

梆梆SDKs详细分析（2） - 安全键盘SDK揭秘

转载

maspchen 于 2016-02-18 10:52:10 发布 2557 收藏 2
分类专栏: [移动安全](#) [android 安全](#) 文章标签: [梆梆加固](#) [安全键盘](#)



[移动安全](#) 同时被 2 个专栏收录

3 篇文章 0 订阅
订阅专栏



[android 安全](#)

3 篇文章 0 订阅
订阅专栏

作者: bighacker

时间: 2016-02-15, 14:57:49

链接: <http://bbs.pediy.com/showthread.php?t=207793>

前言

前段时间银行盗号木马盛行，由于对其中一些技术的好奇，所以乘着放假分析了梆梆的界面劫持SDK。文章发在了看雪上，地址如下：<http://bbs.pediy.com/showthread.php?p=1414652#post1414652>。

分析完梆梆的界面劫持SDK之后，发现梆梆的技术实现比较简单，与其宣称的功效还是有一定的差距。而且还存在诸多的问题，例如，误报多、容易被绕过、仅支持5.0以下机型等。并且梆梆在SDK的介绍文档和集成文档中都没有写出这些问题。

春节期间，为了学习梆梆的一些所谓先进技术，并且也想看看它的实际功效和宣传之间的差距，所以我拿了个用户量最大的安全键盘SDK来分析。

梆梆安全键盘SDK介绍

以下内容摘自梆梆安全键盘SDK介绍文档。

移动App输入键盘的安全现状

移动App开发者们，通常会绞尽脑汁的对服务器数据存储安全、客户端与服务器间的数据通讯安全做很好的加密保护，但他们往往忽略了数据的第一入口保护--移动App键盘保护。很多开发者们仍习惯于让他们的App调用Android系统自带（或用户默认设置的）的输入法，而这将使用户输入的数据裸露在攻击者面前。

目前App的输入法键盘主要采用了三种方式：系统默认输入法，自绘固定键盘和自绘随机键盘。

当用户调用默认的手机输入法时，黑客安装的第三方输入法启动替换掉系统自带的输入法，我们称之为系统输入法被“劫持”。该输入法键盘可以直接记录用户输入的数字、字母、符号，并将这些敏感数据送回攻击者的服务器。

自绘固定键盘，可以避免使用被劫持的系统默认输入，降低敏感数据泄露的风险，但对于键盘记录的防御能力有限。黑客可以记录到键盘点击的位置坐标。

自绘随机键盘是安全性最高的输入方式，不仅避免了被第三方输入法劫持，并且键盘上每次点击位置都是随机的，无法恢复出用户输入的数据。

基于键盘输入窃取信息的各类移动安全攻击非常普遍。黑客们通过反编译一些流行的应用，将键盘钩子（监控程序）捆绑嵌入其中，二次打包后上传到各个应用市场上扩散传播。当用户安装并运行了这些受感染的应用时，嵌入的钩子程序就会被激活，悄悄驻留在后台中，以监控用户通过键盘输入的数据。一些流行的键盘输入攻击包括：



梆梆安全键盘SDK的特点



梆梆安全键盘SDK的优势



梆梆安全键盘样式



在上图中，我们可以看到，梆梆的安全键盘是一个自绘的，并且是数字随机的键盘。这种键盘可以有效防止键盘劫持、记录用户敲击位置等多种黑客攻击。

梆梆安全键盘SDK逆向分析大揭秘

前面的SDK介绍内容大部分都摘自梆梆的介绍文档。看完文档之后，给人的感觉就是梆梆这技术真牛逼。那么真相跟他描述的都一样吗？下面我们通过逆向分析来一一揭穿其真面目。

虚假宣传1 – 键盘按键是图片，且URL、MD5都不同

虚假宣传如下图：



梆梆宣称其按钮都是图片，并且每次都是从不同的URL拿到的，每次拿到的图片MD5也不同。因此，攻击者不可能通过图片来获取相应的内容。

真相如下图：



那么这些按钮实际是怎么回事呢？通过上面梆梆安全键盘SDK的布局文件我们可以知道，数字1，数字2，数字3等按钮其实都是系统自带的Button控件，跟URL、图片什么的没有半毛钱关系。

虚假宣传2 – 客户端记录点击顺序，服务端翻译

虚假宣传如下图：



梆梆的SDK宣传中说到，客户端记录了用户的图片标识及点击顺序，然后服务器端完成将这些标识翻译成实际字符、数字的过程。

那么实际的真相是怎么样的？



我们前面说过，客户端键盘的数字、字母等其实都是Android的Button控件。客户端在初始化阶段将Button控件设置成相应的字符。然后再点击事件中取出这个字符就可以了。没有客户端字母图片一说，所以就更没有服务器端翻译这个事情了。

虚假宣传3 – 安全键盘是一个HTML5安全控件

虚假宣传如下图：



梆梆宣称其安全键盘是一个HTML5安全控件，因此可以有效防御一些列黑客攻击。

真相是这样的：



查看demo的布局文件我们可以知道，安全键盘控件是一个名为com.bangle.safekeyboard.PasswordEditText的控件。通过逆向分析，我们可以知道PasswordEditText是继承自系统的EditText控件。因此，其实现原理简单，根本不存在HTML5安全控件一说。

虚假宣传4 – 可以防止内存dump攻击

虚假宣传如下图：



通过逆向分析，可以发现梆梆的安全键盘确实对输入的数据进行了加密存储。但是，我们依旧可以dump出来加密的数据。

虚假宣传5 – 密码在内存中加密存储，无懈可击

虚假宣传如下图：



通过进一步的逆向分析，我们可以知道梆梆安全键盘使用的加密方式是DES对称加密。并且通过逆向其so，还知道了加解密使用的key。



有了dump出来的加密数据，还知道了加密使用的key，我们完全可以使用Python来编写一个简单的解密脚本。当然，使用更投机取巧一点的方法，我们可以直接调用其so中导出的加解密函数。



总结

通过逆向分析梆梆的安全键盘SDK，发现其使用的都是比较传统、简单的技术，与其宣称的高大上黑科技还是有一定的差距。因此，还是那句老话，不看广告看疗效。

梆梆的安全键盘控件在一定程度上能加大攻击者的利用难度，但是理论上来说，密码最终还得解密出来，因此，攻击者无论如何还是有机会能拿到你的明文密码。

pdf附件：

[梆梆SDKs详细分析（2）-安全键盘SDK揭秘.zip](#) *转载请注明来自看雪论坛@PEdiy.com