分布式Wi-Fi破解系统

版本 <1.0>

修订历史记录

|  |  |  |  |
| --- | --- | --- | --- |
| **日期** | **版本** | **说明** | **作者** |
| 2015年11月12日 | <0.1> | 初稿 | 刘浩 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

目录

1. 简介 3

1.1 目的 3

1.2 范围 3

1.3 定义、首字母缩写词和缩略语 3

1.4 参考资料 3

1.5 概述 3

2. 整体说明 3

3. 具体需求 3

3.1 功能 3

3.1.1 <功能性需求一> 3

3.2 可用性 3

3.2.1 <可用性需求一> 3

3.3 可靠性 3

3.3.1 <可靠性需求一> 3

3.4 性能 3

3.4.1 <性能需求一> 3

3.5 可支持性 3

3.5.1 <可支持性需求一> 3

3.6 设计约束 3

3.6.1 <设计约束一> 3

3.7 联机用户文档和帮助系统需求 3

3.8 购买的构件 3

3.9 接口 3

3.9.1 用户界面 3

3.9.2 硬件接口 3

3.9.3 软件接口 3

3.9.4 通信接口 3

3.10 许可需求 3

3.11 法律、版权及其他声明 3

3.12 适用的标准 3

4. 支持信息 3

# 简介

本文档以传统的自然语言表达SRS而不涉及用例建模。对于涉及用例建模的SRS，请参见《用例实现规约》。

## 目的

[阐明此 **SRS** 的目的。**SRS** 应详细地说明所确定的应用程序或子系统的外部行为。它还要说明非功能性需求、设计约束以及提供完整、综合的软件需求说明所需的其他因素。]

本文档主要说明Wi-Fi Cracker 的功能、性能、可用性等质量需求。

## 范围

[简要说明此 **SRS** 适用的软件应用程序、特性或其他子系统分组、与其相关的用例模型，以及受到此文档影响的任何其他事物。]

本系统采用分布式运算以高效的破解Wi-Fi密码，整个系统由多个应用程序构成。 本系统最终会产生多少个应用程序取决于软件的构架设计，为了便于说明，我们假设本系统包含以下几个应用程序：抓包应用程序(CaptureApp)、破解应用程序(CrackApp)、分布式处理应用程序(DistributionAgentApp， DistributionServerApp)。 本分布式系统的涉及3个硬件单元，分别是：CrackRouter， CrackServer，CrackStation。

本文档将介绍运行于CrackServer和CrackStation的软件完整的需求规格。运行于CrackRouter 上面的软件分为2部分：路由器软件、Wi-Fi破解软件。 路由器软件是所有家用路由器必备的软件，为了完成Wi-Fi破解的功能，我们需要对路由器软件做一部分的修改。 本文档将不会详细描述路由器软件相关的需求，仅仅列举出为了完成Wi-Fi破解，路由器软件应该提供给Wi-Fi破解软件的接口。 同时，本文档也会详细说明CrackRouter上的Wi-Fi破解软件的软件需求规格。

## 定义、首字母缩写词和缩略语

[本小节应提供正确理解此 **SRS** 所需的全部术语的定义、首字母缩写词和缩略语。 这些信息可以通过引用项目词汇表来提供。]

SRS: Software Requirement Specification, 软件需求规约。

CrackRouter: 内置了Wi-Fi Cracker 软件的家用路由器。其主要功能为：抓包， 破解， 为CrackStationA分配破解任务。

CrackStation： 运行Windows的PC。CrackStation分为两类： 第一类是通过CrackRouter的LAN口连接到CrackRouter的PC，我们为其命名为CrackStationA。 第二类是没有通过CrackRouter的LAN口连接到CrackRouter的PC，我们为其命名为CrackStationB。

CrackServer: 运行Linux（或Windows）的PC服务器。

InternetConnectionState: CrackRouter到internet连接状态。InternetConnectionState可以有3种状态，Disconnected, StrainedConnected, FreeConnected。 Disconnected表示当前CrackRouter没有连接到Internet。StrainedConnected 表示当前CrackRouter连接到了internet，但是能使用流量受限， 当用户的路有器没有备用的internet连接时，为了上报Crack任务到CrackServer，我们可能会提示用户将自己的手机作为internet的连接入口，用最少的流量完成任务的分发， 此时，Station的连接状态就属于StrainedConnected。 当前CrackRouter有免流量费的连接到internet时，其连接状态就是FreeConnected。

LocalCrackRouterGroup: 能同时监听同一台TargetRouter的数据包的多台CrackRouter属于同一个LocalCrackRouterGroup。

