```
     004226F2 55                 push    ebp
     004226F3 8BEC               mov     ebp, esp
     004226F5 6AFF               push    0xFF
     004226F7 6888F14200         push    0x0042F188
     004226FC 6854924200         push    0x00429254
     00422701 64A100000000       mov     eax, dword fs:[0x00000000]
     00422707 50                 push    eax
     00422708 64892500000000     mov     dword fs:[0x00000000], esp
     0042270F 83EC10             sub     esp, 0x10
     00422712 53                 push    ebx
     00422713 56                 push    esi
     00422714 57                 push    edi
     00422715 8965E8             mov     dword [ebp-0x18], esp
     00422718 FF1504E14200       call    dword [0x0042E104]
     0042271E 33D2               xor     edx, edx
     00422720 8AD4               mov     dl, ah
     00422722 8915D0704400       mov     dword [0x004470D0], edx
     00422728 8BC8               mov     ecx, eax
     0042272A 81E1FF000000       and     ecx, 0x000000FF
     00422730 890DCC704400       mov     dword [0x004470CC], ecx
     00422736 C1E108             shl     ecx, 0x08
     00422739 03CA               add     ecx, edx
     0042273B 890DC8704400       mov     dword [0x004470C8], ecx
     00422741 C1E810             shr     eax, 0x10
     00422744 A3C4704400         mov     dword [0x004470C4], eax
     00422749 6A01               push    0x01
     0042274B E899570000         call    0x00427EE9              +L09
     00422750 59                 pop     ecx
     00422751 85C0               test    eax, eax
     00422753 7508               jne     0x0042275D              +L04
     ------------------------------------------------------------------
     00422755 6A1C               push    0x1C
     00422757 E8AB000000         call    0x00422807              +L06
     0042275C 59                 pop     ecx
L04:0042275D E895070000         call    0x00422EF7              +L07
     00422762 85C0               test    eax, eax
     00422764 7508               jne     0x0042276E              +L05
     ------------------------------------------------------------------
     00422766 6A10               push    0x10
     00422768 E89A000000         call    0x00422807              +L06
     0042276D 59                 pop     ecx
L05:0042276E 8365FC00           and     dword [ebp-0x04], 0x00
     00422772 E8172F0000         call    0x0042568E              +L08
     00422777 FF1548E04200       call    dword [0x0042E048]
     0042277D A3847A4400         mov     dword [0x00447A84], eax
     00422782 E811710000         call    0x00429898              +L13
     00422787 A33C714400         mov     dword [0x0044713C], eax
     0042278C E8BA6E0000         call    0x0042964B              +L12
     00422791 E8FC6D0000         call    0x00429592              +L11
     00422796 E832EBFFFF         call    0x004212CD              -L02
     0042279B A1E0704400         mov     eax, dword [0x004470E0]
     004227A0 A3E4704400         mov     dword [0x004470E4], eax
     004227A5 50                 push    eax
     004227A6 FF35D8704400       push    dword [0x004470D8]
     004227AC FF35D4704400       push    dword [0x004470D4]
     004227B2 E8898AFFFF         call    0x00418240              -L01
     004227B7 83C40C             add     esp, 0x0C
     004227BA 8945E4             mov     dword [ebp-0x1C], eax
     004227BD 50                 push    eax
     004227BE E837EBFFFF         call    0x004212FA              -L03
     004227C3 8B45EC             mov     eax, dword [ebp-0x14]
     004227C6 8B08               mov     ecx, dword [eax]
     004227C8 8B09               mov     ecx, dword [ecx]
     004227CA 894DE0             mov     dword [ebp-0x20], ecx
     004227CD 50                 push    eax
     004227CE 51                 push    ecx
     004227CF E8456C0000         call    0x0042941A              +L10
     004227D4 59                 pop     ecx
     004227D5 59                 pop     ecx
     004227D6 C3                 ret
```

