北京交通大学

调查报告

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

摘要：随着人类进入信息化时代，人们生产生活的信息已经从依附与实体的纸张逐渐转换成了依托于信息技术的数据流，与此同时涉密信息的存储、处理和传递方式也发生了巨大的变化，在新形势下的保密管理措施，只有通过技术层面上的排查和分析，才能发现和控制涉密信息系统中的各类安全隐患，解决管理工作和制度上的安全漏洞，确保国家秘密的安全。

保密检查是保密工作的重要内容和重要手段，在保密管理体系中具有重要地位和作用。保密技术检查工作是保密检查的重要组成部分，是传统意义上保密管理检查的有力补充和技术保障，加大保密技术检查频度和比重，是今后世界各国保密检查工作发展的必然趋势。

关键词： 信息安全；安全性；物理安全；保密技术

目录

一、调研目的

1. 深入理解保密技术检查的发展现状和实际应用
2. 调研国内和国外的保密技术检查情况，浅知敌我优劣

二、调研方法

这次调研，我主要通过查阅相关论文资料和公开的数据库和已解密的保密文案，例如美国中央情报局在线图书馆、美国联邦调查局资源库、中国国家保密局资料站、维基解密、克格勃资料库等。调研的方法主要采用：

1、结合上课老师内容，进行自身实践，总结工作经验

2、查阅相关文献资料，分析整理，得到真实记录

3、向相关专业人员请教，了解经验

三、调研内容

1、保密技术检查产业供应链自主化

要从根本上提高一个国家的安全保密技术防范能力，就要消除以靠外国技术及产品所带来的安全保密隐患，本质就是要自主化，独立自主研发并配备使用安全保密核心关键技术及产品。

处理器、操作系统、通信网络是当今信息化社会的基石，也是保密技术检查的基石，倘若根基出现了泄密漏洞，则一切的保密检查都是空中楼阁。

倘若涉密计算机或者信息系统使用了包含漏洞的处理器等芯片，将造成不可想象的后果。国际上不曾缺乏因为打印机等普通周边设备使用了外国含有后门漏洞的芯片造成泄密事件的案例，不久之前 Intel 的 Meltdown 与 Spectre 两个 CPU 漏洞暴露了就算在现代高度发达的处理器科技之下，依然存在巨大的安全漏洞。随着纳米工艺的突飞猛进，集成电路工艺的飞速发展，处理器等芯片中包含着数以百亿级的晶体管且结构从原来的二维化向三维立体化发展，传统的逆向工程或者芯片审查等技术手段，已经无法检查出芯片包含的后门或者漏洞等高危泄密隐患，解决这一问题的唯一道路就是实现处理器等芯片产业的完全自主化。美国因为有先发优势，自主化程度极高，在处理器等芯片领域不存在担忧存在高危泄密的隐患。

可喜的是我国的芯片自主化领域在“大基金”战略的支持下，取得了诸多突破性的进展，首台全面采用国产处理器的超算神威太湖之光问鼎世界超算榜首，标志了我国在高性能计算领域的国产化程度。龙芯 3A4000 系列标志着我国在自主知识产权的指令集领域取得了可用性的重大突破，在军工政府领域逐渐普及了使用龙芯处理器的计算机。兆芯的 KX-U6780 处理器标志在我国在民用主流 X86 处理器达到了行业领先水准，民用计算机全面采用国产处理器成为可能。长江存储和紫光存储等国产内存和存储芯片与主控芯片都在今年进入全面量产铺货阶段，全面解决了因为存储芯片受制于人可能存在的泄密问题。总而言之在处理器领域的供应链上我国前景良好。

