一、总体介绍

安全组件是一套保障移动平台应用完整性、应用执行环境可信性、数据机密性的专业完整的安全解决方案。

安全组件初衷是帮助应用开发者低成本接入安全解决方案，全方位保证开发者应用的安全性。

二、功能概要

安全组件核心功能为安全存储、安全加密、安全签名。安全存储可以保证应用隐私数据的机密性，不被恶意应用所窃取；安全加密可以保证应用加解密的安全性，不被恶意攻击者所破解；安全签名可以保证客户端与服务端的请求不被进行篡改和伪造，防止中间人攻击。

上述安全组件的核心功能都构建在我们自主研发的安全沙箱之上。在安全沙箱中，实现了反调试、反篡改、反内存窃取等核心功能，更好的保证应用运行环境的安全性。

安全组件自身也有超强的代码变形与混淆技术，攻击者很难进行静态的逆向与分析。

安全组件多维一体，立体式保证应用的安全性。

安全存储

加解密过程中使用的密钥随机生成，并且与设备绑定。破解者即使拿到了用户手机上的加密数据，在自己的手机上也无法完成解密操作。极大的保证了APP存储在本地的数据安全。

安全加密

通常来说，一个加密过程需要用到三部分内容，密钥、加密算法和加密前的数据。其中，加密算法通常就是一些通用的算法或变形，例如DES、AES。而加密前的数据黑客本身就很容易拿到。因此，在整个加密过程中，密钥的安全存储及使用就非常关键了。

安全组件提供的安全加密功能，其整个加解密过程都在安全沙箱中完成，对外不暴露任何密钥和加密算法。因此，整个加解密过程安全、稳定、可靠。

安全签名

安全签名基于HMAC_SHA1算法和指定密钥Key对数据进行加签，在传输数据时，可以利用加签的结果对传输数据进行数据校验。

客户端APP在与服务器端通信的时候，如果请求的参数没有经过本地加密处理，以及服务器端参数的签名校验，那么该请求就很容易被黑客伪造和篡改。例如，在网银转账的场景中，我想转钱给账户A，黑客通过中间人劫持等手段将该请求中的A账户偷偷的改成了B账户，这时，如果服务器端没有参数的签名校验，那么用户就会在毫无感知的情况下将钱转到了B的账户。

在上述案例中， 可以使用安全组件提供的安全签名功能将请求的每个参数都计算一个签名值，并将这个签名值附加在请求的最后面。服务器在收到该请求的时候，只要使用服务器端安全组件对每个参数重新计算签名值，并和请求中附带的签名值做对比即可判断该请求是否被恶意篡改和伪造。

白盒加密（企业版）

白盒加密和前面所述的安全加密在功能上类似，即都是把明文转化成密文，但是两者在实现方式上完全不同。

白盒加密技术在整个加密过程中不会出现密钥和算法的概念，而是通过大量的查表运算最终得到密文。客户端只能加密，服务器端通过对应的SDK进行解密。

白盒加密，技术新颖、运算迅速。在安全强度上更是远远高于普通的安全加密。

白盒签名（企业版）

使用白盒签名技术将请求服务器的参数计算一个签名值，在安全强度上远远高于普通的安全签名。

模拟器检测（企业版）

多维度的模拟器检测方案，准确率高达99%以上。有效打击在模拟器上产生的一切黑产行为。

三、产品特点

聚安全–安全组件为应用开发者提供了一款安全有保障、方便易接入、运行无影响，体积无增长的安全解决方案。

四、接入流程

Android接入步骤请参考Android接入步骤文档

iOS接入步骤请参考iOS接入步骤文档