元心智能移动操作系统

安全子系统灰盒（设计）测试计划

--------软件质量保证大作业

学院：软件学院

专业：软件工程

学号：14126132

姓名：单晓兰

手机：15600696378

邮箱：14126132@bjtu.edu.cn

引言:学生在去年考研结束后就直接来北京，在现在所实习的公司实习。一年多来,主要负责的就是公司现在自主研发的安全性的手机操作系统元心操作系统的安全接口（灰盒）测试工作,整个安全模块的灰盒测试均由学生负责,所以从最先的阅读需求文档,设计文档,到指定测试计划,测试方法选定,以及测试用例编写执行,还有后期的测试工具编写执行,测试报告等都是学生在公司专业的测评负责人的指导下亲自编写执行。下文这篇灰盒接口的测试计划是在去年大概五六月份期间制定编写的，后期在测试进行过程中进行过相应的调整而完成。本公司在六月份左右将元心操作系统作为安全解决方案申请了国家信息安全测评中心的 ELA 4 级认证，在去年十一月份期间将包括本文在内的整个测试文档以及元心系统交付测评中心。本人认为，在经过了这整个一轮完整的测试过后，对于软件质量保证有了一定的深刻认识，故现将本文交于老师审查，希望老师能给出改进意见。

文档目录

元心智能移动操作系统

安全子系统灰盒（设计）测试计划

1. 概述

1.1. 文档目的

本文档为元心智能移动操作系统的安全子系统灰盒（设计）测试的执行和管理提供工作指导，以便有序的进行测试进度跟踪和管理。

1.2. 文档使用范围

本文档供元心智能移动操作系统安全子系统灰盒（设计）测试组、元心智能移动操作系统项目管理部使用。同时，提供给第三方授权机构以进行评估，由文档管理部门进行归档。

1.3. 文档内容描述

本文档描述了元心智能移动操作系统灰盒测试的总体思路和方法，明确安全子系统灰盒测试的范围、测试的方法和环境要求、测试的阶段性目标和人员、进度安排。

1.4. 缩略及术语说明

表 1-1 缩略及文档术语说明表

序号	名称（中文/英文）	解释	备注
1	元心操作系统	北京元心科技有限公司研发生产的智能移动操作系统的中文简称。	
2	SyberOS	北京元心科技有限公司研发生产的智能移动操作系统的英文简称。	
3	SyberOS_ATE_DPT.P	元心智能移动操作系统安全系统灰盒（设计）测试计划的英文名称。	

2. 灰盒测试对象和范围

2.1. 灰盒测试对象

元心智能移动操作系统灰盒测试对象是元心操作系统安全子系统的安全功能接口，这些安全功能接口即包括安全子系统与非安全功能的接口，也包括安全子系统内部各功能子系统之间的接口，对于某些重要的安全功能子系统还包括功能子系统内部模块间和模块内关键的安全接口。

灰盒测试的安全接口范围仅局限于运行在移动智能终端上的安全子系统软件，包括内核、系统服务和系统应用。元心智能移动操作系统依赖的安全系统和设备的接口不在测试范围内。

2.2. 测试范围

元心智能移动操作系统安全子系统是由 21 个安全功能子系统组成的，其中安全中心是安全功能的管理和操作中心，其接口均通过界面体现，在黑盒测试中已覆盖，在本测试中不再关注这部分内容。这样本测试计划的测试范围如下：

1) 用户身份鉴别子系统外部安全接口、内部模块间接口
2) 防骚扰子系统外部安全接口、内部模块间接口
3) 用户数据加密子系统外部安全接口、内部模块间接口
4) 用户数据安全删除子系统外部安全接口、内部模块间接口
5) 系统时钟子系统外部安全接口、内部模块间接口
6) 安装包身份鉴别子系统外部安全接口、内部模块间接口
7) 应用开发接口访问控制子系统外部安全接口、内部模块间接口
8) 防盗保护子系统外部安全接口、内部模块间接口
9) 系统资源配额管理子系统外部安全接口、内部模块间接口
10) 移动通讯网络资源管理子系统外部安全接口、内部模块间接口
11) 会话管理子系统外部安全接口、内部模块间接口
12) 恢复出厂设置子系统外部安全接口、内部模块间接口
13) 应用运行访问控制（沙箱）子系统外部安全接口、内部模块间接口