倘若涉密计算机和信息系统采用了具有后门的操作系统，也将造成不可挽回的损失。操作系统是计算机的灵魂，是保密技术检查的载体。2013 年震惊世界的棱镜门事件，揭示了

包括微软、雅虎、谷歌、苹果等在内的 9 家国际巨头与美国国家安全局和联邦调查局的肮脏勾当，不得不让人怀疑在如今，微软的 Windows、谷歌的安卓、苹果的 iOS 和 macOS 已经占据了这个世界上 99%的计算机用户的操作系统，是否存在在操作系统中安插后门和恶意代码的可能性。2014 年央视就曾报道苹果承认 iOS 系统中留有后门，就算是一直自称保护用户隐私，从来没有与任何政府机构合作在自己的产品或服务中存在后门的苹果都存在后门，更不用说一直以来与美国政府关系良好，甚至参与过美国军事部门合作研究计划的微软和谷歌两家。具有完全自主知识产权可控的国产操作系统呼之欲出，然而在这一领域一直是我国信息产业的短板，所谓大量的国产操作系统都是基于 Linux 内核，虽然 Linux 是开源的操作系统内核，但是 OpenSSL 的漏洞告诉我们尽管是开源项目，依然可能存在大量的漏洞和后门，拥有一款全面掌控的国产内核是解决当前操作系统困局的关键。希望的曙光在于华为提出了自己的鸿蒙微内核计划和方舟编译器，走出了国产内核的关键一步，未来可期。与此同时，UOS 统一操作系统的开发计划也进行的如火如荼，在党政军领域未来计算机操作系统中将占据重要步伐。

倘若涉密计算机和信息系统采用了具有后门的通信网络系统，尽管有着上网不涉密，涉密不上网的准则，但是在保密系统里依然存在内部通信网络，通信网络将依然成为保密技术检查的重要战线。在通信网络这一块我国与美国成为平起平坐的竞争关系，甚至已经成为未来通信技术的引导者。华为在通信领域的成就世界瞩目，我国的通信网络供应链产业需要趁胜追击，在这领域成为我国高新技术企业的突破口，给我国其他信息产业争取战略空间，带动整个保密技术检查产业供应链自主化的飞跃。

总的来说，我国的保密技术检查产业供应链自主化程度还有很长的一条路要走，美国因为有先发技术优势，在这一领域暂时处于领先地位。

2、现有的计算机终端保密检查装备合格产品

（1）信工所计算机终端保密检查系统 V1.0
（2）中孚计算机终端保密检查系统 V1.0
（3）鼎普计算机终端保密检查系统 V1.0
（4）金密计算机终端保密检查系统 V1.0
（5）万里红计算机终端保密检查系统 V1.0
（6）智华计算机终端保密检查系统 V1.0
（7）华安保计算机终端保密检查系统 V1.0
（8）北信源计算机终端保密检查系统 V1.0
（9）朗威计算机终端保密检查系统 V1.0
（10）安华易计算机终端保密检查系统 V1.0
（11）天桥计算机终端保密检查系统 V1.0
（12）中安计算机终端保密检查系统 V1.0
（13）远望计算机终端保密检查系统 V1.0
（14）信果计算机终端保密检查系统 V1.0
（15）微锐计算机终端保密检查系统 V1.0
（16）博智计算机终端保密检查系统 V1.0
（17）蓝盾计算机终端保密检查系统 V1.0
（18）中天航信计算机终端保密检查系统 V1.0
（19）中国兵器计算机终端保密检查系统 V1.0
（20）天融信计算机终端保密检查系统 V1.0

（21）华安达计算机终端保密检查系统 V1.0

3、保密检查系统的功能

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。

- ◆ 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。
- ◆ 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。

4、保密检查技术

（1）现状

目前国内许多单位购买并在使用通过测评并取得资质证书的自主化保密检查工具，建立了以计算机、通信系统、移动存储介质为主的综合保密检查手段，加强了保密自查自纠工作。许多单位甚至研发了一键式检查工具等，为保密检查提供了技术支撑。但集中化、专用化、

标准化和实用化的检查工具还比较少，且针对声光电磁等立体窃密手段的检查工具还较为稀有。

（2）物理安全保密检查技术

当代各国，都把窃听与电子侦察作为窃取其他国家的军事、政治、经济、科学技术和工业情报的一种重要技术手段。现在的窃听器采用先进的科学技术，制作精细，伪装巧妙，甚至使人难以发现它的存在，有微型录音机、无线窃听器等等。而针对这些窃听手段我们可以通过一-些保密检查技术来防范于未然，比如针对安装在线路和电话中的窃听器材可以用线路检测装置来检测线路中是否有不正常的电流和高阻元器件等。

其中振动激光窃听技术是一种具有显著代表性的窃听技术。激光窃听是利用激光载体获取物体振动信息的一种手段，大致可分为三种技术：检测玻璃振动信息的正反射式激光强度检测窃听技术、穿透玻璃检测物品振动的基于多普勒干涉式激光频率或相位变化的窃听技术以及基于散斑探测的图像处理窃听技术。