FIG. 1
(Prior Art)

```
        13145550 8D12                lea     edx, dword [edx]
        13145552 6800621413          push    0x13146200
        13145557 58                  pop     eax
        13145558 8D3F                lea     edi, dword [edi]
        1314555A DA0C24              fimul   dword [esp]
        1314555D D9FC                frndint
        1314555F 9C                  pushfd
        13145560 DA0424              fiadd   dword [esp]
        13145563 0E                  push    cs
        13145564 D9C8                fxch    st(0), st(0)
        13145566 DDE4                fucom   st(4), st(0)
        13145568 D9EE                fldz
        1314556A D9FE                fsin
        1314556C 8D6D00              lea     ebp, dword [ebp+0x00]
        1314556F 50                  push    eax
        13145570 D9E4                ftst
        13145572 D9FA                fsqrt
        13145574 8D00                lea     eax, dword [eax]
        13145576 DDE6                fucom   st(6), st(0)
        13145578 87F6                xchg    esi, esi
        1314557A 8B4C2404            mov     ecx, dword [esp+0x04]
        1314557E DA1424              ficom   dword [esp]
        13145581 D9FB                fsincos
        13145583 87D2                xchg    edx, edx
        13145585 D9CE                fxch    st(0), st(6)
        13145587 8D36                lea     esi, dword [esi]
        13145589 30C9                xor     cl, cl
        1314558B D9E0                fchs
        1314558D D9FB                fsincos
        1314558F 89D2                mov     edx, edx
        13145591 E308                jecxz   0x1314559E              +L01
        ------------------------------------------------------------------
        13145593 D9FC                frndint
        13145595 89DB                mov     ebx, ebx
        13145597 DF2424              fbld    byte [esp]
        1314559A EB63                jmp     0x131455FF              +L03
        ------------------------------------------------------------------
        1314559C 87F6                xchg    esi, esi
L01:    1314559E D9F0                f2xm1
        131455A0 BA0000007F          mov     edx, 0x7F000000
        131455A5 D9CB                fxch    st(0), st(3)
        131455A7 8D6D00              lea     ebp, dword [ebp+0x00]
        131455AA DA1424              ficom   dword [esp]
        131455AD 8B921400FE00        mov     edx, dword [edx+0x00FE0014]
        131455B3 87ED                xchg    ebp, ebp
        131455B5 DA1424              ficom   dword [esp]
        131455B8 D9F1                fyl2x
        131455BA B90000F701          mov     ecx, 0x01F70000
        131455BF 87D2                xchg    edx, edx
        131455C1 DDE6                fucom   st(6), st(0)
        131455C3 87F6                xchg    esi, esi
        131455C5 87D2                xchg    edx, edx
        131455C7 89D2                mov     edx, edx
L02:    131455C9 FC                  cld
        131455CA D82424              fsub    dword [esp]
        131455CD 89C0                mov     eax, eax
        131455CF 89C9                mov     ecx, ecx
        131455D1 E2F6                loop    0x131455C9              +L02
        ------------------------------------------------------------------
        131455D3 87DB                xchg    ebx, ebx
        131455D5 B90000007F          mov     ecx, 0x7F000000
        131455DA 8D1B                lea     ebx, dword [ebx]
        131455DC 89DB                mov     ebx, ebx
        131455DE 89FF                mov     edi, edi
        131455E0 8B891400FE00        mov     ecx, dword [ecx+0x00FE0014]
        131455E6 8D36                lea     esi, dword [esi]
        131455E8 29CA                sub     edx, ecx
        131455EA 87ED                xchg    ebp, ebp
        131455EC 90                  nop
        131455ED 85D2                test    edx, edx
        131455EF D9E8                fldpi
        131455F1 89C9                mov     ecx, ecx
        131455F3 D9EC                fldlg2
        131455F5 7508                jne     0x131455FF              +L03
```

FIG. 2

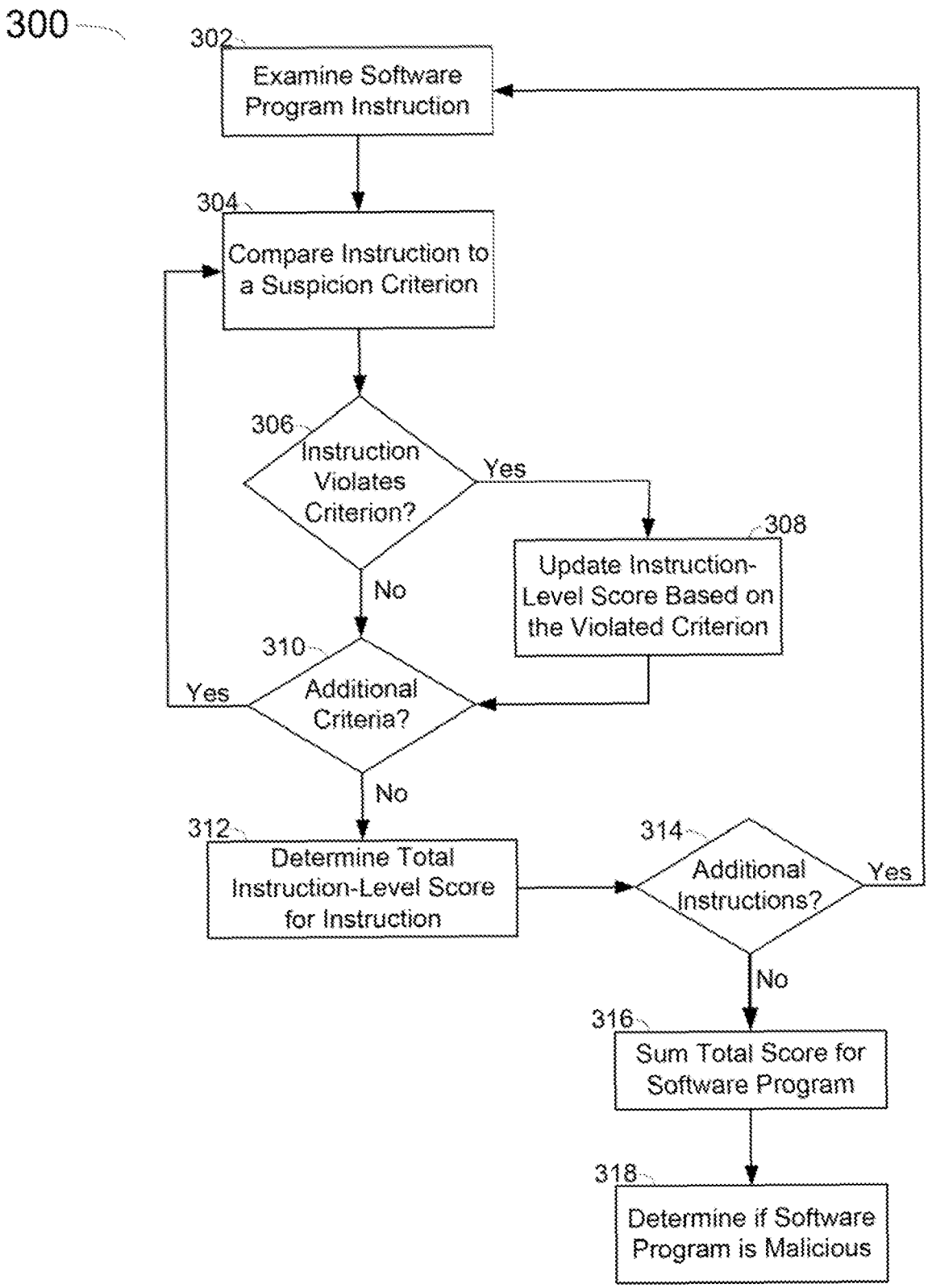
300
302
Examine Software Program Instruction
304
Compare Instruction to a Suspicion Criterion
306
Instruction Violates Criterion?
Yes
No
308
Update Instruction-Level Score Based on the Violated Criterion
310
Additional Criteria?
Yes
No
312
Determine Total Instruction-Level Score for Instruction
314
Additional Instructions?
Yes
No
316
Sum Total Score for Software Program
318
Determine if Software Program is Malicious

