**智能家居系统**

**安全设计**

|  |  |
| --- | --- |
| 文档编号： |  |
| 编 写 人： | 王斐 |
| 审 批 人： | [经理] |
| 生效日期： | 2015/11/16 |

**爱悠团队**

文档历史：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 版本 | 修订者 | 修订内容 | 修订日期 | 审批者 | 审批日期 |
| 0.1.0 | 王斐 | 文档初稿 | 2015-11-21 |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

*填写说明：*

* *版本号规则：版本号采用三级生成规则，即0.0.0，第一位表示主版本号，每一次正式发布，主版本号加1，第二位表示从版本号，每一次对文档进行较大范围修订（增、删章节，修改内容主干等），从版本号加1；第三位为修订版本号，在不改变文档主体内容结构与思想，只做文字上的修饰与调整，则修订版本加1。版本号不采用进制策略，按规则累加，当上层版本变化时，次级版本归0。例如0.0.92，当从版本号升为1时，修订版本号归0，成为0.1.0。*
* *修订内容：详细描述修订及修订内容所在章节*

目 录

[1 引言 4](#_Toc435869424)

[1.1 编写目的 4](#_Toc435869425)

[1.2 项目背景 4](#_Toc435869426)

[1.3 名词解释 4](#_Toc435869427)

[1.4 参考资料 4](#_Toc435869428)

[2 整体架构 5](#_Toc435869429)

[3 账户安全 7](#_Toc435869430)

[3.1 单点登录 7](#_Toc435869431)

[3.2 密码加密存储 7](#_Toc435869432)

[4 设备安全 8](#_Toc435869433)

[4.1 设备编码 8](#_Toc435869434)

[4.2 设备验证 9](#_Toc435869435)

[5 App安全 9](#_Toc435869436)

[5.1 App加密 10](#_Toc435869437)

[5.2 分配令牌 10](#_Toc435869438)

[5.3 验证令牌 10](#_Toc435869439)

[5.4 令牌失效机制 10](#_Toc435869440)

[5.5 短信验证 10](#_Toc435869441)

[6 协议安全 11](#_Toc435869442)

[6.1 协议校验 11](#_Toc435869443)

[7 通信安全 11](#_Toc435869444)

[7.1 TLS加密 12](#_Toc435869445)

[7.1.1 Kamailio开启TLS加密 12](#_Toc435869446)

[7.1.2 网关设备开启TLS加密 13](#_Toc435869447)

[7.1.3 App开启TLS加密 13](#_Toc435869448)

[7.2 HTTPS加密 13](#_Toc435869449)

[7.2.1 Nginx启用HTTPS 13](#_Toc435869450)

[8 附录 14](#_Toc435869451)

# 引言

## 编写目的

优化智能家居系统的架构设计，弥补之前的系统安全设计空缺，避免智能家居系统的安全风险。

## 项目背景

智能系统开发进行中。

## 名词解释

SSO: 单点登录（Single Sign On），是在多个应用系统中，用户只需要登录一次就可以访问所有相互信任的应用系统。它包括可以将这次主要的登录映射到其他应用中用于同一个用户的登录的机制。它是目前比较流行的企业业务整合的解决方案之一。

Kamailio：目前世界上使用比较广泛的开源SIP服务器平台，由OpenSER和SER演进而来，可以开发大型的VoIP平台，实时通信系统，同时也可以和媒体服务器Asterisk/FreeSWITCH对接来实现PSTN网关，PBX 应用功能。

TLS：安全传输层协议（Transport Layer Security），用于在两个通信应用程序之间提供保密性和数据完整性。该协议由两层组成： TLS 记录协议（TLS Record）和 TLS 握手协议（TLS Handshake）。较低的层为 TLS 记录协议，位于某个可靠的传输协议（例如 TCP）上面，与具体的应用无关，所以，一般把TLS协议归为传输层安全协议。

SAML：安全断言标记语言(Security Assertion Markup Language)，是一个基于XML的标准，用于在不同的安全域(security domain)之间交换认证和授权数据。在SAML标准定义了身份提供者(identity provider)和服务提供者(service provider)，这两者构成了前面所说的不同的安全域。 SAML是OASIS组织安全服务技术委员会(Security Services Technical Committee)的产品。

## 参考资料

* 百度百科: http://baike.baidu.com/
* Kamailio软交换中文社区：http://www.kamailio.org.cn/
* 《网关SN码定义》
* 《云端与网关通信协议》
* The README of TLS module is now a complete tutorial about how to tune the parameters for TLS configuration：http://kamailio.org/docs/modules/devel/modules/tls.html
* Configuring TLS support in Kamailio 3.1：http://nil.uniza.sk/network-security/tls/configuring-tls-support-kamailio-31-howto

# 整体架构

整体架构包括账户安全、设备安全、App安全、协议安全、通信安全，整体架构如下图所示。



# 账户安全

账户安全是指保障用户的个人信息安全，避免用户的密码被窃取，避免用户的个人信息泄露。账户安全措施包括单点登录、密码加密存储。

## 单点登录

系统中所有模块应形成一个整体，实现：

* 统一用户管理。实现用户信息的集中管理，并提供标准接口。
* 统一认证。用户认证是集中统一的，用户名/密码、B/S和C/S等多种身份认证方式。
* 单点登录。支持不同域内多个应用系统间的单点登录。

