不安全的无线协议

发表于 2021-01-25 更新于 2021-02-16 分类于 Challenge ， 2020 ， 工业信息安全技能大赛 ， 湖州站
Challenge | 2020 | 工业信息安全技能大赛 | 湖州站 | 不安全的无线协议

点击此处获得更好的阅读体验

WriteUp来源

来自MO1N战队

题目描述

> *某工控环境中使用了不安全的无线协议，安全人员捕获到相关无线信号，请分析名为POC的附件。flag格式为:flag{}。*

题目考点

- *流量分析*
- *Pocsag协议*

解题思路

Pocsag协议正相地址码为1234567

对pocsag编码进行解密，对照信息码字结构

使用urh对无线信号进行解析

可以看到前置码、sc、0为576+32+64位而1由位编号、地址码字、信息码字、在这里只需要将信息码字解析即可。

同步码字的16进制表示为(7CD215D8),

空闲码字的16进制表示为(7A89C197)。

在地址码字中

- *第1位为0*
- *第2~19位为地址*
- *20和21位为状态*
- *22~31位为BCH校验*
- *第32位为奇偶校验*

在信息码字中

- *第1位为1*
- *第2~21位为信息*
- *22~31位为BCH校验*
- *第32位为奇偶校验*

```
1 00110110 00110110 00110110 01100011 00110110 00110001
2 00110110 00110111 00110111 01100010 00110100 00110010
3 00110110 00110001 00110110 00110100 00110110 01100100
4 00110011 00110000 00110011 00110000 00110110 00110100
5 00110111  01100100
```

*共208=26*8位*

而每一个信息码字里面可以传输20位，则需要3个信息码字方能将数据传输完整:

位	***0***	***1-20***	***21-30***	***31***	
码字1	*1*	*0011 0110 0011 0110 0011*	*BCH(31,21)值*	*奇偶校验位*	
码字2	*1*	*0110 0110 0011 0011 0110*	*BCH(31,21)值*	*奇偶校验位*	
码字3	*1*	*0011 0001 0011 0110 0011*	*BCH(31,21)值*	*奇偶校验位*	

在数据传输过程中，如果没有发生错误的话，我们应该接收到的内容应该是：

```
1010  1001  1010  0000  1010  0100  1111  1001 数据 (1)
```

*将接收到的数据(1)与矩阵H进行乘法运算可以得到新矩阵R，称R为伴随式。R = D * H*

其中 D为数据(1)前31位的1行31列矩阵——奇偶校验位不参加运算， H为BCH(31,21)一致校验矩阵的转置矩阵

矩阵的转置矩阵等于原矩阵的行列元素相互交换，如果交换前矩阵元素为MN，则转置后矩阵为NM，示例如下:

*BCH(31,21)一致校验矩阵为10行31列，则它的转置矩阵H为31行10列，D为1行31列。R＝D*H，则R为1行10列的矩阵。*

矩阵乘法示例：

得到R后，我们就可以根据R矩阵来判断具体是哪一位或者哪二位出现的错误，错误的可能只是由1错为0或者相反，发现错误位后直接反转即可纠错。

由前面内容可以知道数据(1)是没有发生错误的，其伴随式R中的所有元素均为0，现将数据(1)第2位反转得到数据(2):

1110 1001 1010 0000 1010 0100 1111 1001 数据 (2)

*R2 ＝ D2 *H，对数据(2)进行译码的结果为：0 1 1 1 0 1 1 0 1 0。可见结果与图3中的第二列一模一样，则可以数据(2)的第二位发生了错误，将其反转纠错。*

发送的数据为:

```
1 00110110001101100011011001100110001100100110110001101110011011100010001101000011001000110110001100010011011000110100001101100110010000110011001100000011001100
```

16进制转换成字符串得到:`666c61677b4261646d3030647d`，再进行16进制转换字符串得到flag

Flag

```
1 flag{Badm00d}
```

- ***本文作者：*** *CTFHub*
- ***本文链接：*** *https://writeup.ctfhub.com/Challenge/2020/工业信息安全技能大赛/湖州站/54RmMzD484DSuKPck6NHs7.html*
- ***版权声明：*** *本博客所有文章除特别声明外，均采用 BY-NC-SA 许可协议。转载请注明出处！*

 # Challenge # 2020 # 工业信息安全技能大赛 # 湖州站
Modbus协议分析
PLC恶意操作