TargetRouter: 当前Wi-Fi Cracker 的攻击对象。

TargetStation: 和 TargetRouter 建立了连接的Station， 可以是PC 或 其他类型的移动终端，如手机等。

## 参考资料

[本小节应完整列出此 **SRS** 中其他部分所引用的任何文档。每个文档应标有标题、报告号（如果适用）、日期和出版单位。列出可从中获取这些参考资料的来源。这些信息可以通过引用附录或其他文档来提供。]

## 概述

[本小节应说明该 **SRS** 中其他部分所包含的内容，并解释此文档的组织方式。]

# 整体说明

[**SRS** 的这一节应说明影响产品及其需求的一般因素。本节并不列出具体的需求，而只是提供在第 3 节中详述的各种需求的背景，以使这些需求便于理解。所包括的内容有：

• 产品总体效果

• 产品功能

• 用户特征

• 约束

• 假设与依赖关系

• 需求子集]

## 整体流程/逻辑关系



## 产品总体效果

CrackRouter 可实时地监听无线范围内的TargetRouter和TargetStation之间的数据包，并通过CrackServer查询当前TargetRouter的Wi-Fi密码，查询成功则使用此密码连接到互联网。 如果查询失败，CrackRouter自动启动破解过程。CrackRouter可根据TargetRouter使用的协议（WEP/WPA），选择最适合的破解算法。 另外，CrackRouter根据internet的连接状态，选择合适的分布式任务分配算法。

为了加快WPA协议的破解效率，我们可动态的增加CrackStation， 特别是CrackStationB。最有效的办法就是和网吧合作，以此增加CrackStationB。 或者， 我们也可以研究并通过木马的方式将我们CrackApp安装到尽可能多的PC上。

CrackStation, CrackRouter, CrackServer上的软件都可以通过配置自动升级到最新版本。

## 约束

第1版的CrackRouter只支持WEP, WPA加密算法的破解。其中WEP采用PTW破解算法，其成功率取决于CrackRouter能在多长时间内监听到数量足够多的数据包。 WPA采用暴力破解算法， 起成功率和破解效率取决于WPA密码的长度及密码可能包含的字符集合。

## 假设与依赖关系

CaptureApp运行的平台也就是家用路由器/带无线网卡的PC。 为了完成抓包过程，我们假设家用路由器具有以下功能：

1. Router 提供API，让CaptureApp设置 开始/停止 抓包。
2. Router 提供API，让CaptureApp注册抓包相关的API。
3. Router提供API，让CaptureApp获取当前路由器的运行状态的通知。 可通知的状态包括：Wi-Fi芯片相关的状态， 用户上网的状态， CPU利用率的状态， 内存利用率的状态。 抓包进程根据这些状态来决定如何使用Router的CPU和Wi-Fi芯片资源。
4. Router 提供API， 让CrackApp获取当前Router的Wi-Fi密码，并上报到CrackServer。
5. Router提供API， 让CrackApp注册回调函数， Router在连接到TargetRouter前，通知注册的回调函数查询TargetRouter 密码信息。
6. Router 提供用户界面，指导用户完成LocalCrackStation的下载， 并启动LocalCrackStation。

# 具体需求

**SRS** 的这一节应包含所有的软件需求，其详细程度应使设计人员能够设计出可以满足这些需求的系统，并使测试人员能够测试该系统是否满足这些需求。 当利用用例建模时，这些需求在用例和适用的补充规约中记录。如果没有利用用例建模，则可以将补充规约的概要直接插入此节。如下所示。]

## 功能

[此节为以自然语言风格表达的需求说明为此设计的系统功能性需求。对于许多应用程序，此节会成为 **SRS** 包的主体部分，所以应仔细考虑此节的组织方式。此节通常按特性来组织，但也可能会有其他适用的组织方式，例如按用户或子系统组织的方式。功能性需求可能包括特性集、性能和安全性。

当利用应用程序开发工具（如需求工具、建模工具等）来获取功能性时，此节文档将引用获取相应数据的方法，并指出用来获取数据的工具的位置和名称。]

