Frontiers of Information Technology & Electronic Engineering
www.jzus.zju.edu.cn; engineering.cae.cn; www.springerlink.com
ISSN 2095-9184 (print); ISSN 2095-9230 (online)
E-mail: jzus@zju.edu.cn

Supplementary materials for

Rongkuan MA, Hao ZHENG, Jingyi WANG, et al., 2022. Automatic protocol reverse engineering for industrial control systems with dynamic taint analysis. *Front Inform Technol Electron Eng*, 23(3):351-360.
https://doi.org/10.1631/FITEE.2000709

```
1  Function 1    enter     eMBPoll   (401d83,401f88,400f55)
2  Function 1    enter     xMBPortEventGet     (40133d,40137b,401dc1)
3  Function 1    enter     xMBPortTCPPool (401588,4018d3,401376)
4  Function 1    enter     select@plt      (400b90,400b9b,4015e8)
5  Function 1    enter     recv@plt  (400a90,400a9b,401784)
6  Taint     (0x604480, 7)
7  ...
8  Instruction 0x401809: mov word ptr [rbp-0xb2], ax 1    4    0x604484  0x0
9  Instruction 0x401810: movzx eax, byte ptr [rip+0x202c6e]    1    5    0
       x604485  0x6
10 Instruction 0x401817: movzx eax, al     1    5    0x604485  0x6
11 Instruction 0x40181a: or word ptr [rbp-0xb2], ax  1    4;5  0x0;0x6
12 Instruction 0x40181a: or word ptr [rbp-0xb2], ax  1    4,5  0x0
13 Instruction 0x40182b: movzx edx, word ptr [rbp-0xb2]   1    4,5  0x604484
       0x6
14 ...
15 Function 1    enter     select@plt      (400b90,400b9b,4016e3)
16 Instruction 0x401755: movzx eax, word ptr [rip+0x202e2e]    1    4,5  0
       x604484  0x5
17 Instruction 0x40175c: movzx edx, ax     1    4,5  0x604484  0x5
18 Function 1    enter     recv@plt  (400a90,400a9b,401784)
19 Taint     (0x604487, 5)
20 Instruction 0x4017d5: movzx eax, word ptr [rip+0x202dae]    1    4,5  0
       x604484  0x5
21 Instruction 0x4017e2: sub eax, edx 1    4,5  0x5;0x5
22 Instruction 0x4017e4: mov word ptr [rip+0x202d9f], ax  1    4,5  0x604484
       0x0
23 Instruction 0x4017fc: movzx eax, byte ptr [rip+0x202c81]    1    4    0
       x604484  0x0
24 ...
25 Instruction 0x40181a: or word ptr [rbp-0xb2], ax  1    4;5  0x0;0x6
26 Instruction 0x40181a: or word ptr [rbp-0xb2], ax  1    4,5  0x0
27 ...
28 Function 1    exit      xMBPortTCPPool
29 Function 1    exit      xMBPortEventGet
30 Function 1    exit      eMBPoll
31 Function 1    enter     eMBPoll   (401d83,401f88,400f55)
32 Function 1    enter     eMBTCPReceive  (401fcc,402087,401dff)
33 Instruction 0x402015: movzx eax, byte ptr [rax]    1    2    0x604482  0x0
34 Instruction 0x402018: movzx eax, al     1    2    0x604482  0x0
35 Instruction 0x40201b: shl eax, 0x8 1    2    0x0
36 Instruction 0x40201e: mov word ptr [rbp-0x16], ax 1    2    0x604482  0x0
37 Instruction 0x40202a: movzx eax, byte ptr [rax]    1    3    0x604483  0x0
38 Instruction 0x40202d: movzx eax, al     1    3    0x604483  0x0
39 Instruction 0x402030: or word ptr [rbp-0x16], ax  1    2;3  0x0;0x0
40 Instruction 0x402030: or word ptr [rbp-0x16], ax  1    2,3  0x0
41 Instruction 0x402034: cmp word ptr [rbp-0x16], 0x0     1    2,3  0x0