14) 网络通信保护子系统外部安全接口、内部模块间接口

15) 防火墙子系统外部安全接口、内部模块间接口

16) 安全审计子系统外部安全接口、内部模块间接口

17) 备份恢复子系统外部安全接口、内部模块间接口

18) 系统自主访问控制子系统外部安全接口、内部模块间接口

19) 系统强制访问控制子系统外部安全接口、内部模块间接口

20) 系统权限能力控制子系统外部安全接口、内部模块间接口

3. 灰盒测试环境和方法

3.1. 概述

元心智能移动操作系统只提供 GUI 方式与用户交互，而元心智能移动操作系统安全子系统的接口均无法通过 GUI 方式进行直接调用和观测。因此，为了进行安全系统的接口测试，必须引入除 GUI 之外的方式与系统进行交互。借助元心智能移动操作系统的 Shell 交互功能，通过对终端设备的改造，从硬件电路引出串口通讯线的方式提供测试人员连接系统运行的 Shell。这样可以借助传统的 Linux Shell 交互方式，通过运行终端测试程序达到接口测试的目的。

此外，元心智能移动操作系统安全功能的安全配置和策略按照安全目标的定义，大部分是预制的并且被妥善保护。这样，元心智能移动操作系统的某些测试场景将无法恢复，尤其是涉及访问控制和权限管理的功能。这就要求测试中必须引入某些只在系统制造过程中存在的工具和特权以完成安全功能接口的测试。

这样元心智能移动操作系统的灰盒测试必须有产品形态的扩充，必须有配合测试使用的特权工具，必须提供不通过应用安装通道引入工具的特权使用场景。并且为模拟真实设备运行环境必须提供能建立移动网络通道的设备，提供满足 ST 要求的模拟外部可信部件。

3.2. 灰盒测试环境

基于上述原因，元心智能移动操作系统灰盒测试需要对元心智能移动操作系统安装的终端设备进行改造，通过硬件引出串口通讯线的方式提供测试人员连接系统运行 Shell 的能力。

另外，为了方便测试终端安装测试工具，元心终端应当通过 WIFI 网络与测试人员使用的普通 PC 设备接入同一局域网环境。这样，所有针对元心智能移动操作系统安全子系统的接口测试均按照如下部署环境进行：

图 3-1 元心智能移动操作系统测试环境

3.3. 灰盒测试方法

元心智能移动操作系统安全子系统安全接口的调用方式包括以下类型：

1）界面调用模式

典型的就是安全中心的界面逻辑

这种接口以界面流转的方式展现，其接口逻辑在黑盒测试中覆盖，在灰盒测试中不再涵盖。此类接口包括安全中心与各安全功能子系统交互的界面元素、也包括各安全功能子系统单独存在的交互类界面元素。

2）消息通讯模式

元心智能移动操作系统为解决应用/服务之间的交互问题，提供消息通讯机制。元心安全子系统的安全功能接口很多也采用消息通讯模式提供调用功能。

元心智能移动操作系统的消息通讯机制是采用 DBus 消息中间件机制来实现的，DBus 消息中间件提供消息发送和监听的工具供用户使用。借助这些工具可以模拟安全功能接口的使用者进行消息接口的调用并观测测试结果。

3）函数调用模式

元心智能移动操作系统大量的安全功能接口是以传统的函数接口的方式提供的。由于元

心系统整体是以 c/c++语言编写开发的，因此这些接口基本以 C 函数接口或 C++类对象方法的形式提供。对这些接口进行测试需要编写测试驱动程序以调用这些接口。

特殊的，元心智能移动操作系统很多安全功能接口是内核态的函数接口，这些接口很多是回调形式的接口。这样，这些内核态接口的测试就无法通过直接的调用形式进行测试，需要通过应用态间接触发的方式进行测试。

4）命令调用模式

元心智能移动操作系统安全子系统的安全功能接口也以命令行工具的方式提供功能接口，这些接口采用 shell 命令执行方式被调用，可以直接通过命令执行过程和反馈进行测试。

4. 灰盒测试计划

4.1. 概述

通过上述分析，灰盒测试整体工作包括测试方案的制定、测试工具的开发、测试环境的搭建、测试用例的执行、测试证据的收集和测试问题的回归。那么灰盒测试计划的制定会涵盖以上范围。

