4G LTE数据链路层漏洞分析_Breaking LTE on Layer Two

angel010 / 2018-07-02 10:05:59 / 浏览数 5823 安全技术 漏洞分析 顶(1) 踩(0)

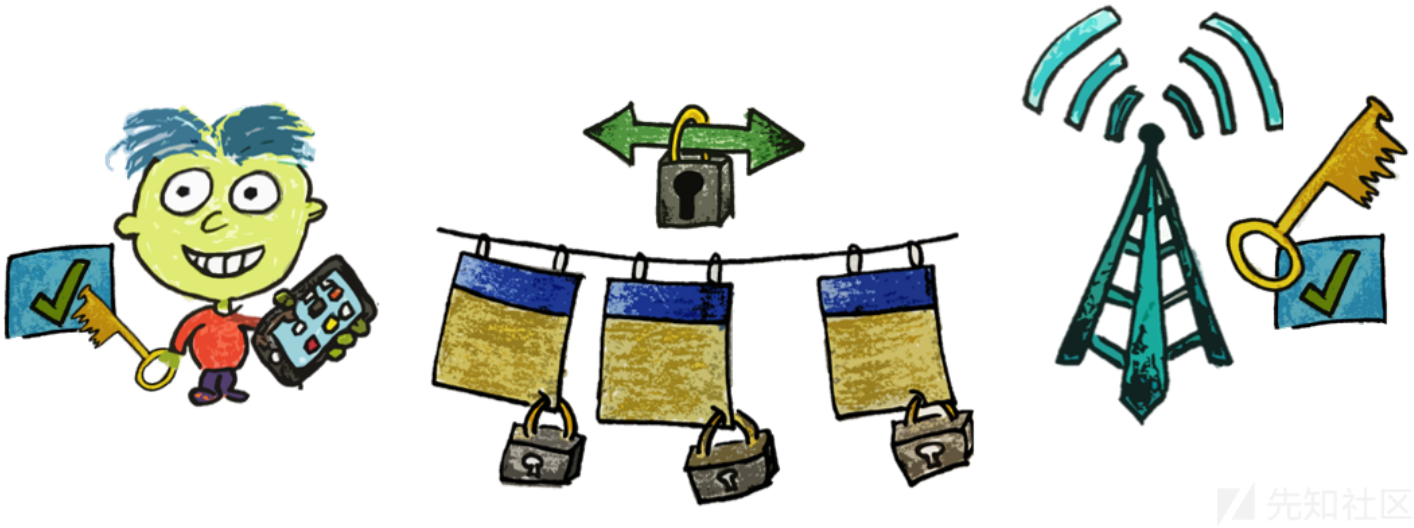
简介

近日，德国Ruhr-University Bochum和New York University Abu Dhabi的研究人员公布了被IEEE S&P 2019录用的一篇文章“Breaking LTE on Layer Two”，研究人员通过分析4G
LTE协议栈发现了数据链路层存在的漏洞，并描述了2种主动攻击和1种被动攻击方式。其中被动攻击分别是身份映射攻击和执行网站指纹识别,主动攻击是aLTEr。

TABLE I
OVERVIEW OF LAYER TWO ATTACKS

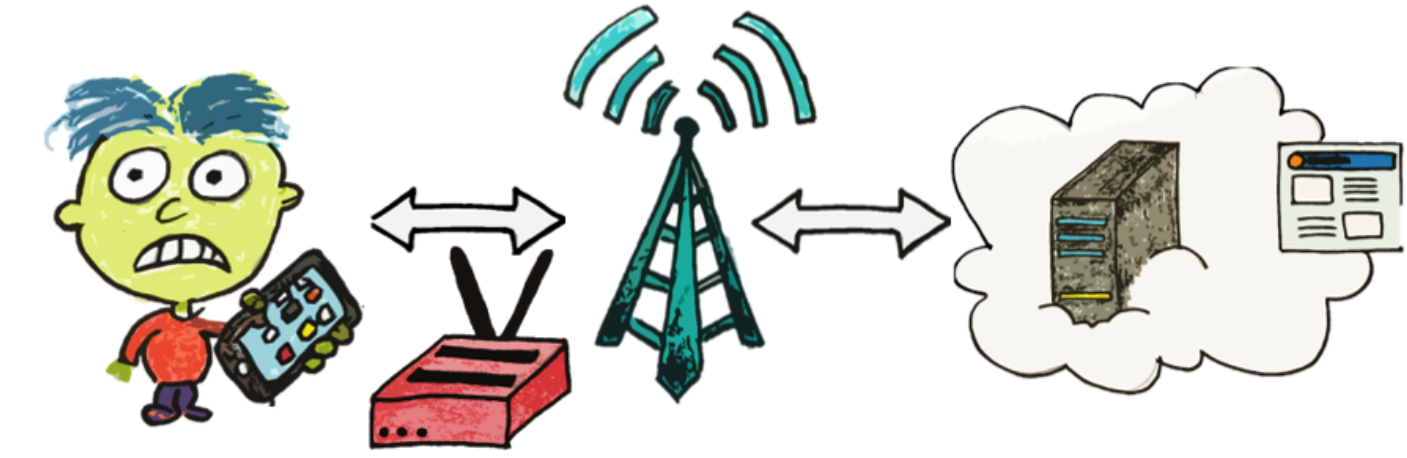
	Model	Attack Vector	Attack Aim	Attack Flaw	Hardware	Implementation
Identity Mapping	Passive	RNTI and TMSI Mapping	Privacy (Identity, Location)	Specification	USRP	Software Stack
Website Fingerprinting	Passive	Layer Two Scheduling Metadata	Confidentiality	Specification	USRP	Software Stack
aLTEr	Active	Lack of Integrity Protection	Confidentiality, Redirection	Specification	2x USRPs	Software Stack

