|  |  |
| --- | --- |
| 产品名称 | 密级 |
|  | 机密 |
| 产品版本 | 共页 |
|  |

安全性设计说明书

*(Title must be in both Chinese and English to facilitate English speaking users' search为方便英语用户检索，此处必须提供中英文版)*

|  |  |  |  |
| --- | --- | --- | --- |
| 拟制 | 史习云 | 日期 | 2015-12-01 |
| 审核 |  | 日期 | yyyy-mm-dd |
| 批准 |  | 日期 | yyyy-mm-dd |



华为技术有限公司

版权所有 侵权必究

修订记录

|  |  |  |  |
| --- | --- | --- | --- |
| 日期 | 修订版本 | 修改描述 | 作者 |
| yyyy-mm-dd | 1.0 | 初稿完成 | 史习云（00359263） |
| yyyy-mm-dd | 1.1 |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

目 录

[1 简介 6](#_Toc408235269)

[1.1 范围 6](#_Toc408235270)

[1.2 特性概述 6](#_Toc408235271)

[1.3 假设和约束 6](#_Toc408235272)

[2 Low Level威胁分析 6](#_Toc408235273)

[3 安全需求设计 6](#_Toc408235274)

[3.1 XX需求 6](#_Toc408235275)

[3.2 YY需求 8](#_Toc408235276)

[4 各模块的分配需求 8](#_Toc408235277)

[5 各模块的接口描述 8](#_Toc408235278)

[6 备注和附录 8](#_Toc408235279)

[6.1 数据字典 9](#_Toc408235280)

[6.1.1 数据字典列表 9](#_Toc408235281)

表目录

表1 样表：响应时间分配 7

表2 样表：XX功能分解表 8

表3 样表：XX功能接口表 10

图目录

图1 样图：处理流程示意图 7

Keywords 关键词： *Provide Keywords in both Chinese and English to facilitate English speaking users' search. 为方便英语用户检索，此处必须提供中英文版*

Abstract 摘要：*Provide Abstract in both Chinese and English to facilitate English speaking users' search. 为方便英语用户检索，此处必须提供中英文版*

缩略语清单：

| 缩略语 | 英文全名 | 中文解释 |
| --- | --- | --- |
| MKT(Marketing) | Marketing Management System | 营销管理系统 |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# 简介

## 范围

写作说明：本文档默认使用的Word格式是“正文缩进”。作者在写作文档主体时，请在菜单“样式和格式”中选择“正文缩进”样式。其它需要用到的表格、图、编号、列表等也已经预定义了样式，请尽量使用已有样式，不要自定义样式。

安全性设计的过程是对当前的特性/业务场景做Low Level威胁建模，识别安全风险并制定消减方案。

本章节简要描述本设计的范围，包括设计的影响范围。

本文描述了MKT（营销管理系统）系统的安全设计和实现方案，覆盖该系统的MKT Server、MySQL数据库、日志存储模块。周边涉及统一Portal、数据平台Hadoop集群等内部系统相关部件。

## 特性概述

*用一段简单的概要对此特性进行描述。*

华为智能终端越来越火爆，线上线下越来越抢手。为了支撑日常的终端的营销，我司需要在各个门户投放广告。选择哪些门户、哪些广告位进行广告的投放，广告投放的效果如何，我们需要设计这么一套系统，在跟踪分析终端广告投放的效果。