### Wi-Fi 协议支持

|  |  |
| --- | --- |
| 功能描述 | 本软件支持WEP， WPA 协议的Wi-Fi密码破解。 其中WEP 采用PTW算法破解。 WPA 采用分布式的暴力算法破解。 |
| 处理流程 | 无 |
| 说明 | 分布式破解要求CrackRouter连接到internet。 |
| 质量属性 | 可用性: 1 在正常运行的场景下, CrackRouter在判定TargetRouter使用的WEP协议，并已经开始了破解过程， 此时如果CrackRouter监听到了来自TargetRouter的WPA包， 说明TargetRouter的配置发生了变化。此时，CrackRouter应该中断破解任务， 并重启新的破解任务。  性能: 在抓包成功的情况下， WEP 在2分钟之内完成破解过程， WPA 分布式破解争取做到75% 的情况下在60分钟内完成破解。 |
| 优先级 | 高 |

### Wi-Fi 云端存储，多用户共享

|  |  |
| --- | --- |
| 功能描述 | 任何时候，只要CrackRouter获取到了新的TargetRouter的密码， CrackRouter都会将此密码发送给CrackServer， CrackServer将此密码保存到数据库。 将来只要有新的CrackRouter需要连接到此TargetRouter， 在开始破解之前都先会查询数据库。  另外，CrackRouter也会将自己的密码保存到云端。 CrackRouter的用户不可设置是否共享自己的网络给其他CrackRouter。 |
| 处理流程 | 无 |
| 说明 | 分布式破解要求CrackRouter连接到internet。 |
| 质量属性 | 性能: 在抓包成功的情况下， WEP 在2分钟之内完成破解过程， WPA 分布式破解争取做到75% 的情况下在60分钟内完成破解。 |
| 优先级 | 高 |

### Wi-Fi 云端存储，多用户共享

|  |  |
| --- | --- |
| 功能描述 | 在正常运行的场景下, 如果CrackRouter通过云端获取到了某台TargetRouter的密码后登陆失败，说明TargetRouter的密码已经被修改过了，或者TargetRouter上设置了MAC地址过滤，此时CrackRouter应该为相应的记录设置标志位，并尝试重新开启破解任务，并在任务成功后修改云端的记录 。 |
| 处理流程 | 无 |
| 说明 | 无 |
| 质量属性 | 性能: 在抓包成功的情况下， WEP 在2分钟之内完成破解过程， WPA 分布式破解争取做到75% 的情况下在60分钟内完成破解。 |
| 优先级 | 高 |

### 环路检测

|  |  |
| --- | --- |
| 功能描述 | 多台CrackRouter共享internet连接资源时， 需要做环路检测。否则，上行数据可能在多台CrackRouter之间形成死循环。 |
| 处理流程 | 无 |
| 说明 | 此功能属于CrackRouter中Router的功能。 |
| 质量属性 | 无 |
| 优先级 | 中 |

### Wi-Fi覆盖范围内的CrackRouter共享TargetRouter的Wi-Fi密码

|  |  |
| --- | --- |
| 功能描述 | CrackRouter 实时通过Wi-Fi的广播本地的TargetRouter的密码。 用户新买的CrackRouter在没有internet连接的情况下， 可通过邻近的CrackRouter连接到CrackServer。 |
| 处理流程 | 无 |
| 说明 | 分布式破解要求CrackRouter连接到internet。 |
| 质量属性 | 无 |
| 优先级 | 高 |

### CrackRouter, CrackStation软件动态升级

|  |  |
| --- | --- |
| 场景 | CrackRouter, CrackStation连接到internet |
| 功能描述 | Crack相关的可执行文件、字典、配置文件可动态升级。 |
| 处理流程 | CrackRouter 按照一定的时间间隔查询CrackServer上最新的软件版本，如发现新版本，启动升级过程。 |
| 说明 |  |
| 质量属性 | 可用性：   1. 尽可能的确保升级过程不影响CrackRouter的正常运行。 2. 升级过程智能化，不需要用户参与。 3. 升级过程中， 用户如果通过IE上网， 确保用户可得到正确的提示（如华为的路由器）， 此功能为需要router的支持。 |
| 优先级 | 高 |

### CrackServer软件升级

|  |  |
| --- | --- |
| 功能描述 | CrackServer相关的可执行文件、字典、配置文件升级。 |
| 处理流程 | 1. 管理员新版本的可执行文件及升级脚本上传到指定目录. 2. 管理员登陆到CrackServer的管理页面，输入升级文件的路径，点击升级按钮。 |
| 说明 | 如果CrackServer存在双机备份, 参考交换机堆叠的升级流程. |
| 质量属性 | 可用性:   1. 升级期间, 服务中断时间少于1分钟. 2. 根据升级可能涉及到的修改（如： 数据库的表结构是否需要修改）, 升级过程有不同的算法, 升级算法可动态修改. |
| 优先级 | 高 |