单点登录采用SAML解决方案，使用SimpleSAMLphp实现统一认证服务。认证系统应提供：

* 统一的用户注册API。
* 统一的用户登录认证API。

各模块在处理用户注册和用户登录、退出操作业务时，应统一调用SimpleSAMLphp服务器提供的API，并根据返回结果处理下一步业务。

## 密码加密存储

为保证用户密码安全，保障即使用户的密码是一样的，加密后保存的密码也是不同的，数据库中存储密码的字段应设为CHAR(64)的长度，该字段的内容由两部分组成：

1．MD5(时间戳) 做为密钥；

2．MD5(用户密码+密钥) + 密钥作为为数据库存储的最终密码。

当用户登录时，系统首先获取用户输入的密码跟数据库存储的密码，截取出盐部分重新加密，判断是否一致。具体实现的PHP代码如下：

*protected function encryption($key)*

*{*

*return md5($key . md5(intval(LARAVEL\_START))) . md5(intval(LARAVEL\_START));*

*}*

*/\*\**

*\* @power 断言输入的密码是否和DB的是一样的*

*\* @param $key 输入的密码*

*\* @param $value DB中的密码*

*\* @return bool*

*\*/*

*protected function assertEncryption($key, $value)*

*{*

*if (strlen($value) != 64) {*

*return 0;*

*}*

*//拿到盐*

*$salt = substr($value, 32, 63);*

*return md5($key . $salt) . $salt == $value;*

*}*

# 设备安全

设备安全是指公司出售的产品统一记录和授权，仅经过系统授权过的设备可接入系统正常工作，避免未经授权或伪装的设备进入系统，干扰系统的正常运行。设备安全包括设备编码、设备验证。

## 设备编码

设备编码是指公司对生产出的设备，按照预先制定的规则，每个设备分配一个唯一的设备ID，用于标识设备唯一性。设备入库时，设备ID连同设备的其他信息一起入库记录。

网关设备ID的定义如下：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 网关S/N码定义 | | 定义说明 | 确定时间 |  |
|  |
| 包括内容 | 条码格式：SYYWWVVXXXXN | 共12位数字 | 2015/11/10 |  |
| 厂家代码：S | S=1至9，数字 |  |
| 生产日期：YYWW | YY=年份，如：15表示2015年 WW=周期，如：45表示第45周，包含11月1日至7日 |  |
| 产品版本：VV | 从00至99 |  |
| 流水号：XXXX | 从0001开始，到9999结束 |  |
| 扩展码：N | 0至9，数字，默认为9 |  |
| 备注：如上数字均为十进制数字 | |  |

## 设备验证

设备ID入库后，系统中就生成了以设备ID为唯一标识的设备记录。设备在连接到云端系统时，需主动上报本设备所分配的ID作为身份凭证。

云端的Kamailio服务后台接收到网关的入网连接请求后，应做如下处理：

1. 查询网关设备ID是否已在系统数据库中登记过；
2. 若登记过，则进行下一步业务处理；
3. 若未登记过，则返回未找到设备ID信息的错误结果，并中断与该网关设备的连接。

# App安全

App安全用于在优化用户体验的前提下，对部分App源码进行加密处理和对连入系统的App做安全审核，避免伪造的App请求干扰系统的正常运行。

## App加密

由于未加密的Android App存在被反编译后泄露源代码的风险，因此Android App的apk文件必须经过加密后方可对外发布，避免恶意用户反编译智能家居App后，干扰系统的正常运行。

## 分配令牌

用户在App上执行用户登录操作后，云端系统应给App分配一个系统唯一的令牌（Token）作为系统认证App后的阶段性标识ID:

* Token使用CHAR(36)存储；
* 系统应记录用户ID与App Token的对应关系；
* App在请求操作智能设备时，需上传用户ID和App Token。

## 验证令牌

系统应对App发送的智能家居设备操作请求验证Token的有效性：

1. 验证App上传的Token是否为系统分配的合法Token；
2. 验证Token是否在有效期内；
3. 验证Token是否与用户ID匹配。

## 令牌失效机制

云端分配给App的Token，并非永久有效，在一定的条件下会失效：

1. 用户在App上执行用户退出操作时；

2. 用户卸载App后；

3. 用户更换手机后，在新手机登录App；

4. 系统检测到用户使用App的行为异常；

5. 用户长时间未使用App，超过1个月的Token有效期。

Token失效后，用户需在App重新进行用户登录操作，以获取更新后的有效Token。

## 短信验证

短信验证用于系统验证用户手机号码的真实性及确认用户的重要操作业务，包括：

* 用户使用手机号注册；
* 用户绑定手机号；
* 系统检测到用户账号异常，通过手机号验证用户；

短信中的验证码由云端生成并通过调用云端的统一API发送到用户手机:

1. 若用户输入正确的验证码，则继续进行下一步业务；
2. 若用户输入错误的验证码，则提示用户输入的验证码有误，停留在本页面继续等待用户重新输入；
3. 单用户再次请求发送验证码的等待时间为60s。