1、创建营销活动，每个活动产生多个广告位。对于每个广告位的着陆链接进行生成监控代码，后续广告投放时，就会通过http消息上报对于的数据。

2、将数据平台获得的数据进行统计，将统计出来的汇总值在系统中展示。

## 假设和约束

本章节罗列假设和约束，包括环境特征用户特征、软硬件约束、遵守的标准、已知的问题等。

该系统用户为产品、运营等公司内部人员；

访问该系统时，必须接入公司iaccess或者使用运维vpn；

该系统的数据来源为数据平台的数据仓库，该仓库仅对部署在同一网络环境内的内部系统开放访问权限，不直接对外提供任务服务。

本系统支持Firefox、chrome浏览器（暂不支持IE浏览器）

# Low Level威胁分析

## 2-DFD

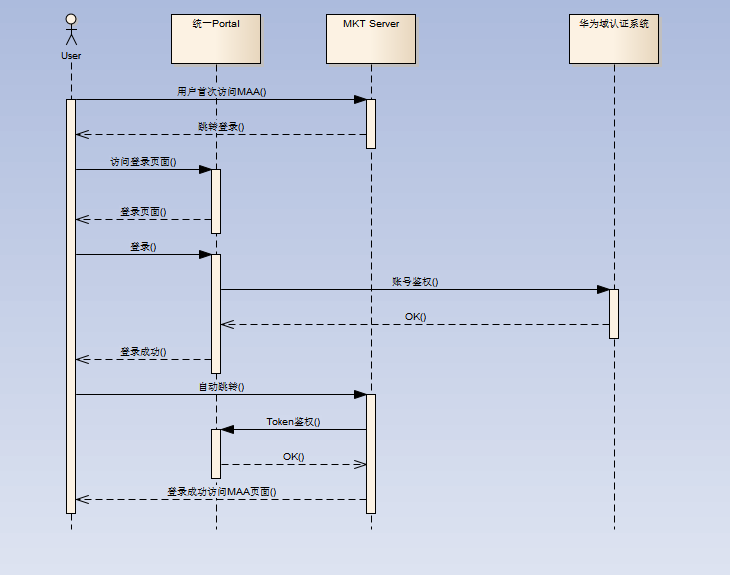
### 数据流图



### 业务场景及信任边界说明

涉及信任边界的业务场景主要包括数据统计、用户登录（查看报表）、发送邮件活动三个场景

#### 用户登录



信任边界主要为网络边界：

用户与MKT Server、MKT Server与统一portal 、MKT Server和邮件服务器为网络边界，信任度较低。

注：统一Portal华为域认证服务器之间为IT机房内部网络信任度较高，且MKT Server不直接与域认证服务器交互，此处不做分析。MKT Server和邮件服务器亦然。

#### 数据统计

MKT Server：用户在MKT中配置应用信息存储在MySQL中，用户的所有的日志操作也存储于Mysql中

Hadoop(BI数据仓库)：负责根据上报数据信息离线统计各类应用数据，统计完后数据同步到MySQL，以供前台展示使用。

该场景中，MKT Server、Hadoop部署在统一网络内，之间使用内部IP进行通信；信任度较高可以作为内部威胁来分析。

### 外部交互方分析

#### Hadoop

|  |  |  |
| --- | --- | --- |
| 元素名称 | Hadoop | |
| 元素概述 | 支撑后台数据 | |
| 威胁 | SR | |
| 仿冒（S） | 风险（Risk） | **风险等级：无**  **影响：**  局域网内内部组件，在同一信任区域内  **可能性评估：**  无 |
| 已有消减措施 | NA |
| 建议消减措施 | NA |
| 产品落地计划 | NA |
| 抵赖（R） | 风险（Risk） | **风险等级：无**  **影响：**  局域网内内部组件，在同一信任区域内  **可能性评估：**  无 |
| 已有消减措施 | NA |
| 建议消减措施 | NA |
| 产品落地计划 | NA |

#### 统一Portal

|  |  |  |
| --- | --- | --- |
| 元素名称 | 统一Portal | |
| 元素概述 | 用户统一认证 | |
| 威胁 | SR | |
| 仿冒（S） | 风险（Risk） | **风险等级：无**  **影响：**  华为IT机房内交互，在信任边界内  **可能性评估：**  无 |
| 已有消减措施 | NA |
| 建议消减措施 | NA |
| 产品落地计划 | NA |
| 抵赖（R） | 风险（Risk） | **风险等级：无**  **影响：**  华为IT机房内交互，在信任边界内  **可能性评估：** |
| 已有消减措施 | NA |
| 建议消减措施 | NA |
| 产品落地计划 | NA |