FIG. 3

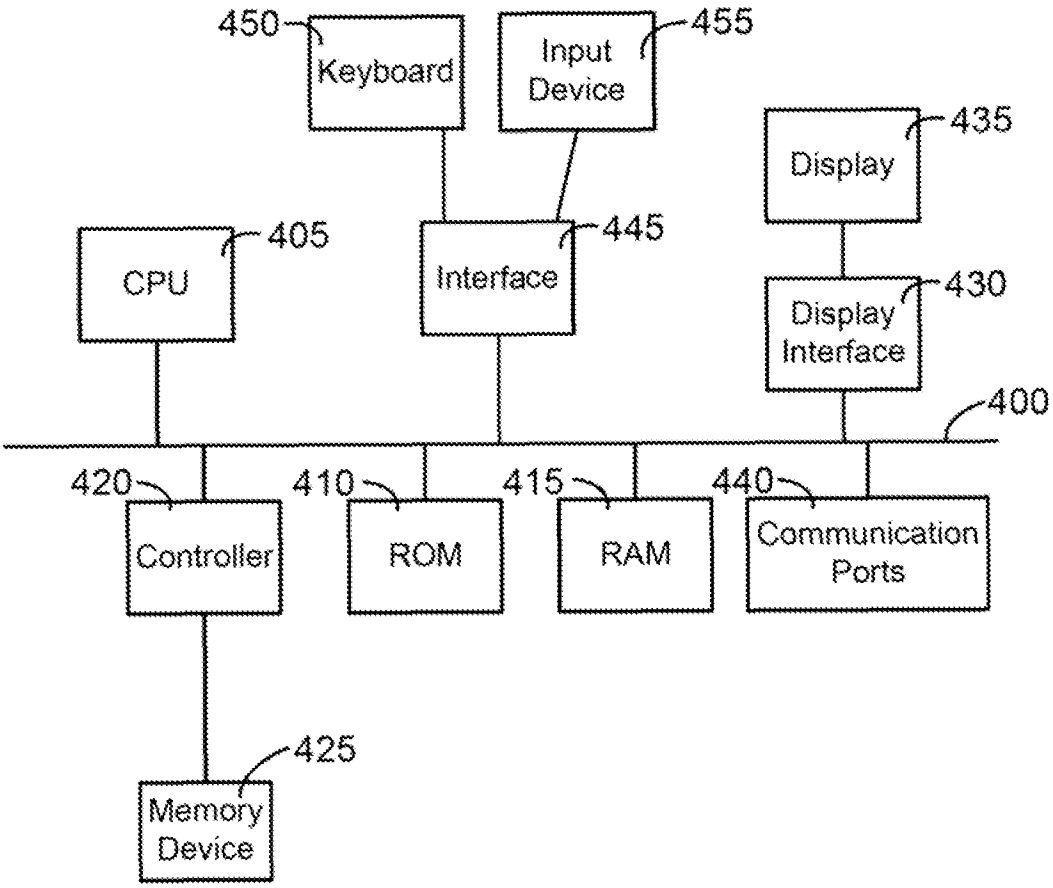
450
Keyboard
Input Device
455
Display
435
CPU
405
Interface
445
Display Interface
430
400
420
Controller
410
ROM
415
RAM
440
Communication Ports
425
Memory Device

Fig. 4