### WeChat的音视频通话监控的总结文档

## 需求：

现在很多犯罪分子经常使用WeChat进行发布传播一些扰乱国家秩序的内容。为了维护社会稳定我们需要监听这些WeChat内容。WeChat软件厂商是为了保护用户的隐私，这些监控功能是一般不开放给相关部门的。 所以相关部门使用都是第三方监控软件。

## **实现目标：**

1. 部署在审计产品平台上 音视频播放文件生成器。

2. 一款音视频播放文件的播放器

## **主要内容：**

1. APP 的防护手段

2.网络数据包保护

3.播放器的设计

4.版本差异

## **App主要防护手段：**

1. 热修复更新代码逻辑

我们分析App时，一般直接对APK文件解压，然后文件里面的DEX文件，或者SO文件。但是对于支持热修复的APP， 我们分析可能是个假so或者dex。

2. 重要逻辑放在App子进程

这款IM软件一个重要逻辑代码放在子进程调试，调试子进程是一件特别比较麻烦。

## **数据包防护**

1. 数据包特征：

长连接, UDP数据包

首字节 : 0x76 / 0x75

2. 数据包 加解/密算法

旧版本： RC4

新版本： chacha20-poly1305

1. 数据包的密钥

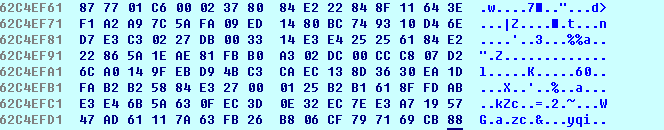
旧版本：密钥是roomkey , roomid, 使用TCP协议 明文传输

新版本：密钥是roomkey, decrptedKey, 使用mmtls协议传输密钥

## **播放器的设计**

1. 变异RTP数据包 ：

音视频数据包通过解密之后是一个变异的RTP数据包。很难实现从RTP数据包中提取出流媒体播放文件， 于是我们选择使用Wechat本身直接作为我们播放器。



2. 播放器的设计

实时播放: 网络数据包实时处理用于播放

本地播放： 网络数据包生成播放文件

3. 远程控制 播放

对于播放器的实现，我们是通过注入技术实现的，为了是实时控制播放器，我们在注入的so模块，增加Socket通信功能， 用于我们对播放器的控制，例如实现: 重放，回放，暂停， etc 等播放器应有的功能 。



## **消除版本差异**

1. 数据包的差异

由于播放文件需要里面存储着音视频通话数据包，和对应数据包的解密密钥。 不同版本的Wechat音视频 数据包格式是不一样的，密钥也不一样。 所以我们需要设计一个播放文件格式来消除这种差异性。

1. 播放器的差异

不同版本Wechat只能播放对象的数据包，所以我们需要设计一款播放器管理器来管理这些不同版本的播放器

## **问题 && 展望**

问题1：对于新版本6.5.8及6.5.8以上版本， 使用MMTLS 传输密钥。对于MMTLS协议破解是一件不易的事。

问题2：对于播放器目前功能还是比较简单，需要花费时间去开发， 希望有人帮忙支持一下。