#### 用户

|  |  |  |
| --- | --- | --- |
| 元素名称 | 用户 | |
| 元素概述 | NA | |
| 威胁 | SR | |
| 仿冒（S） | 风险（Risk） | **风险等级：低**  **影响：**  【影响】  用户被仿冒,可以配置查看系统的数据  【可能性】  1. 同时获得vpn账号、vpn证书和华为员工域账号密码  2.同时获得iaccess接入权限和华为员工域账号密码  **可能性评估：**  无 |
| 已有消减措施 | 1.使用公司域账号进行认证  2.必须接入iaccess或vpn才能访问  3.使用https通道 |
| 建议消减措施 | NA |
| 产品落地计划 | NA |
| 抵赖（R） | 风险（Risk） | **风险等级：低**  **影响：**  【影响】  修改系统配置信息  【可能性】  获取授权系统账号及数据库账号删除操作日志数据  **可能性评估：**  无 |
| 已有消减措施 | 1.只有运维人员通过vpn才能访问业务数据库  2.只有授权的Linux账号才能访问数据库并删除数据  3.通过接口等方式也无法访问日志数据  4.根据运维管理制度，运维人员定期修改密码 |
| 建议消减措施 | NA |
| 产品落地计划 | NA |

#### 邮件服务器

|  |  |  |
| --- | --- | --- |
| 元素名称 | 邮件服务器 | |
| 元素概述 | 对系统操作人员发送邮件 | |
| 威胁 | SR | |
| 仿冒（S） | 风险（Risk） | **风险等级：无**  **影响：**  华为IT机房内交互，在信任边界内  **可能性评估：**  NA |
| 已有消减措施 | NA |
| 建议消减措施 | NA |
| 产品落地计划 | NA |
| 抵赖（R） | 风险（Risk） | **风险等级：无**  **影响：**  华为IT机房内交互，在信任边界内  **可能性评估：**  NA |
| 已有消减措施 | NA |
| 建议消减措施 | NA |
| 产品落地计划 | NA |

### 数据流分析

#### Hadoop⇒Mysql(数据导出)

|  |  |  |
| --- | --- | --- |
| 元素名称 | Hadoop⇒Mysql(数据导出) | |
| 元素概述 | 统计数据汇聚后以供前台查询 | |
| 威胁 | TID | |
| 篡改（T） | 风险（Risk） | **不分析：在信任边界内**  内部处理模块，不对外交互，不做分析 |
| 已有消减措施 | NA |
| 建议消减措施 | NA |
| 产品落地计划 | NA |
| 信息泄漏（I） | 风险（Risk） | **不分析：在信任边界内**  内部处理模块，不对外交互，不做分析 |
| 已有消减措施 | NA |
| 建议消减措施 | NA |
| 产品落地计划 | NA |
| 拒绝服务（D） | 风险（Risk） | **不分析：在信任边界内**  内部处理模块，不对外交互，不做分析 |
| 已有消减措施 | NA |
| 建议消减措施 | NA |
| 产品落地计划 | NA |

#### MKT Server⇒邮件服务器(发送邮件)

|  |  |  |
| --- | --- | --- |
| 元素名称 | MKT Server⇒邮件服务器(发送邮件) | |
| 元素概述 | 根据业务需求发送邮件给相关人员 | |
| 威胁 | TID | |
| 篡改（T） | 风险（Risk） | **不分析：在信任边界内**  内部处理模块，不对外交互，不做分析 |
| 已有消减措施 | NA |
| 建议消减措施 | NA |
| 产品落地计划 | NA |
| 信息泄漏（I） | 风险（Risk） | **不分析：在信任边界内**  内部处理模块，不对外交互，不做分析 |
| 已有消减措施 | NA |
| 建议消减措施 | NA |
| 产品落地计划 | NA |
| 拒绝服务（D） | 风险（Risk） | **不分析：在信任边界内**  内部处理模块，不对外交互，不做分析 |
| 已有消减措施 | NA |
| 建议消减措施 | NA |
| 产品落地计划 | NA |

#### Mysql⇔MKT Server(用户权限/广告营销信息/日志)

|  |  |  |
| --- | --- | --- |
| 元素名称 | Mysql⇔MKT Server(用户权限/广告营销信息/日志) | |
| 元素概述 | 支撑前台数据 | |
| 威胁 | TID | |
| 篡改（T） | 风险（Risk） | **不分析：在信任边界内**  内部处理模块，不对外交互，不做分析 |
| 已有消减措施 | NA |
| 建议消减措施 | NA |
| 产品落地计划 | NA |
| 信息泄漏（I） | 风险（Risk） | **不分析：在信任边界内**  内部处理模块，不对外交互，不做分析 |
| 已有消减措施 | NA |
| 建议消减措施 | NA |
| 产品落地计划 | NA |
| 拒绝服务（D） | 风险（Risk） | **不分析：在信任边界内**  内部处理模块，不对外交互，不做分析 |
| 已有消减措施 | NA |
| 建议消减措施 | NA |
| 产品落地计划 | NA |