由于元心系统的开发方式决定了系统接口的变更只会在有限范围内进行，因此灰盒测试的工作计划按照传统的瀑布模型推进。

首先确定测试方法，根据测试方法开发测试工具同时编写测试用例，根据用例要求搭建测试环境，按照产品研发进度安排测试执行和证据收集，并依据产品更新进行问题回归和确认。

根据如上测试推进方式，灰盒测试制定里程碑：

1) 测试计划确定。
2) 测试方案确定。
3) 测试进行 50%，产品版本功能基本完备。
4) 测试进行完毕，产品达到发售状态。
5) 测试文档整理完毕可以提交。

整体计划如下图所示：

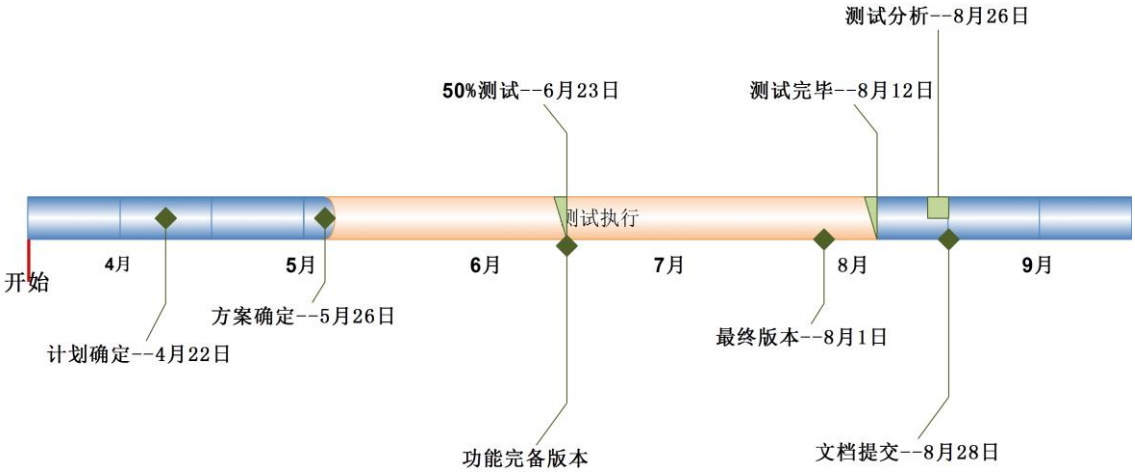

图 4-1 灰盒测试里程碑

4.2. 灰盒测试计划制定

4.2.1.阶段目标

根据产品开发计划和测评计划制定灰盒测试计划，确定灰盒测试各阶段工作内容和时间节点。评估各阶段的工作任务和资源需求，给出各阶段具体实施计划。

该阶段交付物为《D-0102-W301-1400-S1-V1.0_SyberOS_ATE_DPT.P_元心移动操作系统安全子系统灰盒（设计）测试计划》文档。

4.2.2.人员与进度计划

该阶段需确认灰盒测试设计人员一名，由该名成员进行灰盒测试计划梳理工作。该阶段工作计划的制定依赖产品研发路径的确认、产品功能规范的确认和产品研发规模的确认。

下表为该阶段人员与进度安排：

表 4-1 灰盒测试计划制定工作进度安排

编号	工作		计划日期	工时	资源
	任务	子任务			
1	测试任务分解	元心系统安全子系统功能评估	4 月 11 日-4 月 14 日	2 天/人	灰盒测试设计人员
		元心系统安全子系统接口规模评估	4 月 15 日-4 月 16 日	2 天/人	灰盒测试设计人员
		元心系统产品研发里程碑评估	4 月 17 日-4 月 18 日	1 天/人	灰盒测试设计人员

		安全子系统设计测试工作分解	4 月 18 日-4 月 21 日	2 天/人	灰盒测试设计人员
2	测试计划制定	任务计划文档制定	4 月 21 日-4 月 22 日	1 天/人	灰盒测试设计人员

