中间人攻击 & 防御方式全解

关于网络安全有一个非常有意思的事，就是随着技术的变化，古老的网络攻击方式还会再次被利用。正如中间人攻击(MiTM)。这种攻击的目的很简单，就是在有线或者无线连接的中间放置一个攻击者。但是，随着云计算、物联网(IoT)、BYOT 等网络技术的发展，攻击者也开始寻找新的方式以使那些古老的攻击方式可以重新被利用。下面是每个专业的网络人员都应该知道的关于 MiTM 攻击的各种方式。

MiT-cloud (MiTC)

过去这几年，云计算越来越受欢迎，一个常见的云服务就是云存储，很多企业都在使用。这些云服务使得庞大的数据传输和存储工作变得很简单。这个领域的参与者有 Dropbox、OneDrive 以及 Google Drive 等等。通常情况下，这些服务不会要求你每次使用服务的时候都要重新登录，因为你验证后，它会在你的本地系统上保留会话令牌(token)。MiTC 就是利用的会话管理。如果攻击者获取了你的 token，他们就能访问你的账户，这样，他们就能窃取你的数据，更改文件信息，或是上传恶意软件使你的电脑感染病毒。

MiT-browser (MiTB)

你上一次写支票是什么时候?我是想说，如今大多数人都使用网上银行。MiTB 攻击就发生在这个时候，攻击者会诱导你下载木马(Trojan)。一旦你访问特定的财务或银行网站的时候，恶意软件就会往你访问的页面注入新的 HTML 代码，然后诱导你输入 SSN 号、ATM PIN 码或是银行路由代码。MiTB 会把它自己直接集成到网页上，还能保持原有的域名和 SSL 设置，看起来和真正的网页一样。

MiT-mobile (MiTMO)

攻击者不光针对台式机和笔记本。很多用户可能更多的是在他们的智能手机上进行转账付款等操作，这就给攻击者创造了更多的机会。这也是为什么 MiTMO 越来越受到关注的原因。这种攻击关注移动交易验证码(mTANs)以及其它各种类型的交易验证码。这种类型的中间人攻击会拦截 SMS 流量，并且捕捉这些代码，然后把它们转发给攻击者。MiTMO 给带外身份验证系统带来了很大的挑战。

MiT-app (MiTA)

不知道你是不是和我一样，还记得有智能手机以前的生活，那时你可能会有很多灵感，如今这些想法都已经被智能手机替代了。随着智能手机的发展，应用程序也迅速激增，如果应用程序没有执行有效的证书验证，那就给了 MiTA 攻击的机会。MiTA 会让攻击者插入一个自签名的证书，来和应用程序通信。它的工作原理是利用应用程序处理信任的方式，扩展 MiTM 攻击模式。

MiT-IoT

随着越来越多的用户和企业都开始采用 IoT(物联网)，MiTM 攻击也越来越受到关注。其中有一种类型的攻击就是 MiT-IoT，这种攻击方式是利用传递信任和较差的证书验证。举个例子来说，一种能够显示用户的 Google 日历的 IoT 冰箱就发现没有验证 SSL 证书。这会导致攻击者利用这种漏洞安装一个 MiTM 攻击，窃取用户的 Google 证书。

上面说的每种攻击都是对网络安全专业人士的挑战，但是，有一些方法可以减少这些攻击发生。具体方法如下：

- 通过采用动态 ARP 检测、DHCP Snooping 等控制操作来加强网络基础设施

• 采用传输加密：SSL 和 TLS 可以阻止攻击者使用和分析网络流量。像 Google 等公司如今都有高级的网站搜索引擎优化，默认状态下都提供 HTTPS。

• 使用 CASBs(云访问安全代理)：CASBs 可以提供加密、访问控制、异常保护以及数据丢失保护等一系列功能。

• 创建 RASP(实时应用程序自我保护)：这是一个新概念，内置于应用程序中，用来防止实时攻击。

• 阻止自签名证书：自签名证书很容易伪造。但是目前还没有撤销它们的机制。所以，应该使用有效证书颁发机构提供的证书。

• 强制使用 SSL pinning：这是对抗 MiTM 攻击的另一种方式。使用有效证书颁发机构提供的证书是第一步，它是通过返回的受信任的根证书以及是否与主机名匹配来验证该服务器提供的证书的有效性。通过 SSL pinning 可以验证客户端检查服务器证书的有效性。

• 安装 DAM(数据库活动监控)：DAM 可以监控数据库活动，检测篡改数据。

MiTM 攻击是一个很大的挑战，它是利用用户和用户连接的服务器之间的信任。这种攻击的危险之处在于，用户想当然的认为他们的连接很安全。只有我们开始意识到这种攻击的危险真正存在，并且花很多时间去进行适当的控制时，比如加密、适当的验证、强大的应用程序验证以及通过系统来检测篡改等，才可以防御 MiTM 攻击。