#### 统一Portal⇔MKT Server(认证Token/用户信息)

|  |  |  |
| --- | --- | --- |
| 元素名称 | 统一Portal⇔MKT Server(认证Token/用户信息) | |
| 元素概述 | MKT到统一Portal认证token是否合法,统一Portal同步用户信息到MKT | |
| 威胁 | TID | |
| 篡改（T） | 风险（Risk） | **风险等级：低**  **影响：**  【影响】  影响业务登录,同步错误的用户信息  【可能性】  网元被劫持篡改数据  **可能性评估：**  无 |
| 已有消减措施 | 1.https传输，认证证书  2.认证消息头和时间戳 |
| 建议消减措施 | NA |
| 产品落地计划 | NA |
| 信息泄漏（I） | 风险（Risk） | **风险等级：低**  **影响：**  【影响】  泄露用户token信息  【可能性】  网络嗅探抓包分析  **可能性评估：**  无 |
| 已有消减措施 | 1.https传输 |
| 建议消减措施 | NA |
| 产品落地计划 | NA |
| 拒绝服务（D） | 风险（Risk） | **风险等级：低**  **影响：**  【影响】  攻击者发起大量请求导致统一Portal拒绝服务  【可能性】  攻击者模拟消息请求  **可能性评估：**  无 |
| 已有消减措施 | 1. 访问设置白名单IP控制  2.https配置证书认证  3.前段设有防火墙及Nginx进行流控 |
| 建议消减措施 | NA |
| 产品落地计划 | NA |

#### 用户⇔MKT Server(操作请求/Token/响应结果)

|  |  |  |
| --- | --- | --- |
| 元素名称 | 用户⇒MKT Server(操作请求/Token/响应结果) | |
| 元素概述 | 用户配置应用信息，查询统计数据 | |
| 威胁 | TID | |
| 篡改（T） | 风险（Risk） | **风险等级：低**  **影响：**  【影响】  数据被篡改后MKT执行错误的操作，用户看到异常的结果  【可能性】  劫持网元修改数据流内容  **可能性评估：**  无 |
| 已有消减措施 | 1.运维vpn或者iaccess通道，不对外提供服务  2.https加密传输 |
| 建议消减措施 | 1. 无 |
| 产品落地计划 | 1. 无 |
| 信息泄漏（I） | 风险（Risk） | **风险等级：中**  **影响：**  【影响】  泄露用户token及数据统计结果  【可能性】  网络抓包分析  **可能性评估：**  无 |
| 已有消减措施 | 1.运维vpn或者iaccess通道，不对外提供服务  2.https加密传输 |
| 建议消减措施 | 1. 无 |
| 产品落地计划 | 1. 无 |
| 拒绝服务（D） | 风险（Risk） | **风险等级：中**  **影响：**  【影响】  恶意攻击导致MKT拒绝服务  【可能性】  模拟数据攻击  **可能性评估：**  无 |
| 已有消减措施 | 1.运维vpn或者iaccess通道，不对外提供服务  2.域账号密码认证  3.设置有防火墙进行流控 |
| 建议消减措施 | 1. 无 |
| 产品落地计划 | 1. 无 |