```

```
42 Function 1 exit eMBTCPReceive
43 Function 1 exit eMBPoll
44 Function 1 enter eMBPoll (401d83,401f88,400f55)
45 Instruction 0x401e43: movzx eax, byte ptr [rax] 1 7 0x604487 0x4
46 ...
47 Function 1 enter eMBFuncReadInputRegister (402975,402abc,401eb5)
48 ...
49 Instruction 0x4029ae: mov word ptr [rbp-0x14], ax 1 8 0x604488 0x0
50 Instruction 0x4029ba: movzx eax, byte ptr [rax] 1 9 0x604489 0x0
51 Instruction 0x4029bd: movzx eax, al 1 9 0x604489 0x0
52 Instruction 0x4029c0: or word ptr [rbp-0x14], ax 1 8;9 0x0;0x0
53 Instruction 0x4029c0: or word ptr [rbp-0x14], ax 1 8,9 0x0
54 ...
55 Instruction 0x4029e0: mov word ptr [rbp-0x12], ax 1 10 0x60448a 0x0
56 Instruction 0x4029ec: movzx eax, byte ptr [rax] 1 11 0x60448b 0x1
57 Instruction 0x4029ef: movzx eax, al 1 11 0x60448b 0x1
58 Instruction 0x4029f2: or word ptr [rbp-0x12], ax 1 10;11 0x0;0x1
59 Instruction 0x4029f2: or word ptr [rbp-0x12], ax 1 10,11 0x0
60 ...
61 Instruction 0x402a4f: mov byte ptr [rax], dl 1 11 0x60448b 0x2
62 Instruction 0x402a62: movzx edx, word ptr [rbp-0x12] 1 10,11 0
    x60448a 0x1
63 Instruction 0x402a66: movzx ecx, word ptr [rbp-0x14] 1 8,9 0x604488
    0x1
64 Instruction 0x402a6e: mov esi, ecx 1 8,9 0x604488 0x1
65 Function 1 enter eMBRegInputCB (400fd1,401071,402a78)
66 ...
67 Instruction 0x400fec: movzx edx, word ptr [rbp-0x1c] 1 8,9 0x604488
    0x1
68 Instruction 0x400ff0: movzx eax, word ptr [rbp-0x20] 1 10,11 0
    x60448a 0x1
69 Instruction 0x400ff4: add eax, edx 1 10,11;8,9 0x1;0x1
70 Instruction 0x400ff6: cmp eax, 0x4 1 10,11 0x2
71 Instruction 0x400ffb: movzx edx, word ptr [rbp-0x1c] 1 8,9 0x604488
    0x1
72 ...
73 Function 1 exit eMBRegInputCB
74 Instruction 0x402a97: movzx edx, word ptr [rbp-0x12] 1 10,11 0
    x60448a 0x1
75 Instruction 0x402a9b: add edx, edx 1 10,11;10,11 0x1;0x1
76 ...
77 Function 1 exit eMBFuncReadInputRegister
78 Instruction 0x401f43: movzx edx, word ptr [rip+0x202686] 1 10,11
    0x60448a 0x4
79 Function 1 enter eMBTCPSend (402088,402103,401f62)
80 ...
81 Instruction 0x4020cc: sar edx, 0x8 1 10 0x5
82 Instruction 0x4020cf: mov byte ptr [rax], dl 1 10 0x60448a 0x0
83 Instruction 0x4020d9: movzx edx, word ptr [rbp-0x18] 1 10,11 0
    x60448a 0x4
84 Instruction 0x4020dd: add edx, 0x1 1 10,11 0x4
85 Instruction 0x4020e0: mov byte ptr [rax], dl 1 11 0x60448b 0x5
86 Instruction 0x4020e2: movzx edx, word ptr [rbp-0xe] 1 10,11 0
    x60448a 0xb
87 Instruction 0x4020ea: mov esi, edx 1 10,11 0x60448a 0xb
88 Function 1 enter xMBTCPPortSendResponse (401912,4019c4,4020f4)
89 Instruction 0x40191e: mov eax, esi 1 10,11 0x60448a 0xb
90 ...
91 Function 1 enter send@plt (400af0,400afb,401964)
92 Instruction 0x4019a3: movzx eax, word ptr [rbp-0x1c] 1 10,11 0
    x60448a 0xb
93 ...
94 Function 1 exit xMBTCPPortSendResponse
95 Function 1 exit eMBTCPSend
96 Function 1 exit eMBPoll
```

Fig. S1 A log example recorded by ICSPRF when monitoring the execution of processing a request by freemodbus