LTE的安全机制



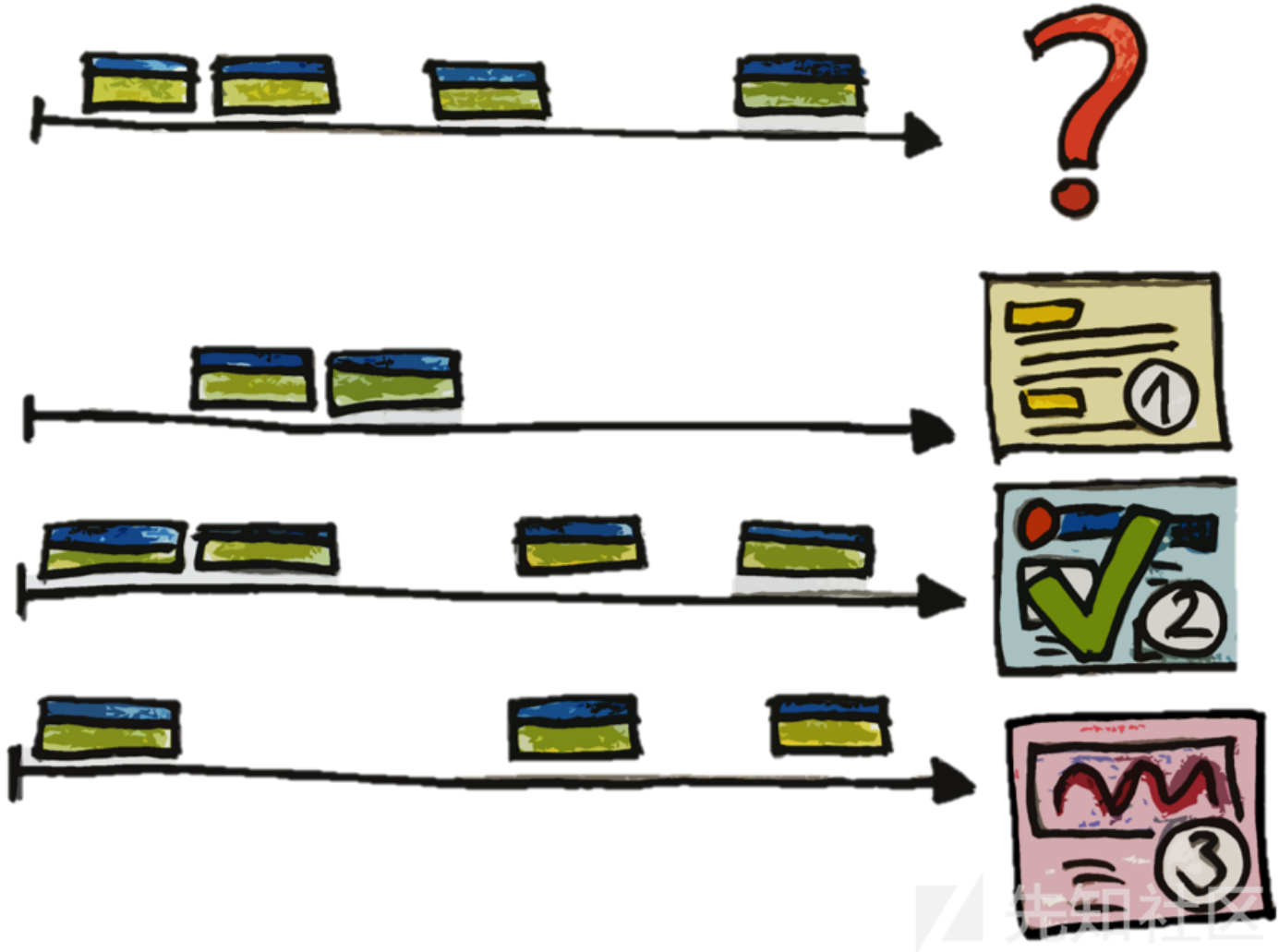
LTE有许多的安全机制。当Bob的手机连接到网络时，会建立多重认证和共享密钥。多重认证意味着手机和网络可以分别互相识别对方。密钥用来加密控制流和用户流。控制

