功能，运行即可获得系统的常规检查报告



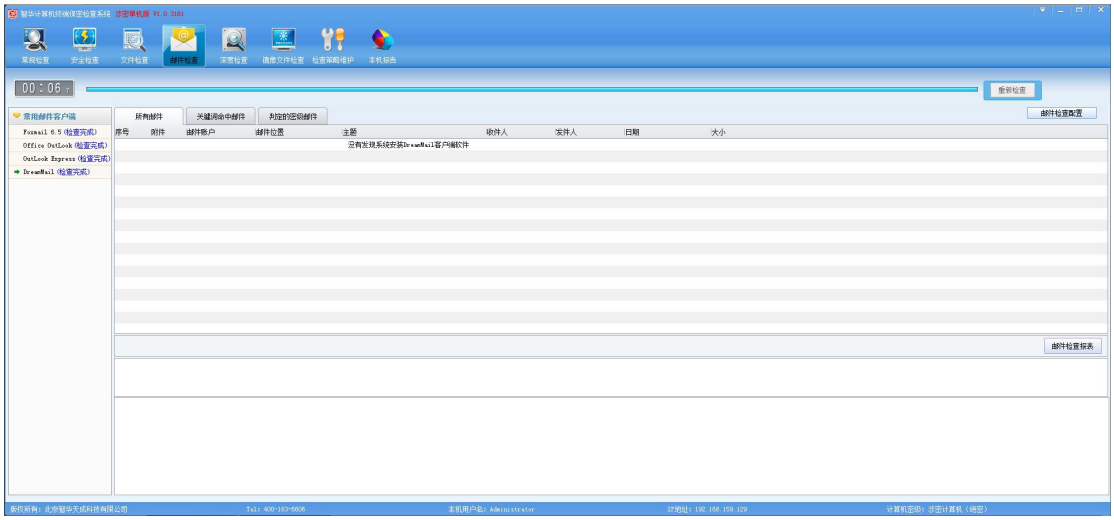
（2）安全检查



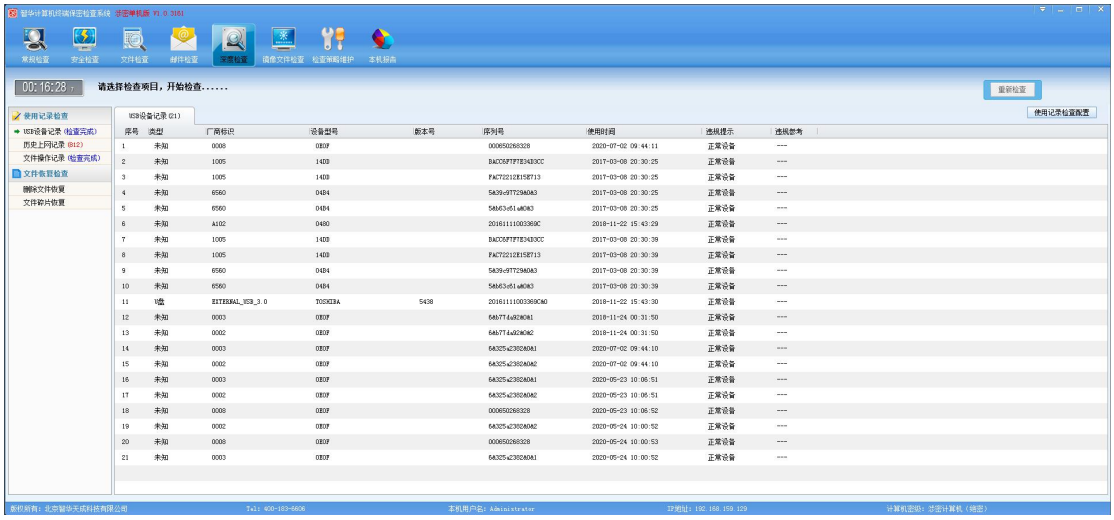
（3）文件检查



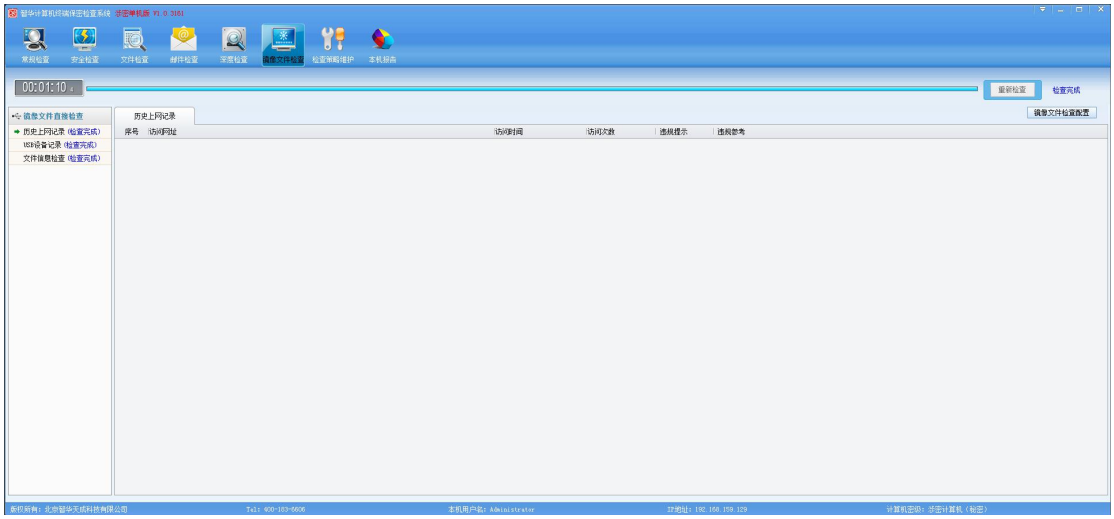
（4）邮件检查



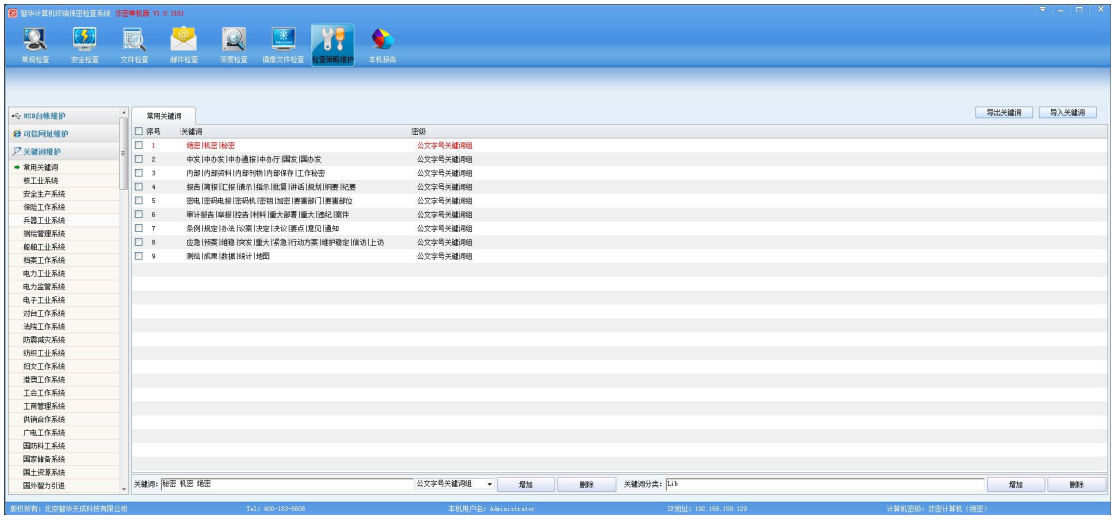
（5）深度检查



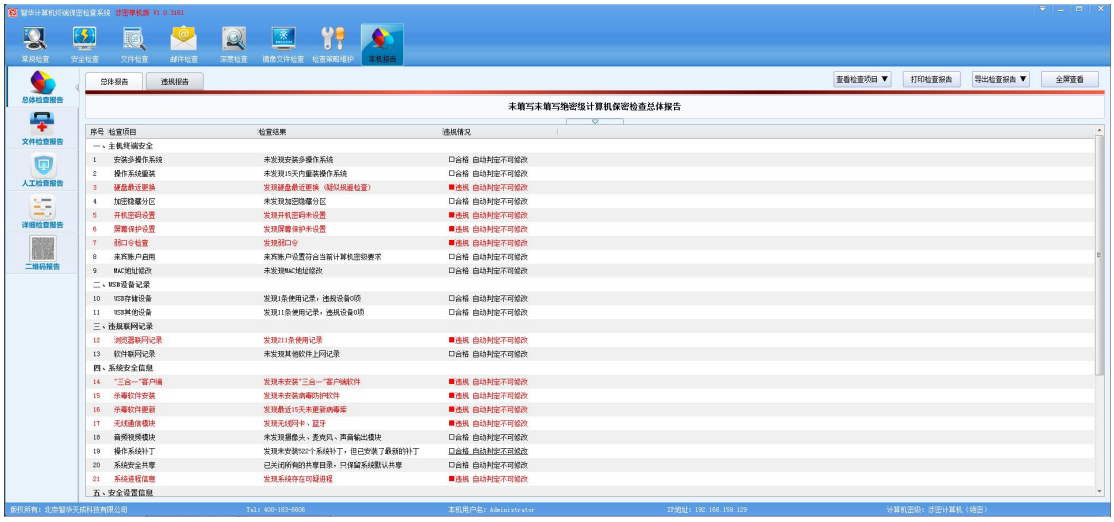
（6）镜像文件检查



（7）检查策略维护



（8）本机报告



六、实验思考与收获

（1）实验思考

保密检查技术一门具有高度专业性的技术。有关部门在日常保密工作中应加大保密技术

检查力度，遵照国家有关法规和标准要求，根据单位涉密信息系统的实际特点，建立健全保密监督检查办法，培养一支专家型技术检查团队，制定出针对性强的技术检查条款，配合基础性的保密管理检查要求，定期对单位进行全方位、多层次的保密“体检”，才能保证密监督检查的科学性、合理性、全面性和有效性。