### 处理过程分析

#### MKT Server

|  |  |  |
| --- | --- | --- |
| 元素名称 | MKT Server | |
| 元素概述 | 为用户提供操作入口,配置信息、生成BICODE代码以供后台统计数据使用、查询营销活动的广告位各类指标数据 | |
| 威胁 | STRIDE | |
| 仿冒（S） | 风险（Risk） | **风险等级：低**  **影响：**  【影响】  仿冒MKT为客户端浏览器提供服务  【可能性】  用户本地hosts被修改，或者DNS被劫持，导致用户 访问到仿冒的钓鱼网站  **可能性评估：**  无 |
| 已有消减措施 | 用户本地需要是vpn或iaccess接入，规避DNS被篡改 |
| 建议消减措施 | NA |
| 产品落地计划 | NA |
| 篡改（T） | 风险（Risk） | **风险等级：中**  **影响：**  【影响】  影响正常的业务逻辑  【可能性】  利用输入通道注入，获取相应权限篡改程序  **可能性评估：**  无 |
| 已有消减措施 | 1. 代码层面完成安全编码（codecc、代码检视等）  2.系统层面通过appscan扫描 防止出现注入  3.系统运行环境和容器定时更新漏洞 |
| 建议消减措施 | NA |
| 产品落地计划 | NA |
| 抵赖（R） | 风险（Risk） | **风险等级：低**  **影响：**  【影响】  修改系统配置信息  【可能性】  获取授权系统账号及数据库账号删除操作日志数据  **可能性评估：**  无 |
| 已有消减措施 | 1.只有运维人员通过vpn才能访问业务数据库  2.只有授权的Linux账号才能访问数据库并删除数据  3.通过接口等方式也无法访问日志数据  4.根据运维管理制度，运维人员定期修改密码 |
| 建议消减措施 | NA |
| 产品落地计划 | NA |
| 信息泄漏（I） | 风险（Risk） | **风险等级：低**  **影响：**  影响】  泄露系统信息  【可能性】  1.利用漏洞获取特权  **可能性评估：**  无 |
| 已有消减措施 | 1.系统中不存在涉及用户隐私的数据  2.appscan扫描防止漏洞出现  3.codecc 检查、规范日志 防止泄露系统信息  4.系统运行环境仅运维人员通过vpn接入才能访问 |
| 建议消减措施 | NA |
| 产品落地计划 | NA |
| 拒绝服务（D） | 风险（Risk） | **风险等级：低**  **影响：**  系统提供服务相应变慢  【可能性】  恶意用户Dos攻击  **可能性评估：**  无 |
| 已有消减措施 | 1. 内部系统，必须通过iaccess/vpn访问，用户量较少，且有操作日志。可以减少恶意攻击的风险  2. 关键资源有排队机制，超出范围数据等待  3.提供主备倒换能力  4.系统设有防火墙减少恶意攻击  5.运维对cpu、内存等使用情况有监控机制 |
| 建议消减措施 | NA |
| 产品落地计划 | NA |
| 特权提升（E） | 风险（Risk） | **风险等级：低**  **影响：**  【影响】  获得高级权限，查看高级数据或执行高级操作  【可能性】  低  **可能性评估：**  无 |
| 已有消减措施 | 1.账号使用华为域账号  2.权限基于角色进行管理  3.使用拦截器实现用户权限控制  4.以单独的linux账号运行程序，且仅分配必须的权限 |
| 建议消减措施 | NA |
| 产品落地计划 | NA |

### 数据存储分析

#### Mysql

|  |  |  |
| --- | --- | --- |
| 元素名称 | Mysql | |
| 元素概述 | 业务数据库，存储用户权限、统计数据、操作日志等 | |
| 威胁 | TRID | |
| 篡改（T） | 风险（Risk） | **风险等级：低**  **影响：**  【影响】  业务流程异常或数据异常  【可能性】  通过SSH登录MySQL服务器，在用MySQL账号密码登录MySQL，用MySQL命令修改或删除内容  **可能性评估：**  无 |
| 已有消减措施 | 1. 华为专有机房，只有华为运维人员才能登录  2. 业务通过JDBC访问MySQL是独立的最小授权用户  3. MySQL通过访问者的IP和用户名做了权限的控制  4. MySql与对应业务在同一内部组网中，进队该业务服务，不对外提供服务。  5. 运维每天例行备份数据库 |
| 建议消减措施 | NA |
| 产品落地计划 | NA |
| 抵赖（R） | 风险（Risk） | **风险等级：无**  **影响：**  NA  **可能性评估：**  NA |
| 已有消减措施 | NA |
| 建议消减措施 | NA |
| 产品落地计划 | NA |
| 信息泄漏（I） | 风险（Risk） | **风险等级：低**  **影响：**  【影响】  泄露业务数据  【可能性】  通过SSH登录MySQL服务器，在用MySQL账号密码登录MySQL，用MySQL命令查看  **可能性评估：**  无 |
| 已有消减措施 | 1. 华为专有机房，只有华为运维人员才能登录  2. 业务通过JDBC访问MySQL是独立的最小授权用户  3. MySQL通过访问者的IP和用户名做了权限的控制  4. MySql与对应业务在同一内部组网中，进队该业务服务，不对外提供服务。  5.涉及用户隐私的数据加密存储 |
| 建议消减措施 | NA |
| 产品落地计划 | NA |
| 拒绝服务（D） | 风险（Risk） | **风险等级：低**  **影响：**  【影响】  数据库不可用  【可能性】  1、写入大量数据导致存储空间变大  2、大量非法请求占用MySQL连接数，使正常请求无法进入  **可能性评估：**  无 |
| 已有消减措施 | 1. MySQL通过访问者的IP和用户名做了权限的控制,只有内部部件才能访问。  2、存储空间超过设置的阈值有告警。  3、运维监控对应设备的运行情况如cpu、内存、磁盘等 |
| 建议消减措施 | NA |
| 产品落地计划 | NA |

