IoT

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， 济南站
Challenge | 2020 | 工业信息安全技能大赛 | 济南站 | IoT

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

> *一台奇怪的单片机上运行着奇怪的程序，请您帮助调试相关程序。Flag格式为：flag{}*

题目考点

- *RISC-V逆向*

解题思路

RISC-V是一个基于精简指令集（RISC）原则的开源指令集架构（ISA）。

与大多数指令集相比，RISC-V指令集可以自由地用于任何目的，允许任何人设计、制造和销售RISC-V芯片和软件。虽然这不是第一个开源指令集，但它具有重要意义，因为其设计使其适用于现代计算设备（如仓库规模云计算机、高端移动电话和微小嵌入式系统）。设计者考虑到了这些用途中的性能与功率效率。该指令集还具有众多支持的软件，这解决了新指令集通常的弱点。

IDA和ghidra无法直接加载，需要用新的LOADER

https://github.com/bingseclab/ida_riscv

因为RISC-V的汇编并不好分析，选择qemu使用动态调试的方法，注意要使用gdb 8.0+才可以

通过动态调试分析后会发现实际是两个数组进行xor，解密即可

```
cyt = [
    249, 149, 286, 132,  67,
    286, 328, 390, 356, 264,
    345, 222, 191, 120, 483,
    200, 340, 507, 158, 260
]

xor = [
    159, 249, 383, 227,  56,
    326, 295, 468, 315, 321,
    364, 129, 236,  72, 444,
    141, 309, 392, 231, 377
]

flag = ''
for i in range(len(xor)):
    flag += chr(xor[i]^cyt[i])
print(flag)
```

Flag

```
flag{XoR_I5_S0_Easy}
```

- ***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/济南站/tRBwdk3Fhmdm4UVjpAYQHy.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 #济南站
异常的S7数据
被篡改的数据