安全认证

吉富逵

2019/6/27

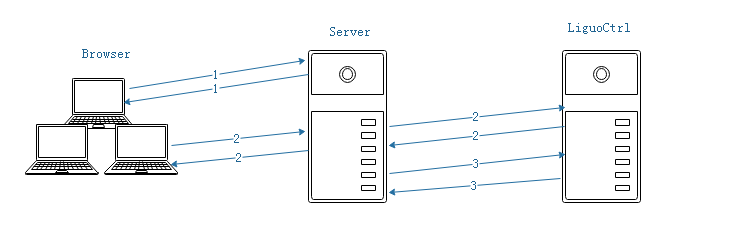
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Edition ID** | **Date** | **Author** | **Version** | **Description** |
| 1.0 | 27Jun. 2019 | 吉富逵 | 1.0.0 | 预订 |

# 目的

本文档的目的是为以后利国网页安全认证程序的指导性文件和功能测试的依据。

# 功能简介

利国带有网页的控制的设备的结构框图如下图所示。



网页控制结构图

由图可以知道用户进行网页请求主要分为两种：一种是直接访问服务器资源（路线1），一种是获取设备资源需要通过Server作为桥梁获取LiguoCtrl的数据资源。安全认证应当属于服务器资源，由于LiguoCtrl是整个服务的核心控制整个设备服务的运行状态所以Server需要通知LiguoCtrl安全状态的变化，LiguoCtrl可以对Server安全认证的状态进行控制和更新修改查看删除服务器用户信息。

## 2.1前端网页功能

1.安全认证网页。

2.用户名密码前端限制。

3.根据权限定义功能、页面、操作的可行性。

## 2.2服务端功能

1.用户名密码认证。

2.向LiguoCtrl通知安全状态变化。

3.更新用户名密码。

## 2.3LiguoCtrl功能

1.广播安全状态变化时的安全状态。

2.设置查询服务器安全状态。

# 3.测试功能

## 3.1认证关闭

认证关闭时，不需要输入用户名和密码即可登录设备控制网页进行网页的控制。

## 3.2认证打开

进入控制网页需要进行安全认证，认证成功进入控制网页，认证失败继续认证，取消认证显示认证失败网页。

## 3.3认证状态变化

（1）改变认证状态，需要Admin密码。

（2）认证状态变化成功，向LiguoCtrl通知认证状态的变化，根据/nandflash/webserver/thttpd/bin/security.json 的security 字段的数值判断安全状态非0为安全认证打开，0为安全状态关闭。

{"security": 1, "User": [{"username": "Admin", "password": ""}]}。

（3）由认证关闭到认证打开所有连接的请求进行安全认证。

## 3.4用户密码修改

（1）需要原始密码和修改之后的密码

（2）密码修改成功根据安全状态判断是否进程安全认证，对于需要认证的所有打开的连接都需要重新进行安全认证。

## 3.5设备复位

（1）设备出厂复位时首先删除/nandflash/webserver/thttpd/bin/security.json此文件，默认状态安全关闭，用用只有一个Admin密码为空字符串。

（2）重新启动thttpd程序。

# 4.测试

（1）安全状态在服务器端和LiguoCtrl端和浏览器端的状态一致。

（2）密码在服务器端和浏览器端一致。

（3）安全状态和密码和上述叙述效果一致。

（4）IE10及以上，Chrome，Firefox浏览器测试。