# 安全需求设计

## 传输安全需求

所有涉及与周边部件的交互必须确保传输过程是安全的。

1. 本系统与周边部件的交互，必须使用内部ip进行，且配置有对应的白名单。
2. 本系统与用户交互的部分，采用的是web方式，必须采用https传输协议。同时要求用户必须登录运维vpn或者公司iaccess。当用户使用vpn登录时，用户请求直接经过vpn通道达到服务器。

当用户通过iaccess访问时，请求通过iaccess先到达公司研发区域的HIS反向代理，在有反向代理链接北京华为机房的nginx代理，所以要求nginx代理使用白名单方式控制访问请求，仅允许HIS反向代理和vpn通道进行访问。

## YY需求

# 各模块的分配需求

本章节从模块的角度罗列各个模块上的分配需求。

例如，分配在CC这个模块的系统需求如下：

（1）VPDN用户认证时，同一般PPP用户一样，认证信息送AAA认证处理；当收到AAA的认证响应时，直接返回给PPP模块处理；

（2）接受L2TP模块会话CID的申请、释放处理；通知L2TP会话拆除；

（3）在CIB表项中互存CID以及所在槽位信息以关联VPDN用户的PPP会话和L2TP会话；

（4）在L2TP通知会话连接建立时，维护L2TP会话CIB表，并下发到SPUE业务板；在L2TP通知会话连接拆除时，清除L2TP会话CIB表，同时通知用户对应的PPP会话拆除连接；在由AAA通知会话拆除时，则同时通知用户对应的PPP会话和L2TP会话连接拆除；

（5）在PPP上报连接UP时，通过CA模块下发PPP CIB表项到用户侧接口板LPUI(SPU)，同时向AAA发送启动计费通知； 而PPP上报连接DOWN时，向AAA发送停止计费通知，并在AAA通知清除表项时，清除PPP CIB表项，并同步清除对应接口板上表项。

# 各模块的接口描述

本章节从模块的角度罗列各个模块的接口。

建议采用以下形式描述：

1. 样表：XX功能接口表

|  |  |  |  |
| --- | --- | --- | --- |
| 接口名称 | 接口类型 | 涉及的模块 | 描述 |
| LRCI | 点对点消息通信 | OMA调用CLRC | 此接口完成XXX功能，。。。 |
|  |  |  |  |

# 备注和附录

本章节描述需要说明的附加内容。如果使用了DFD方法，则可能需要下面的“数据流图”和“数据字典”的章节。

## 数据字典

### 数据字典列表

罗列用到的数据名称和定义。

参考资料清单：

请罗列本文档所参考的有关参考文献和相关文档，格式如下：

作者＋书名（或杂志、文献、文档）＋出版社（或期号、卷号、公司文档编号）＋出版日期+起止页码

例如：

1. D. B. Leeson, “A Simple Model of Feedback Oscillator Noise Spectrum,” Proc. IEEE, pp329-330, February 1966
2. D. Wolaver, Phase-Locked Loop Circuit Design, Prentice Hall, New Jersey,1991