被动攻击



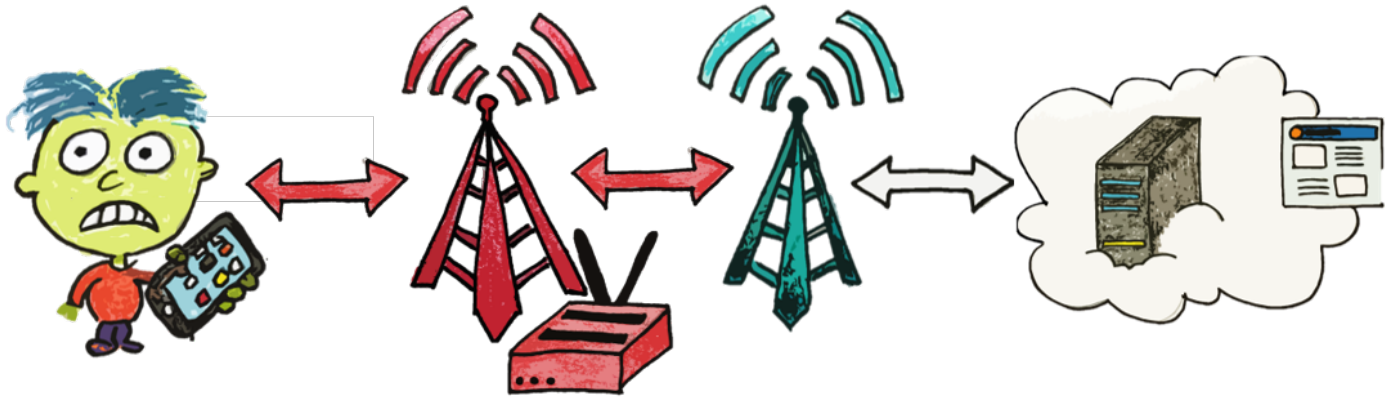
在被动攻击中不会干扰网络的正常连接，只能通过窃听的手段获取流量中的数据。窃听者 Eve 通过在 Bob
附近部署一个嗅探设备来实现这一点。因此，她可以访问 Bob
发送给网络以及从网络接收到的所有信息。尽管数据链路层的数据都是经过加密保护的，攻击者仍然可以获得在通信过程中的元数据（例如：数据传输的时间和频率）。

网站指纹



数据链路层的元信息可以泄露关于单位时间数据消耗的信息。例如，当 Bob 观看视频时的流量肯定比他访问简单的网站大。作为攻击的前奏，Eve
可以记录访问一些常见网站时的数据链路层的元信息特征（也就是网站指纹），在她窃听到一些元信息之后，根据网站指纹去匹配，有比较大的概率可以知道目标访问了哪

