**可行性研究报告**

面向系统安全的软件设计

网络08-2 王丹 08083765

2011.5.22

**可行性研究报告**

1. 引言……...……………………………………………………………………………………3
   1. 编写目的……...………...…………………………………………...………………......3
   2. 背景…...……...…...……...……………………………………………………………..3
   3. 参考资料……...…………………………………………………………………………3
2. **可行性研究的前提……...…………………………………………………………………...3**
   1. 要求……...…………………………………………………………………………….....3
   2. 目标…...……...…………………………………………………………………………..3
   3. 条件、假定和限制……...……...………………………………………………………..3
   4. 进行可行性研究的方法……...…………………………………………………………4
   5. 评价尺度……...………………………………………………………………………….3
3. **对现有系统的分析……...……………………………………………………………………4**
   1. 处理流程和数据流程……...…………...………………………………………………..5
   2. 工作负荷……...………………………………………………………………………….5
   3. 费用开支...……...……………………………………………………………………….5
   4. 人员……...………………………………………………………………………………5
   5. 设备……...……...………………………………………………………………………5
   6. 局限性……...…………………………………………………………………………….6
4. **所建议的系统……...…………………………………………………………………………7**
   1. 对所建议系统的说明……...…………………………………………………………….7
   2. 影响……...……………………………………………………………………………….7
      1. 对设备的影响……...…………………………………………………………..7
      2. 对软件的影响……...…………………………………………………………...8
      3. 对用户单位机构的影响……...………………………………………………...8
      4. 对系统运行过程的影响……...………………………………………………...8
      5. 对开发的影响……...…………………………………………………………...8
      6. 对地点和设施的影响……......…………………………………………………8
      7. 对经费开支的影响……...……………………………………………………...8
   3. 技术条件方面的可行性……...………………………………………………………….8
5. **可选择的其他系统方案……...………………………………………………………………8**
   1. 可选择的系统方案1……...……………………………………………………………..8
   2. 可选择的系统方案2……...……………………………………………………………..8
6. **投资及效益分析……...………………………………………………………………………9**
   1. 支出……...……………………………………………………………………………….9
      1. 基本建设投资……...……………………………………………………...........9
      2. 其他一次性支出……...……………………………………………………….9
      3. 非一次性支出……...………………………………………………………….9
   2. 收益……...……………………………………………………………………………...9
      1. 一次性收益……...…………………………………………………………….9
      2. 非一次性收益……...………………………………………………………….9
      3. 不可定量的收益……...……………………………………………………….9
   3. 收益/投资比……...……………………………………………………………………..10
   4. 投资回收周期……...…………………………………………………………………...10
   5. 敏感性分析……...……………………………………………………………………...10
7. **社会因素方面的可行性……...……………………………………………………………...10**
   1. 法律方面的可行性……...……………………………………………………………...10
   2. 使用方面的可行性……...……………………………………………………………...10
8. **结论……...…………………………………………………………………………………...10**
9. **引言**
   1. **编写目的**

为了更进一步提高计算机的安全使用，所以选择了面向系统安全的软件设计。主要涉及对系统监控、保护、防控、病毒检测等。

**背景**

第十三届计算机文化节软件设计比赛。

**参考资料**

1. 张艳平等《windows程序设计》人民邮电出版社，2008
2. Stanley B.Lippman 等《C++Primer》 人民邮电出版
3. （美）Jeffrey Richter 等《Windows核心编程》清华大学出版社 2008
4. 《Windows 黑客技术揭秘与攻防 》 裴要强 等 中国铁道出版社 2010
5. 《win32多线程编程》 候俊杰 华中科技大学出版社

**2． 可行性研究的前提**

**2.1 要求**

主要可涉及对系统监控、保护、防控、病毒检测等。

A,对指定的用户或系统文件进行监控，产生日志文件，记录用户对文件的重命名、删除、更改以及在文件夹内添加文件等行为。

B,对注册表进行监控，并且可对指定的用户程序进行注册表监控

C，进程管理，列出用户进程并且可以对指定程序的进程进行详细操作，

可以列出进程的具体模块信息。

D,病毒查杀，可以进行简单的病毒查杀，用户可以自定义查杀方式。

E，良好的人机界面，可以进行换程序皮肤等美化程序的功能。

**2.2 目标：**

为了提高计算机的安全使用，方便用户安全使用个人计算机。

**2.3 条件、假定和限制**

开发时间：2011年5.20 -6.9

经费来源：个人筹集

**2.4 进行可行性研究**

对于开发软件，主要从经济技术运行和法律方面进行可行性研究

1. 经济：校内的课程设计作业，可以忽略经济方面。
2. 技术：现有的技术水平早已经可以实现这类软件，360卫士就是很好的证明。
3. 运行：可以在多个系统，平台上运行。