# 协议安全

协议安全用于校验智能家居的通信协议有效性，避免通信协议被窃听后遭到伪造，从而干扰智能家居系统的正常运行。协议安全主要靠校验协议完整性来实现。

## 协议校验

在智能家居的通信协议中，倒数第2个字节（结束符之前）作为校验位，用于校验本次指令的有效性。

校验字节的值应为校验位之前的所有字节的累计和（不计溢出和符号）。校验和的具体算法参见《云端与网关通信协议》。

云端、网关、App互相通讯时，应互相验证校验和字节有效性：

* 若校验和有效且通过验证，则进行下一步业务处理；
* 若校验和无效，则中断本次通信，向对方发送校验和错误的错误结果。

# 通信安全

通信安全是指加密云端与设备、云端与App之间的通信链路，避免智能家居通信数据被轻易监听和破解。其中，又分为长连接加密和短连接加密。长连接主要用于Kamailio与设备和App之间的通信，使用TLS加密通信数据；短连接主要是Web Server通过HTTP与设备和App之间的通信，使用HTTPS加密。

## TLS加密

Kamailio服务与设备和App之间的通信，使用TLS加密通信数据。TLS协议用于两个应用程序之间提供保密性和数据完整性。该协议由两层组成：TLS 记录协议（TLS Record）和 TLS 握手协议（TLS Handshake）。较低的层为 TLS 记录协议，位于某个可靠的传输协议（例如 TCP）上面。

TLS 记录协议提供的连接安全性具有两个基本特性：

* 私有――对称加密用以数据加密（DES 、RC4 等）。对称加密所产生的密钥对每个连接都是唯一的，且此密钥基于另一个协议（如握手协议）协商。记录协议也可以不加密使用。
* 可靠――信息传输包括使用密钥的MAC进行信息完整性检查。安全哈希功能（ SHA、MD5 等）用于 MAC 计算。记录协议在没有 MAC 的情况下也能操作，但一般只能用于这种模式，即有另一个协议正在使用记录协议传输协商安全参数。

TLS记录协议用于封装各种高层协议。作为这种封装协议之一的握手协议允许服务器与客户机在应用程序协议传输和接收其第一个数据字节前彼此之间相互认证，协商加密算法和加密密钥。 TLS 握手协议提供的连接安全具有三个基本属性：

* 可以使用非对称的，或公共密钥的密码术来认证对等方的身份。该认证是可选的，但至少需要一个结点方。
* 共享加密密钥的协商是安全的。对偷窃者来说协商加密是难以获得的。此外经过认证过的连接不能获得加密，即使是进入连接中间的攻击者也不能。
* 协商是可靠的。没有经过通信方成员的检测，任何攻击者都不能修改通信协商。

TLS的最大优势就在于：TLS是独立于应用协议。高层协议可以透明地分布在TLS协议上面。然而， TLS 标准并没有规定应用程序如何在TLS上增加安全性；它把如何启动 TLS 握手协议以及如何解释交换的认证证书的决定权留给协议的设计者和实施者来判断。

### Kamailio开启TLS加密

Kamailio从v3.0.0版开始，通过加载TLS模块的方式，实现了对TLS的支持。

*loadmodule "modules/tls/tls.so"*

*modparam("tls", "private\_key", "./andrei-test.pem")*

*modparam("tls", "certificate", "./andrei-test.pem")*

*modparam("tls", "ca\_list", "./calist.pem")*

*enable\_tls=yes*

*route{*

*# ....*

*}*

### 网关设备开启TLS加密

在调用Linphone Android SDK时，启用TLS加密配置。

### App开启TLS加密

Android App在调用Linphone Android SDK时，启用TLS加密配置。

iOS App在调用PJSip SDK时，启用TLS加密配置。

## HTTPS加密

HTTPS(Hyper Text Transfer Protocol over Secure Socket Layer) 是以安全为目标的HTTP通道，即HTTP下加入SSL层，HTTPS的安全基础是SSL，因此加密的详细内容就需要SSL。 它是一个URI Scheme（抽象标识符体系），用于安全的HTTP数据传输。HTTPS存在不同于HTTP的默认端口及一个加密/身份验证层（在HTTP与TCP之间）。最初研发由网景公司(Netscape)进行，并内置于其浏览器Netscape Navigator中，提供了身份验证与加密通讯方法。现在它被广泛用于万维网上安全敏感的通讯。

HTTPS在智能家居系统里主要用于加密RESTful API相关的数据通信，保障Web Server（Nginx）与Web Client（App、浏览器、网关）之间的通信安全，避免通过RESTful API通信的数据被破解和篡改后干扰智能家居系统的正航运行。

### Nginx启用HTTPS

Nginx可以通过修改配置文件中的“Server”段的配置启用HTTPS。

*server {*

*listen 443;*

*ssl on;*

*ssl\_certificate /usr/local/nginx/conf/server.crt;*

*ssl\_certificate\_key /usr/local/nginx/conf/server\_nopwd.key;*

*}*

# 附录

无