4.2.3. 风险与预案

该阶段存在以下风险：

1) 系统功能研发过程的功能变化

应对措施：与产品规划和设计人员进行充分沟通，该工作在后续阶段持续进行，整个测试任务计划根据功能变更进行对应性修订。

2) 系统开发规模的变化及准确评估性

应对措施：与产品设计人员和研发人员进行充分沟通，采取多人评估方式进行综合度量。该工作在后续阶段持续进行，在任务进行期间根据系统变更进行对应性修订。

3) 研发计划的调整及细节不明确

应对措施：测试分两阶段进行，期间针对研发计划做对应性修订。

4. 3. 灰盒测试方案制定

4.3.1. 阶段目标

根据产品规划和安全子系统的设计，制定灰盒测试方案。明确各接口测试方法、确定测试数据选择方式、确定测试用例编写方法、确定测试工具开发类型、确定测试结果分析方式。

该阶段交付物为《元心智能移动操作系统安全系统灰盒（设计）测试方案》文档。

4.3.2. 人员与进度计划

该阶段需确认灰盒测试设计人员两名，由该名成员进行灰盒测试方案梳理工作。该阶段工作成果依赖安全子系统设计方案的确定和安全子系统实现方案的确定。

下表为该阶段人员与进度安排：

表 4-2 灰盒测试方案制定工作进度安排

编号	工作		计划日期	工时	资源
	任务	子任务			

1	安全子系统设计方案分析	元心系统安全子系统设计方案梳理	4 月 23 日-4 月 28 日	8 人天	灰盒测试设计人员 2 人
		元心系统安全子系统接口方式梳理	4 月 29 日-5 月 07 日	10 人天	灰盒测试设计人员 2 人
		元心系统安全子系统接口实现方式梳理	5 月 08 日-5 月 14 日	10 人天	灰盒测试设计人员 2 人
		元心系统安全子系统测试工具梳理	5 月 15 日-5 月 19 日	6 人天	灰盒测试设计人员 2 人
2	安全子系统设计方案发布	元心系统安全子系统设计方案制定	5 月 20 日-5 月 26 日	12 人天	灰盒测试设计人员 2 人

4.3.3. 风险与预案

该阶段存在以下风险：

1) 设计方案存在变更风险。

应对措施：预留方案变更的进度，测试方案后续阶段持续进行，测试方案根据功能变更进行对应性修订。

2) 接口存在变更风险。

应对措施：与产品设计人员和研发人员进行充分沟通，采取多人评估方式进行综合评定。测试方案在后续阶段持续维护，在任务进行期间根据系统变更进行对应性修订。

3) 接口实现方法存在变更风险。

应对措施：测试分两阶段进行，对变更的接口进行对应性修订。

4. 4. 灰盒测试阶段一

4.4.1. 阶段目标

根据测试设计和灰盒测试方案进行测试用例编写，开发测试工具，开始进行简单的明确的接口测试并分析测试结果。

该阶段交付物为《元心智能移动操作系统安全系统灰盒测试用例》文档（多份）、测试工具、阶段性测试报告。

4.4.2. 人员与进度计划

该阶段需确认灰盒测试开发工程师两名、灰盒测试用例编写/执行工程师三名。

下表为该阶段人员与进度安排：

表 4-3 灰盒测试阶段一工作进度安排

编号	工作		计划日期	工时	资源
	任务	子任务			
1	灰盒测试用例设计	测试用例编写	5 月 27 日-6 月 17 日	30 人天	灰盒测试用例编写人员 2 人
		测试数据集合梳理	6 月 09 日-6 月 20 日	20 人天	灰盒测试用例编写人员 2 人
		测试工具要求梳理	6 月 08 日-6 月 18 日	16 人天	灰盒测试用例编写人员 1 人
		测试步骤原理性验证	5 月 27 日-6 月 17 日	10 人天	灰盒测试用例编写人员 1 人
2	灰盒工具开发	测试工具开发	6 月 03 日-6 月 13 日	20 人天	灰盒开发人员 2 人
3	灰盒测试执行	测试用例执行	6 月 13 日-6 月 23 日	24 人天	灰盒测试用例执行人员 3 人