### 为破解任务划分优先级

|  |  |
| --- | --- |
| 场景 | CrackStation 可能同时收到了多个破解任务 |
| 功能描述 | 为了高效的破解， CrackStation为破解任务划分优先级，并按照优先级从高到低的方式执行破解。  破解过程中， 优先级是动态变化的， 如：WPA暴力破解的字典项被分解为多个子字典,每个子字典的优先级各不相同。  任务的优先级范围为 1~10000。 |
| 处理流程 | 无 |
| 说明 | 优先级计算的输入参数为： 协议类型（WEP， WPA）， 任务地址属性（本地，异地任务）， 字典常用指数，任务目的类型（测试任务，真实任务），任务的发起者（CrackRouter）是否已经有可正常使用的internet接入方式。 |
| 质量属性 | 可修改性:   1. 优先级计算的算法可动态修改。 |
| 优先级 | 高 |

### 为破解任务分配合理的资源

|  |  |
| --- | --- |
| 功能描述 | CrackRouter 可能在不影响用户上网的同时完成破解任务  在监听TargetRouter 通讯的同时， CrackRouter可能已经有其他的Internet接入账号了。 此时， CrackRouter需要首先确保用户上网的功能不中断的同时，最大可能的完成破解任务。  CrackRouter中主要包含2种可分配的资源： CrackRouter的CPU资源， CrackRouter的Wi-Fi芯片资源。 Wi-Fi芯片可能影响到用户是否能够在上网的同时，CrackRouter还在抓取TargetRouter的握手包。 |
| 处理流程 | 无 |
| 说明 | 实现时需要考虑到 CrackRouter 的Wi-Fi芯片的特性。 首先需要确保抓包过程不影响用户正常上网。  有可能需要修改硬件设计。 |
| 质量属性 | 可修改性:   1. 资源分配的算法可动态修改， 不同的CrackRouter芯片可采用不同的算法。 |
| 优先级 | 高 |

### CrackStation多种获取Crack任务的方式

|  |  |
| --- | --- |
| 功能描述 | 根据CrackStation的不同类型(CrackStationA, CrackStationB), CrackStation有2种不同的获取破解任务的方式:   1. CrackStationA 只从本地CrackRouter获取破解任务. 2. CrackStationB 只从CrackServer获取破解任务。 |
| 处理流程 | 无 |
| 说明 | 无 |
| 质量属性 | 无 |
| 优先级 | 中 |

### WPA分布式破解

|  |  |
| --- | --- |
| 功能描述 | 为了提高破解效率, WPA破解任务支持分布式破解。 CrackRouter在收集到了WPA的握手包以后，通过CrackServer将任务分发到所有的CrackStation。 |
| 处理流程 | 无 |
| 说明 | 无 |
| 质量属性 | 可用性：   1. CrackServer 要求24\*7 不间断运行。 一年中终止服务的时间低于5小时。 2. CrackStation和CrackServer间的流量控制。 设计合理的通讯机制，字典划分的粒度，以确保使用最少的网络流量。 |
| 优先级 | 中 |

## 安全性

### 数据库安全

CrackRouter没有权限直接访问数据库， 必须通过CrackServer间接的读写数据库中的记录。CrackServer 连接数据时， 必须提供正确的用户名+密码。 数据库的用户名+密码保存在CrackServer的加密过的配置文件中。CrackServer解密配置文件的算法是动态配置的， 其目的在于避免本公司员工获得知道了加密算法后非法的访问数据库中的内容。 开发过程中，加密算法为空算法， 以方便程序调试。

### CrackServer 安全

CrackRouter 请求连接到CrackServer时， 必须要有认证过程。

CrackRouter 和CrackServer之间的通讯必须要加密， 以防止非法的CrackRouter破坏数据库的内容。

CrackServer 具备防止DOS攻击的能力。

## 可用性

[此节应包括所有影响可用性的需求。例如，

• 指出普通用户和高级用户要高效地执行特定操作所需的培训时间

• 指出典型任务的可评测任务次数或根据用户已知或喜欢的其他系统确定新系统的可用性需求

• 指出在符合公认的可用性标准（如 IBM 的 CUA 标准和 Microsoft 的 GUI 标准）方面的需求]

### 有效的检查监听到的用户破解的数据包的正确性

为了确保数据包错误不会造成故障。 CrackRouter在监听到TargetRouter 和TargetStation之间的数据包时， 首先需要检查数据包的正确性和完整性。 CrackServer 收到来自CrackRouter的数据包时，也需要数据包的完整性和正确性（可利用TCP 自带的校验和来确保任务的完整性）。