20 世纪 80 年代，美国开始使用正反射式激光窃听技术来获取语音信息，自此之后，俄罗斯、日本、英国、美国十分重视这一技术的研究，并于 90 年代开发出自己的产品。2006 年至 2011 年期间，散斑干涉法也逐渐被应用在了语音检测中，2009 年以色列巴依兰大学 Zeev Zalevsky 等人提出了基于散斑模式的多语音源及心跳的实时远距离提取。2011 年，俄罗斯科学院的 A.A.Veber 利用目标散斑特性还原出了语音。

由此为例子，说明当前在涉密场所防护技术和技术检查产品上还需要进一步加强研发。比如在会议室如何合理安装声音遮蔽系统，如何综合检查声源限制与监控、振动声隔、声防护、声掩蔽与管道消声，如何综合检查措施对于防止光信息泄露。

（3）量子保密通信研究

当今时代，互联网承载的海量敏感、私密与机密信息正不断遭受到各种各样的网络攻击。国家互联网应急中心数据显示，我国已成为网络攻击的主要受害国。因此，保障信息通信与网络安全至关重要。目前，保障信息通信与网络安全所普遍使用的公钥密码体制面临强大的量子计算机和高效的攻击算法的威胁。量子密钥分发技术可以在认证的合法双方之间实现理论上无条件安全的对称密钥分发，具有为信息通信与网络提供长期的安全性和保密性的潜力。量子密钥分发的安全性由量子不可克隆定律和海森堡测不准原理等量子力学基本原理保障，任何试图窃听量子密钥分发的行为都会被发现。

5、保密技术检查的关注点

（1）物理隔离

重点检查单位是否有使用无线键鼠、无线耳机等具有无线互联功能的信息设备及办公自动化设备，检查涉密计算机、打印机、复印机是否有连接过国际互联网或其他公共信息网络，检查涉密计算机、打印机、复印机等信息设备和办公自动化设备是否安装无线网卡、蓝牙、红外等无线互联设备装置。针对普及的智能手机时代，需要特别关注是否有手机等移动通信

设备插拔连接涉密计算机的违规记录。

（2）身份鉴别

验证身份鉴别措施的有效性，核查登 录方式，重点检查涉密计算机终端身份鉴别是否符合要 求，是否设置了 BIOS 开机密码，查看应用系统用户口令、 服务器操作系统口令、数据库系统口令是否符合要求， 如计算机口令长度是否达到相应位数、口令复杂度是否 体现了包含大小写字母、数字或特殊字符，身份鉴别尝 试次数是否达到规定次数，拔掉密钥 KEY 后，屏幕保护 设定是否符合要求。

（3）电磁泄漏发射防护

查看涉密信息设备和办公自动化设备是否正确使用红黑电源隔离插座，是否日常开启视频保护器，涉密设备与非涉密设备间距是否保持在合理的安全距离之.上，是否保证涉密设备放置在安全可控区域，计算机显示屏不正对且不靠近科研生产办公区域的门窗位置摆放。

（4）密码保护措施

重点检查涉密信息系统是否配备符合国家标准规定的密码设备，按照国家有关规定采取密码保护措施。

（5）操作系统安全

查看系统是否定期安装了补丁程序，各类安全配置是否有效实施，查毒软件版本和病毒库是否定期更新升级并及时查杀，重点检查操作系统和数据库是否仍然存在不合规的弱口令、开放多余服务或端口、私自格式化或重装操作系统、存在感染木马、病毒等安全保密隐患的情况。

（6）安全域边界防护

验证涉密信息系统安全域之间设置的访问控制策略是否有效，安全域边界防护措施是否有效，重点检查是否有高密级信息由高等级安全域流向低等级安全域的违规情况发生。

（7）违规外联监控

查看涉密信息系统是否采取了有效的监控违规接入设备技术措施，涉密计算机有无通过拨号、有线/无线网卡登录国际互联网或其他公共信息网络的.上网记录，有无插拔未经注册或授权的 U 盘、SD 卡、MP3、MP4 等移动存储介质的违规行为，计算机光驱是否得到禁用，重点检查涉密计算机和非涉密计算机之间是否有交叉使用移动存储介质的情况发生。

（8）信息输入输出控制

对输入输出中间机和窗口机 进行病毒扫描和木马检测[89]关注杀毒软件查杀清除病毒的记录，重点检查涉密信息输入输出登记审批记录，查 看打印、复印、扫描文件资料名称、密级和用途等栏目是 否与登记本、审批表所述相一致