4.4.3. 风险与预案

该阶段存在以下风险：

1) 功能理解存在偏差

应对措施：研发人员和测试人员充分沟通，先进行原理验证，后设计用例，再开发工具并测试执行。

2) 产品计划延误

应对措施：加强用例编写详细程度和可用性验证，使用例达到能够简单易懂方便执行的状态。在产品延误时，可以增加人员并发进行测试。

4.5. 灰盒测试阶段二

4.5.1. 阶段目标

根据第一阶段测试结果进行灰盒测试方案修订、测试用例修订。完成剩余接口的测试、完善测试工具、回归验证第一轮产生的 Bug。

该阶段交付物为《元心智能移动操作系统安全系统灰盒测试用例》文档（多份）、测试工具、阶段性测试报告。

4.5.2. 人员与进度计划

该阶段需确认需确认灰盒测试设计人员一名、灰盒测试开发工程师一名、灰盒测试用例编写/执行工程师三名。

下表为该阶段人员与进度安排：

表 4-4 灰盒测试阶段二工作进度安排

编号	工作		计划日期	工时	资源
	任务	子任务			
1	灰盒测试用例方案修订	已进行测试方案总结	6 月 24 日-6 月 30 日	5 人天	灰盒测试用例设计人员 1 人
		根据变更进行方案修订	7 月 1 日- 7 月 4 日	4 人天	灰盒测试用例设计人员 1 人
2	灰盒测试用例修订	根据测试方案修订测试用例	7 月 1 日-7 月 11 日	18 人天	灰盒测试用例编写人员 2 人
3	灰盒测试工具修订	根据测试用例修订测试工具	7 月 08 日-7 月 18 日	9 人天	灰盒开发人员 1 人
4	灰盒测试执行	测试用例执行 1	6 月 24 日-7 月 11 日	14 人天	灰盒测试用例执行人员 1 人
		测试用例执行 2	7 月 14 日-8 月 1 日	45 人天	灰盒测试用例执行人员 3 人
		测试用例 Bug 回归	8 月 1 日 - 8 月 12 日	21 人天	灰盒测试用例执行人员 3 人

4.5.3. 风险与预案

该阶段存在以下风险：

1) 开发进度计划变更风险。

应对措施：Bug 回归工作可以分阶段进行，可以根据开发进度情况进行调整；测试模块

顺序可以随时调整，在测试方案完备的情况下根据进度状况调整测试模块顺序。

2) 设计变更风险。

应对措施：与产品设计人员和研发人员进行充分沟通，采取多人评估方式进行综合评定。测试方案和用例持续维护，在任务进行期间根据系统变更进行对应性修订。

3) 测试实现难度风险。

应对措施：在测试方案阶段进行充分的原理验证，在测试进行过程中持续与研发沟通，并进行技术培训。

4.6. 灰盒测试文档整理

4.6.1.阶段目标

总结测试结果，修订灰盒测试方案，整理测试证据，修订测试用例。对测试结果进行测试深度分析，形成测试深度分析文档。

该阶段交付物为《元心智能移动操作系统安全系统灰盒（设计）测试方案》文档、《元心智能移动操作系统安全系统灰盒（设计）测试用例》文档（多份）、元心智能移动操作系统安全系统灰盒（设计）测试证据（多份）、《元心智能移动操作系统安全系统灰盒（设计）测试深度分析》文档。

4.6.2.人员与进度计划

该阶段需确认灰盒测试设计人员 2 名，由该名成员进行灰盒测试方案修订和深度分析工作；测试用例编写人员 3 名，由该成员进行灰盒测试用例整理和测试证据整理。该阶段工作成果依赖灰盒测试的全面完成确定。

下表为该阶段人员与进度安排：

表 4-5 灰盒测试计划制定工作进度安排

编号	工作		计划日期	工时	资源
	任务	子任务			
1	测试方案	元心系统安全子系统灰盒测试方案整理	8 月 13 日-8 月 15 日	6 人天	灰盒测试设计人员 2 人

2	测试用例和证据	测试用例整理	8 月 13 日-8 月 22 日	16 人天	灰盒用例编写人员 2 人
		测试证据一致性对应	8 月 13 日-8 月 26 日	10 人天	灰盒用例编写人员 1 人
3	测试分析	元心系统灰盒测试报告	8 月 18 日-8 月 26 日	10 人天	灰盒测试设计人员 2 人
		元心系统灰盒测试深度分析	8 月 18 日-8 月 21 日	4 人天	灰盒测试设计人员 1 人