（4）法律：此软件为小组开发，方便人们的交流，使人们的生活更加便利，不会有法律上的纠纷。  
**2.5 评价尺度**

1．是否功能齐全，运行稳定。

2. 是否具有多任务，高效率的特点。

3. 是否具有界面友好，操作简单的特点。   
**3．对现有系统的分析**

**3.1 处理流程**

把此系统主要分五个模块：

包括、进程管理模块、注册表监控、文件监控模块、杀毒软件模块、程序主界面模块（整合模块）。采取高内聚低耦合的编程思想。

A，进程管理模块可以对本机的进程进行列表，并且可以查看所有进程的映像名称以及PID，以及文件映像的路径。并且对指定的进程。

主要利用windows 底层　ＡＰＩ<Tlhelp32.h>， <psapi.h>　对对本机的进程进行列表，并显示具体模块信息。

使用ToolHelp提供的API函数来实现对进程的枚举，实现非常简单。

1、调用CreateToolhelp32Snapshot创建进程快照，返回快照句柄。

2、使用Process32First从意思就知道是对第一个进程进行操作，就是入口进程。

3、使用Process32Next逐个的读取进程，就像游标一样吧，多放在循环中。

Ｂ，注册表监视主要利用ＨＯＯＫ技术，Windows操作系统是建立在事件驱动机制之上的，系统各部分之间的沟通也都是通过消息的相互传递而实现的。但在通常情况下，应用程序只能处理来自进程内部的消息或是从其他进程发过来的消息，如果需要对在进程外传递的消息进行拦截处理就必须采取一种被称为HOOK（钩子）的技术。钩子是Windows操作系统中非常重要的一种系统接口，用它可以轻松截获并处理在其他应用程序之间传递的消息，并由此可以完成一些普通应用程序难以实现的特殊功能。基于钩子在消息拦截处理中的强大功能。

在注册监视模块中采用微软研究院Detour开发包之API拦截技术（Detours是一个在x86平台上截获任意Win32函数调用的kit。<http://research.microsoft.com/research/downloads/Details/d36340fb-4d3c-4ddd-bf5b-1db25d03713d/Details.aspx>

**）**此模块和进程管理模块涉及到进程通信。

C,文件监控，可以利用API ReadDirectoryChangesW 建立一个线程进行监控。

D,病毒查杀模块，查毒基本分两种，一种是基于特征码的，一种是基于行为的。本次主要涉及特征码查杀病毒

查杀流程：选择扫描目标——开始扫描硬盘——把文件加入扫描队列——按多线程病毒库对比（照特征码识别出病毒文件）——查找病毒进程——结束病毒进程——把可疑文件加入可疑文件队列中——删除病毒启动设置——列出可疑文件——其余清理。

**3.2 工作负荷**

**3.3 费用开支**

**3.4 人员**

自己。

**3.5 设备**

装有Windows7系统的计算机

**3.6 局限性**

相比现有的比较成熟的安全软件，该软件可能存在功能少，不稳定的缺点。

**4．所建议的系统**

**4.1 对所建议系统的说明**

本系统将大大改善数据处理速度，并且更加方便的对数据进行管理，同时可以减少人力资源的浪费以及工资支出 。

**4.2 影响**

**4.2.1对设备的影响**

无。

**4.2.2对软件的影响**

无

**4.2.3对用户单位机构的影响**

为了建立和运行所建议系统，需要提高管理人员的技术水平。   
**4.2.4对系统运行过程的影响**

所建议系统没有影响运行过程。

**4.2.5对开发的影响**

所建议系统对软件开发人员要求不高，但是对硬件要求比较高。

**4.2.6对地点和设施的影响**

所建议系统对建筑物无改造，可以利用原有的通信线路。

**4.2.7对用户的影响**

需要短时间来熟悉新系统，但不需要大量的培训。

* 1. **技术条件方面的可行性**

本软件有计算机系的学生开发，调试，由计算机系老师知道。可完成性很高。   
**5可选择的其他系统方案**

**5.1引进已有管理系统**

操作人员需要重新上机培训，可以避免大量开发费用

**5.2将程序开发工作移交专业软件公司制作**

不需学校投入大量相关人力，但相对物力比本方案要多

**6投资及效益分析（略）**

* 1. **敏感性分析**

现在人们非常需要一种安全软件来满足人们进行电脑方便使用，方便用户管理电脑。

本系统在Microsoft Visual Studio 6.0环境下实现，要求对系统监控、保护、防控、病毒检测等功能。主要是利用Vc++6.0 中 的MFC实现。这个编译软件是个功能十分强大的软件所以在市场可以占有一定的份额。

　　1）工程产品所追求的市场  
　　本系统所占有的市场为欲扩大客户使用规模，增添电脑安全使用，它追求的是简单、易学、易懂、易用，能够更有利的解决用户的需求，能够帮助使用者进行方便的电脑使用和管理。  
　　2）市场现状  
 现在比较有成熟的安全软件产品比如360，诺顿 等等，我主要利用学习的目的进行一次计算机安全方面的开发工作（计算机安全方面是一个很重要的领域），我开发这个软件纯属兴趣。

**7社会因素方面的可行性**

**7.1法律方面的可行性**

所有技术资料都由提出方保管。

合同制定确定违约责任

**7.2使用方面的可行性**

PcGuard软件的应用是可行的。

**8结论**

本系统可以马上开始实施，并尽可能做到提前完成。所以在几个可选择的方案中推荐此方案为最佳方案。