6、国外间谍软件发展应用

（1）美国国家安全局

2013 年 12 月 30 日，德国《明镜》周刊披露了一份长达 50 页的 ANT 产品文件，该文件披露了一个名为 ANT 的秘密组织为美国国家安全局下属的“获取特定情报行动办公室”（TAO）提供的 48 种秘密监控技术产品。在这些产品中，可以看出国家安全局所使用的一些间谍软件，如“源头”（HEADWATER）和“退学吉普”（DROPPUTJEEP）。

（2）美国中央情报局

2017 年 3 月 7 日，维基解密（Wiki Leaks）曝光了美国中央情报局代号为“Vault7”的文件，披露了该局从 2013 年至 2016 年的大量机密文件以及大批有分量的间谍软件，包括“哭泣天使”（Weeping Angel）、DerStarke 和 RickyBobby 等。

（3）美国联邦调查局

近年来，美国新闻媒体也多次披露了美国联邦调查局使用的间谍软件，包括“幻灯”“互联网通信协议地址校验器”（CIPAV）等。

“幻灯”是美国联邦调查局研发的“击键记录”软件，它可以通过邮件附件或利用操作系统漏洞进行远程安装。联邦调查局使用“幻灯”时，可以通过嫌疑人所信任的人的名义发送给他，也能通过常见的系统漏洞潜入系统。“幻灯”会自动安装在他人的计算机上。当嫌疑人使用电子邮件时，程序就会被激活。此时，“幻灯”会记录计算机的击键情况，并将收集到的加密信息发回联邦调查局，这样联邦调查局人员就可以解密嫌疑人的通信内容。

“互联网通信协议地址校验器”可以安装在嫌疑人计算机上，用以监控嫌疑人的计算机活动。

四、调研结论及建议

随着信息系统的普及，传统管理检查手段已经不能适应新形势下安全保密工作的要求，保密技术检查问题日益凸显。保密技术检查本质上是保密科技与保密管理相结合的产物，保密科技进步是保密技术检查的根本推动力，保密管理的严格规范是保密技术检查的重要保证。

我国保密技术检查还存在着以下问题：

（1）信息产业产业链依然存在诸多无法自主掌控的环节，若要从根本上做到保密技术检查大国，我国需要在这些方面继续加大投入力度

（2）集中化、专用化、标准化和实用化的检查工具和平台还比较少，技术单位需要针对这些方面加强研发

（3）针对全新的声光电磁复合保密战场，大部分单位对此依然处于低警惕，且相关科技检查技术依然匮乏，保密战场需要在这些领域攻防兼备

（4）国外情报部门的间谍软件更新手法迭代速度极快，攻击面越来越宽广，我国的保密部门需要增强在信息安全领域的攻防能力

（5）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，各单位应依据国家有关保密法律法规和标准规定，在明确职责划分的基础上，重新制订涉密信息系统保密监督检查办法，丰富保密监督检查类别和形式，细化保密检查具体要求和内容，补充便于操作、便于追溯、便于验证的保密技术检查条款。树立保密技术检查的权威性，增强保密技术检查的威慑力，做到有章可循，实现有章必循

五、参考文献

[1] 李元峰 . 涉密信息系统保密技术检查探索体会 [A]. 中航工业北京航空材料研究院 1009-8054（2013）06-074-03.

[2] 黎仪 . 浅谈保密检查技术与保密防护技术 [A].哈尔滨工程大学

[3] 王仕艳 .计算机网络安全中的信息保密技术[J].信息与电脑(理论版),2017(22):193-194.

[4] 中国电子科技集团公司第三十研究所 . 自主化原则在保密技术防护和检查中的运用

[5] 虞金龙 . 国家保密局保密技术检查中心 .保密技术检查中发现问题的思考.

[6] 潘正运,荆涛.网络安全与信息保密[J].中国计算机用户,2000(10):61.

[7] 陈平，易勇.计算机网络安全中信息保密技术探究[J].中国新通信,2018(8):80.

[8] Aldrich, Richard J.（ 2006 ）, The Hidden Hand: Britain, America and Cold War Secret Intelligence, London: John Murray ISBN 978-1-58567-274-5

[9] CENTRAL INTELLIGENCE AGENCY. CREST : 25-Year Program Archive

[10] NSA Cybersecurity Directorate. National Security Agency

[11] Центральный архив ФСБ России. ФСБ