4.6.3. 风险与预案

该阶段存在以下风险：

1) 产品版本变更引起证据不一致。

应对措施：进行一致性分析，发现证据不一致及时做回归，安排专人进行一致性梳理。

5. 计划汇总

表 5-1 灰盒测试计划进度安排表

编号	工作		计划日期	工时	资源
	任务	子任务			
1	安全子系统设计方案分析	元心系统安全子系统设计方案梳理	4 月 23 日-4 月 28 日	8 人天	灰盒测试设计人员 2 人
		元心系统安全子系统接口方式梳理	4 月 29 日-5 月 07 日	10 人天	灰盒测试设计人员 2 人
		元心系统安全子系统接口实现方式梳理	5 月 08 日-5 月 14 日	10 人天	灰盒测试设计人员 2 人
		元心系统安全子系统测试工具梳理	5 月 15 日-5 月 19 日	6 人天	灰盒测试设计人员 2 人
2	安全子系统设计方	元心系统安全子系统设计方案制	5 月 20 日-5 月 26 日	12 人	灰盒测试设计人员 2

	案发布	定		天	人
3	安全子系统设计方案分析	元心系统安全子系统设计方案梳理	4 月 23 日-4 月 28 日	8 人天	灰盒测试设计人员 2 人
		元心系统安全子系统接口方式梳理	4 月 29 日-5 月 07 日	10 人天	灰盒测试设计人员 2 人
		元心系统安全子系统接口实现方式梳理	5 月 08 日-5 月 14 日	10 人天	灰盒测试设计人员 2 人
		元心系统安全子系统测试工具梳理	5 月 15 日-5 月 19 日	6 人天	灰盒测试设计人员 2 人
4	安全子系统设计方案发布	元心系统安全子系统设计方案制定	5 月 20 日-5 月 26 日	12 人天	灰盒测试设计人员 2 人
5	灰盒测试用例设计	测试用例编写	5 月 27 日-6 月 17 日	30 人天	灰盒测试用例编写人员 2 人
		测试数据集合梳理	6 月 09 日-6 月 20 日	20 人天	灰盒测试用例编写人员 2 人
		测试工具要求梳理	6 月 08 日-6 月 18 日	16 人天	灰盒测试用例编写人员 1 人
		测试步骤原理性验证	5 月 27 日-6 月 17 日	10 人天	灰盒测试用例编写人员 1 人
6	灰盒工具开发	测试工具开发	6 月 03 日-6 月 13 日	20 人天	灰盒开发人员 2 人
7	灰盒测试执行	测试用例执行	6 月 13 日-6 月 23 日	24 人天	灰盒测试用例执行人员 3 人
8	灰盒测试用例方案修订	已进行测试方案总结	6 月 24 日-6 月 30 日	5 人天	灰盒测试用例设计人员 1 人
		根据变更进行方案修订	7 月 1 日- 7 月 4 日	4 人天	灰盒测试用例设计人员 1 人
9	灰盒测试用例修订	根据测试方案修订测试用例	7 月 1 日-7 月 11 日	18 人	灰盒测试用例编写人员

				天	2 人
10	灰盒测试工具修订	根据测试用例修订测试工具	7 月 08 日-7 月 18 日	9 人天	灰盒开发人员 1 人
11	灰盒测试执行	测试用例执行 1	6 月 24 日-7 月 11 日	14 人天	灰盒测试用例执行人员 1 人
		测试用例执行 2	7 月 14 日-8 月 1 日	45 人天	灰盒测试用例执行人员 3 人
		测试用例 Bug 回归	8 月 1 日 - 8 月 12 日	21 人天	灰盒测试用例执行人员 3 人
12	测试方案	元心系统安全子系统灰盒测试方案整理	8 月 13 日-8 月 15 日	6 人天	灰盒测试设计人员 2 人
13	测试用例和证据	测试用例整理	8 月 13 日-8 月 22 日	16 人天	灰盒用例编写人员 2 人
		测试证据一致性对应	8 月 13 日-8 月 26 日	10 人天	灰盒用例编写人员 1 人
14	测试分析	元心系统灰盒测试报告	8 月 18 日-8 月 26 日	10 人天	灰盒测试设计人员 2 人
		元心系统灰盒测试深度分析	8 月 18 日-8 月 21 日	4 人天	灰盒测试设计人员 1 人

制作单位：北京元心科技有限公司

部门名称：安全中心

日　　期：2014 年 10 月 15 日