aLTEr攻击



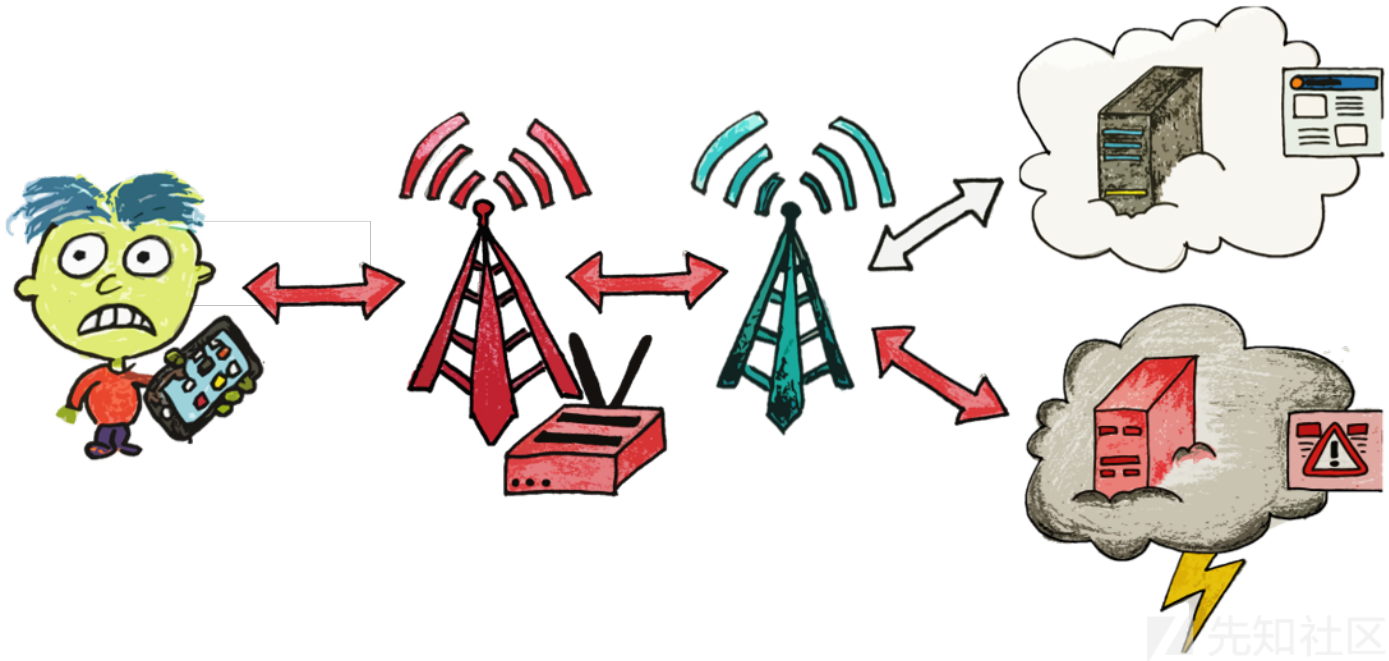
因为主动攻击具有入侵的能力，可以通过DNS欺骗将用户重定向到恶意站点，所以研究人员将主动攻击命名为aLTEr。
在主动攻击中，攻击者通过模拟合法的网络或用户设备向网络或设备发送信号。在我们的实验中，攻击者可以同时拦截并重放Bob 和网络之间传输的所有数据。在

Bob 眼中，所有的访问都是正常的，不会有任何明显的异常。

用户数据重定向

LTE 是在数据链路层以上的层使用相互认证来防止 Bob
的手机连接到假的网络。但是，攻击者可以转发高层的消息到不受保护的低层。用户数据重定向攻击的核心就是利用用户数据不受完整性保护。因此，如果攻击者知道原始的
DNS 数据包，我们知道原始 DNS 服务器的地址，攻击者可以通过添加特定的偏移量，将 DNS 重定向到攻击者可控制的 DNS 服务器。

DNS 欺骗



恶意的 DNS 服务器执行 DNS 欺骗，将正常的域名解析到恶意的 IP 地址。手机在访问一个网站的时候，实际访问的就是攻击者指定的恶意网站。DNS
欺骗是互联网上常见的攻击，在攻击者控制 DNS 服务器的下一跳即可发动攻击。跟用户数据重定向攻击相比，攻击者只需要靠近受害者即可执行此类攻击。

实验结果

为了演示 aLTEr 攻击的可行性，研究人员在实验室环境中的商用网络和商用电话内实施了全面的端到端攻击。通过软件无线电系统实现了基于开源 LTE 软件栈
srsLTE 的 LTE 中继。使用屏蔽盒来稳定无线电层并防止被真实网络的意外打断。另外，设置了两台服务器来模拟攻击者如何重定向网络连接：一台 DNS
服务器，对特定的 DNS 查询回复恶意的 IP 地址；一台 HTTP 服务器，模拟用户登录页面，IP 就是 DNS 回复的恶意 IP ，视频演示如下：
https://www.youtube.com/watch?v=H85lsA9Y0Yg

影响

实施这三针攻击需要特殊和昂贵的设备、定制的软件。为实施这样的攻击，攻击者需要使用专门的硬件（软件定义无线电）和定制的LTE协议栈。还需要一个受控的环境来确

影响5G标准？

研究人员已将漏洞相关情况通报给了GSM Association (GSMA)，3rd Generation Partnership Project
(3GPP)和相关公司，并称漏洞会影响5G标准。也有专家称5G标准中含有额外的安全特征（数据层的强加密）来防止aLTEr攻击的产生，但这些安全特征不是必选项。

更多关于攻击的情况可以参考https://alter-attack.net/
论文：Breaking LTE on Layer Two https://alter-attack.net/media/breaking_lte_on_layer_two.pdf

点击收藏 | 0 关注 | 1

上一篇：SSRF攻击文档翻译 下一篇：如何利用SettingConten...

1. 0 条回复
   - 动动手指，沙发就是你的了！