### 破解过程不影响用户CrackRouter的最最基本的功能：即一个普通路由器的功能

如果CrackRouter上的破解相关进程崩溃，不影响连接到CrackRouter的终端正常的伤亡的功能。

如果CrackRouter上的破解相关进程崩溃， 在一定的时间内这些进程会被重启。

CrackRouter上的破解相关进程不至于占用太多的CPU和内存资源， 否则将对上网的功能造成负面影响。

CrackRouter在监听数据包时， 不影响用户正常上网。

### CrackServer 24\*7 不间断工作

CrackServer 要求24\*7 不间断运行。 一年中终止服务的时间低于5小时。

CrackServer 的数据库需要每天备份一次，保存到云存储的云端。

## 可靠性

[对系统可靠性的需求应在此处说明。以下是一些建议：

• 可用性—指出可用时间百分比 ( xx.xx%)、使用小时数、维护访问权、降级模式操作等。

• 平均故障间隔时间 (MTBF) – 通常表示为小时数，但也可表示为天数、月数或年数。

• 平均修复时间 (MTTR) — 系统在发生故障后可以暂停运行的时间。

• 精确度 — 指出系统输出要求具备的精密度（分辨率）和精确度（按照某一已知的标准）。

• 最高错误或缺陷率—通常表示为每千行代码的错误数目 (bugs/KLOC) 或每个功能点的错误数目 (bugs/function-point)。

• 错误或缺陷率—按照小错误、大错误和严重错误来分类。需求中必须对“严重”错误进行界定，例如：数据完全丢失或完全不能使用系统的某部分功能。]

### <可靠性需求一>

[需求说明。]

## 性能

[此节应概述系统的性能特征。其中需包括具体的响应时间。如果可行，按名称引用相关用例。

• 对事务的响应时间（平均、最长）

• 吞吐量，例如每秒处理的事务数

• 容量，例如系统可以容纳的客户或事务数

• 降级模式（当系统以某种形式降级时可接受的运行模式）

• 资源利用情况，如内存、磁盘、通信等

### <性能需求一>

[在此给出需求说明。]

## 可支持性

[此节应列出将提高所构建系统的可支持性或可维护性的所有需求，其中包括编码标准、命名约定、类库、维护访问权和维护实用程序。]

### <可支持性需求一>

[在此给出需求说明。]

## 设计约束

[此节应列出所构建系统的所有设计约束。设计约束代表已经批准并必须遵循的设计决定。其中包括软件语言、软件流程需求、开发工具的指定用途、构架及设计约束、购买的构件、类库等。]

### <设计约束一>

[在此给出需求说明。]

## 联机用户文档和帮助系统需求

[如果存在对联机用户文档、帮助系统、关于声明的帮助等的需求，请在此说明。]

## 购买的构件

[此节说明在系统中使用的所有购入构件、所有适用的许可或使用限制，以及所有相关的兼容性及互操作性或接口标准。]

## 接口

[此节规定应用程序必须支持的接口/界面。它应非常具体，包含协议、端口和逻辑地址等，以便于按照接口/界面需求开发并检验软件。]

### 用户界面

[说明软件将实现的用户界面。]

### 硬件接口

[此节指出软件所支持的所有硬件接口，其中包括逻辑结构、物理地址、预期行为等。]

### 软件接口

[此节说明软件系统中与其他构件之间的软件接口。这些构件可以是购入的构件、取自其他应用程序重新利用的构件，也可以是为此 **SRS** 范围之外的子系统开发，但该软件应用程序必须与之交互的构件。]

### 通信接口

[说明与其他系统或设备（如局域网、远程串行设备等）的所有通信接口。]

## 许可需求

[定义所有许可执行需求或软件将体现的其他使用限制需求。]

## 法律、版权及其他声明

[此节说明软件涉及的所有必需的法律免责声明、保证、版权声明、专利声明、字标、商标或徽标符合性问题。]

## 适用的标准

[通过引用，此节说明了所有适用的标准以及适用于所述系统的相应标准的具体部分。例如，其中可以包括法律、质量及法规标准；业界在可用性、互操作性、国际化、操作系统相容性等方面的标准。]

# 支持信息

[支持信息用于使 **SRS** 更易于使用。它包括：

• 目录

• 索引

• 附录

其中可以包括用例示意板或用户界面原型。

如果包含附录，**SRS** 应明确指出是否将附录当作需求的一部分。]