有了专业科学的保密技术检查团队，还需要有相应的规章制度来保证。完善的保密管理规章制度是做好保密技术检查工作的前提。保密管理以保密技术为依托，保密技术靠保密管理来保障的新的涉密信息系统管理工作模式正在逐步产生、发展并最终走向成熟，涉密信息系统安全保密检查作为一个复杂的系统性工程，保密管理检查和保密技术检查是相辅相成的。

（2）收获

1、学会使用了基本的保密技术检查工具，对于保密技术检查工作的基本流程有了较为清晰的概念

2、通过查看自己计算机的保密技术检查报告，对于如何更好的改进自己计算机的保密性能有了显著的认知提升。立即开始了自检自查，提升了自己对于计算机安全的能力

3、学会了如何设计保密检查用表，根据设计保密检查用表，对于每一个检查项目的来源、作用与改进方法有了深刻的认识，增加了自己的保密意识

七、设计保密检查用表

涉密计算机保密情况检查表

表一：基础信息登记表

序号	项目	信息
1	检查时间	
2	检查单位	
3	检查人	
4	行政区域	
5	被检单位	
6	单位类型	
7	被检部门	
8	被检人员	
9	计算机密级	
10	终端型号	
11	主机名称	
12	主板序列号	
13	主硬盘序列号	
14	Mac 地址	
15	IP 地址	
16	违规项目	
17	合格项目	
18	未检查项目	

表二：总体检查报告

（1）主机终端安全

序号	检查内容	检查结果	违规情况
1	安装多操作系统		
2	操作系统重装		
3	硬盘最近更换		
4	加密隐藏分区		
5	开机密码设置		
6	屏幕保护设置		
7	弱口令检查		
8	来宾账户启用		
9	MAC 地址修改		

（2）USB 设备记录

序号	检查内容	检查结果	违规情况
1	USB 存储设备		
2	USB 其他设备		

（3）违规联网记录

序号	检查内容	检查结果	违规情况
1	浏览器联网记录		
2	软件联网记录		

（4）系统安全信息

序号	检查内容	检查结果	违规情况
1	“三合一”客户端		
2	杀毒软件安装		
3	杀毒软件更新		
4	无线通信模块		
5	音频视频模块		
6	操作系统补丁		
7	系统安全共享		
8	系统进程信息		

（5）安全设置信息

序号	检查内容	检查结果	违规情况
1	本地安全配置		
2	系统服务配置		
3	系统端口复制		

（6）文本文件检查

序号	检查内容	检查结果	违规情况
1	判定的越级存储文件		
2	关键词命中文件		

（7）图片文件检查

序号	检查内容	检查结果	违规情况
1	判定的越级存储文件		
2	关键词命中文件		

检查结果说明：

整改处理意见：

表三：人工检查报告

序号	检查内容	检查结果	违规情况
1	本年度是否出现过的泄密事件，并及时向同级保密管理部门报告		
2	是否配备经过测评认证的保密技术检查装备工具，且为最新版本		
3	是否定期开展计算机信息系统的自检自查，并建立自查台帐		
4	是否设立保密工作机构，并有专人负责保密工作		
5	保密工作所需经费是否列入年度财政预算或者收支计划		
6	涉密场所、会议及所涉及的设施、设备是否符合保密要求		
7	保密要害部门、部位是否采取人防、技防、物防等防护措施		
8	涉密人员上岗、在岗、离岗是否建立相关管理制度并签订保密承诺书		
9	是否建立宣传报道和		

	信息公开保密审查制度，并有相关记录		
10	涉密网络设备及服务器是否直接或间接与互联网或公共网络连接		
11	处理涉密信息打印机多功能一体设备是否与公共电话线连接		
12	显示器和主机是否正确张贴密级标识及标明基本配置和责任人		
13	中心机房是否采用有效的机械锁具、IC 卡和生理特征门控措施		
14	所有设备是否按照涉密非涉密分类安放，并满足相关要求		
15	打印机、制图机等系统输出设备是否放在公共区域		
16	显示器、投影机等显示输出设备是否面对门、窗、玻璃墙摆放		
17	涉密信息存储介质是否存放在安全场所，并采取了安全保密措施		
18	涉密设备借用、外出、归还是否有登记记录		
19	涉密设备维修是否有人员陪同、维修的相关记录		
20	涉密设备报废是否有设备存储硬件和固件销毁，并有最终去向等相关记录		
21	是否通过技术手段控制可移动存储设备的非授权接入		
22	是否正确配备使用电源隔离插座、视频干扰器		
23	终端计算机及设备是		

	否进行准确分类定级		
24	终端计算机及设备是否具有完善的台账管理，并与实际相符		
25	终端计算机是否安装必备的应用软件		
26	终端计算机是否安装禁用的应用软件		

检查结果说明：

整改处理意见：

最终评分等级：

计算机责任人（签字）：　　主管领导（签字）：