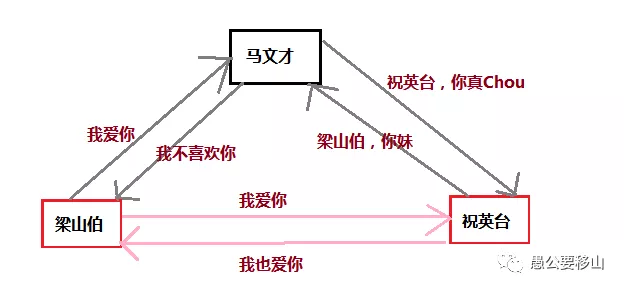
https://mp.weixin.qq.com/s/Ttp1q3edKHRb2E8iMsa4oA

# 什么是中间人攻击

梁山伯要向祝英台表白，于是写了一封信给祝英台，结果第三者马英才拦截到了这封信，把这封信进行了篡改，于是乎在他们之间进行搞破坏行动。这个马文才就是中间人，实施的就是中间人攻击。这篇文章就来好好聊聊什么是中间人攻击。

## 一、什么是中间人攻击

中间人攻击英文名叫Man-in-the-MiddleAttack，简称“MITM攻击”。指攻击者与通讯的两端分别创建独立的联系，并交换其所收到的数据，使通讯的两端认为他们正在通过一个私密的连接与对方直接对话，但事实上整个会话都被攻击者完全控制。我们画一张图：

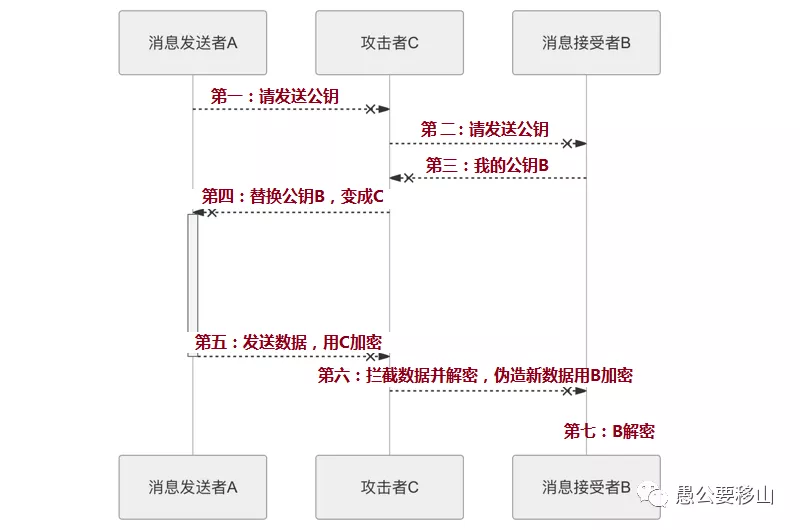


从这张图可以看到，中间人其实就是攻击者。通过这种原理，有很多实现的用途，比如说，你在手机上浏览不健康网站的时候，手机就会提示你，此网站可能含有病毒，是否继续访问还是做其他的操作等等。

下面我们说说中间人攻击的原理：

## 二、中间人攻击的原理

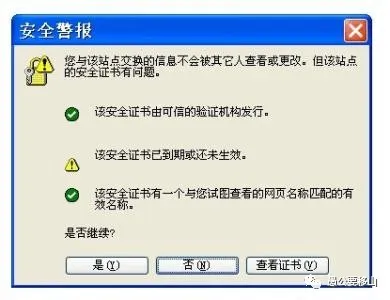
我们直接使用一张图来演示：本图来源于：flydean的《java哪些事专栏》，并对图片进行了更改和调整。特在此说明。



这是一个基本的完整的流程，具体步骤可以依据图片来看，这里就不在用文字再叙述一遍了。

## 三、中间人攻击如何避免？

既然知道了中间人攻击的原理也知道了他的危险，现在我们看看如何避免。相信我们都遇到过下面这种状况：



出现这个界面的很多情况下，都是遇到了中间人攻击的现象，需要对安全证书进行及时地监测。而且大名鼎鼎的github网站，也曾遭遇过中间人攻击：



不过github已经找到了这个攻击者：346608453，后面是QQ邮箱。

想要避免中间人攻击的方法目前主要有两个：

1、客户端不要轻易相信证书：因为这些证书极有可能是中间人。

2、App 可以提前预埋证书在本地：意思是我们本地提前有一些证书，这样其他证书就不能再起作用了。

OK，这个中间人攻击比较简单。先介绍这么多，面试问题足够。