电力智能终端数据采集无线通信安全

徐瑶

国网陕西西咸新区供电公司　陕西　西咸新区　712000

[摘　要]信息技术的进步，衍生了电力的智能终端、智能电表，实现了信息化的远程自动读表，节省了挨家挨户登门抄表的人力和时间成本。文章针对远程自动抄表智能终端将数据传输到电力信息采集系统的无线传输过程中的信息安全问题，开展数据在无线传输的过程中，有没有可能使用中间人攻击的方式，取得篡改数据的成果，从而威胁智能电表的通信安全的研究。

[关键词]电力数据采集系统；通信安全；中间人

【DOI】10.12252/j.issn.2096-627X.2021.10.322

1 GSM MITM中间人嗅探劫持攻击

1.1 中间人（Man-in-the-middleattack，MITM）攻击

一般在正常的客户端和服务端通信之间，利用各种手段进入一个具有双重身份的攻击者，这个攻击者的身份就是中间人。对于客户端，攻击者伪装成为正常的服务器；对于服务器，攻击者伪装成正常的客户端，将正常的客户端和服务器通信的流量劫持，然后转发，客户端和服务器整个过程的通信数据都经过中间人，所以中间人可以查看并修改客户端和服务器的通信流量。GPRS中间人嗅探劫持攻击只是中间人攻击的一个应用场景，中间人在各个通信领域都有应用。中间人在攻击期间获得的信息，可用于多种目的，例如身份信息盗取、敏感信息获取、信息资料篡改等。

1.2 伪基站

其利用通信网络的一些技术漏洞，劫持正常用户的手机通讯，骗取用户信息，强行发送广告、诈骗等信息，嗅探和劫持正常用户的通信流量，以此达到非法目的

1.3 GSM伪基站原理

由于全球移动通信系统（Global System for Mobile Communications，GSM）通信网络设计的缺陷，GSM网络是单向验证，即基站验证手机；手机不验证基站，而且盲目相信基站广播的信息。手机（MS）在开机时会优先驻留（Camping）SIM卡允许的运营商网络里的信号最强的基站，因此伪基站信号强是有意义的，但是用户并不会经常开关机，所以即使信号不是最强也影响不大。比开关机更经常发生的是位置更新（Location Update），伪基站主要靠Location Update流程来吸引MS驻留。伪基站工作时通常伪装成相邻基站列表里的在当前位置信号最弱的基站以减少同频干扰，但是LAC（Location Area Code）会设置成跟正常网络不冲突的数字范围，还会改变Cell Reselection参数。MS在Location Update时，伪基站会发出身份认证请求（Identity Request）给MS，要求MS提交IMSI，国际移动用户识别码捕获器（Stingray / IMSI Catcher）还会再次发出Identity Request，要求MS提交IMEI。为了少惊动目标，目的达到后，伪基站记录该IMSI，然后尽可能快地把该MS弹回（Reject）原网络。这会在MS再次提交Location Updating Request时完成。为了能尽快地让MS再次提交Location Updating Request，伪基站有两个办法，一是频繁改变LAC，二是广播更短的位置更新周期，比如把T3212设为1分钟。

1.4 GSM MITM攻击原理

GSM MITM攻击原理即在运营商基站和目标手机之间插入一台伪基站和一部攻击手机，诱导目标手机附着到伪基站，然后攻击手机以目标手机身份在运营商网络注册，使得目标手机的所有进出通信都经过伪基站和攻击手机中转，以此能够拦截、修改、仿冒各种通信内容。

1.5 GSMMITM攻击流程

（1）取得目标的手机号码（MSISDN）；（2）通过HLR Lookup查得目标的IMSI；（3）通过Paging/HLR Lookup/社工确定目标所在的蜂窝小区（Cell ID）；（4）肉身到目标附近，50m～300m；（5）打开伪基站，吸引周围手机前来附着，Reject除目标IMSI外的所有手机；（6）目标手机附着后，启动攻击手机进行身份劫持；（7）拦截目标手机的短信和流量。

2 GPRS通信中间人攻击试验

通用分组无线服务技术（General Packet Radio Service，GPRS）是GSM移动电话用户可用的一种移动数据业务，属于第二代移动通信中的数据传输技术，服务由国内的运营商提供。如果攻击者想要进行GPRS中间人攻击，就必须劫持手机终端与运营商基站之间的通信流量，再将流量进行转发。如何才能在手机终端和运营商基站之间，伪装成一个具有双重身份的中间人劫持手机终端和运营商基站之间的通信流量。攻击者会采用技术手段，自己搭建一套和运营商无线通信网络一样的通信网络，俗称伪基站。

2.1篡改通信协议数据

一旦设备成功接入搭建的中间人测试平台，就可以对经过的流量进行任意操作，例如修改数据内容和代理转发。实验以篡改终端发送到服务端的电能数据包为例：首先，找到要攻击的目标数据包，为此应对截获的协议报文进行解析和筛选，依据就是协议数据帧格式的控制码和数据标识；然后，替换掉帧格式里的数据部分，需要注意的是，修改数据后，数据帧后面的校验码也要做相应的修改，否则服务端收到不正确的校验码会直接丢弃掉数据帧。这里可以对接收的数据包进行加工处理，最后转发到服务端，篡改电表电能数据包示意图。

2.2流量嗅探与分析

实施中间人攻击后，数据流经过中间人的篡改，再转发到数据的采集终端。终端发送的有功总电能数据项的值会发生改变，这意味着电表发往服务端的有功总电能遭受篡改。

3 结束语

本文针对电网终端数据在采集传输中的安全性问题，研究能否将智能终端采集的电力数据安全、完整、稳定地传回数据采集系统，在数据的传输过程中能否抵御监听、篡改、破坏等网络攻击行为，并证明远程自动抄表智能终端将数据传输到电力信息采集系统的无线传输过程中存在信息安全风险。

参考文献

[1]吴金宇，陈海倩，张丽娟等.基于可信计算的主动配电网信息安全防护研究[J].广东电力，2020，33（3）：79-87.

[2]卢兵，岳慧清.基于国密算法的LTE230系统终端安全的研究[J].供用电，2018，35（12）：14-20.