根据五一假期和大家的沟通、讨论，我对课程的编排做了一些调整，希望接下来的课程能让大家大呼过瘾。

调整主要是下面两方面

- 启发式教学：从实践到理论而非从理论到实践

  主要针对问题：

  > 我是一个刚入门SO的新人，我知道密码学很重要，但我听不进去，因为我不知道什么场景下会用到它们。。。就好像小时候也都明白读书重要，但没被社会毒打过，体会不深，还是不知道读书的好。

  所以要让大家"挨社会的打"，先讲样本，从样本中引出问题，然后解决问题。即理论为实践服务，避免"光造轮子不跑车"或者大学的密码学课堂。

- 尽可能展示真实的分析流程

  主要体现在两点上

  - 使用一些真实样本而非纯粹自写DEMO

    ps.目的不是算法还原，只是针对授课内容做对应部分的、研究角度上的案例讲解。

  - 不念稿

    > 我之前报过别家的培训，感觉分析讲的不够细，好像拿着剧本一样，不知道它为什么从这儿跳到那儿，也不知道老师是怎么想的。

    确实如此，对于一个真实的样本而言，逆向几天甚至几周都是有可能的，一两小时的逆向分析过程，简直有点像"表演"，在这一点上，我也会做一些尝试，尽量细一些，慢一些，不说"显而易见"。

首先看一下样本mt，这个样本的对应部分我们会后续仔细分析。

我们已经提前写好了Frida主动调用的脚本

这一个环节，我们需要回答以下的问题

仅通过Frida 主动调用，我们可以粗略估计出哪些信息？

——加密算法类型（分组 or 序列）

——加密算法工作模式（是否是ECB）

——加密算法大致种类，是AES还是DES

为什么这么说，世上只有AES和DES两种加密算法吗？

我们要搞清楚两件事

1.不同加密算法有不同的用处

比如前段时间主讲的哈希算法，它用于签名校验，而非数据的加密。

适合用于数据加密的是对称加密算法和非对称加密算法，前者加解密密钥是一个，后者加解密采用两个密钥，公钥与私钥。

非对称加密算法安全性好，但运算太慢，所以一般采用对称加密算法加密数据，而RSA这些非对称加密算法用于生成和传输对称加密算法的密钥。这种方案叫混合加密体制，是一种成熟且安全的通信方案。

所以关于数据的加密，焦点就是对称加密算法。对称加密算法有非常多种类，但最为标准的就是美国的两个标准。

1是"美国数据加密标准"，即DES。DES用了几十年后，安全性不够好了。

于是遴选"美国高级加密标准"，胜出者就叫AES。Rijni就是胜出者。

所以遇到SO中的加密算法，第一反应就应该是AES。同时，花再多的时间去讲它都不为过。

DES和3DES 的使用已经比较少了。

AES就是现在的最主流加密标准。而且和哈希算法不太一样，哈希算法尽管用的频繁，但花样也比较少，既不用考虑密钥，也没有IV或者分组的考虑，魔改也一般就改个常数，而AES花样可就太多了。我们后续慢慢看有哪些花样。

需要注意的是，这些论断都不是绝对的，我们后续会再提起。

接下来看第一类样本，看一下我们最常规的，OPENSSL 怎么实现AES 加密、

——引入OPENSSL的相关知识

EVP实现（rong360）

底层实现（DEMO）

第二类样本——糟了，没有符号 tiny aes

- 怎么从代码中看是否是AES加密呢?
- 怎么从代码中看AES的工作模式呢?
- 怎么从代码中看AES的密钥呢?

逐步引入AES的原理

引入S盒

以及AES 的轮函数，以及xor，等等知识。

第三类样本

魔改S盒（DEMO）

强迫我们去了解算法原理咯

第四类样本

美团，扩展密钥算法

第五类样本

qdd

到这儿为止都属于AES基础以及SO基础内容，下面是进阶。

白盒AES 样本

?

这部分给大家准备了一些资料