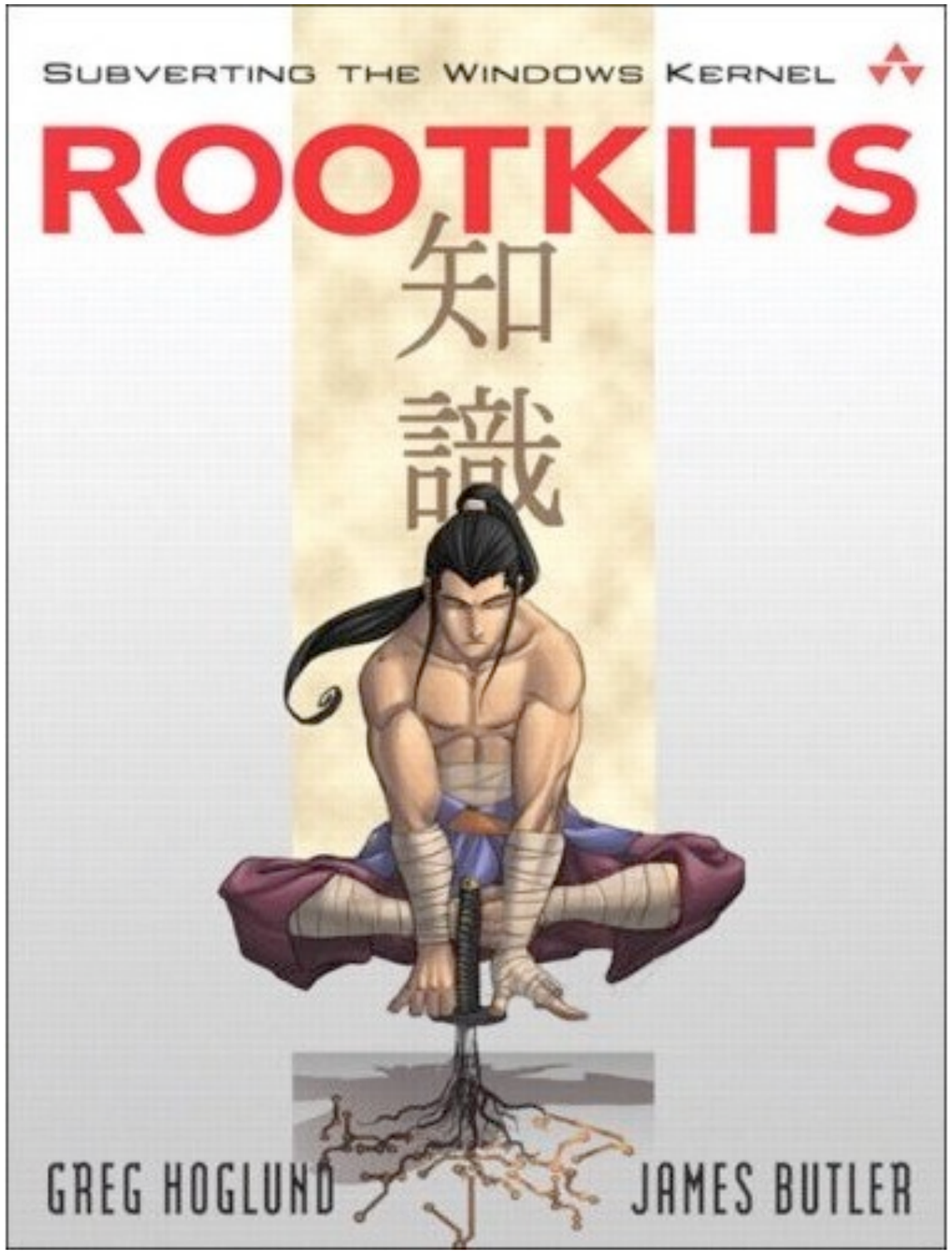
Robust Signatures for Kernel Data Structures

Brendan Dolan-Gavitt, Abhinav Srivastava,
Patrick Traynor, and Jonathon Giffin

Georgia Institute of Technology

{brendan,abhinav,traynor,giffin}@cc.gatech.edu

Context

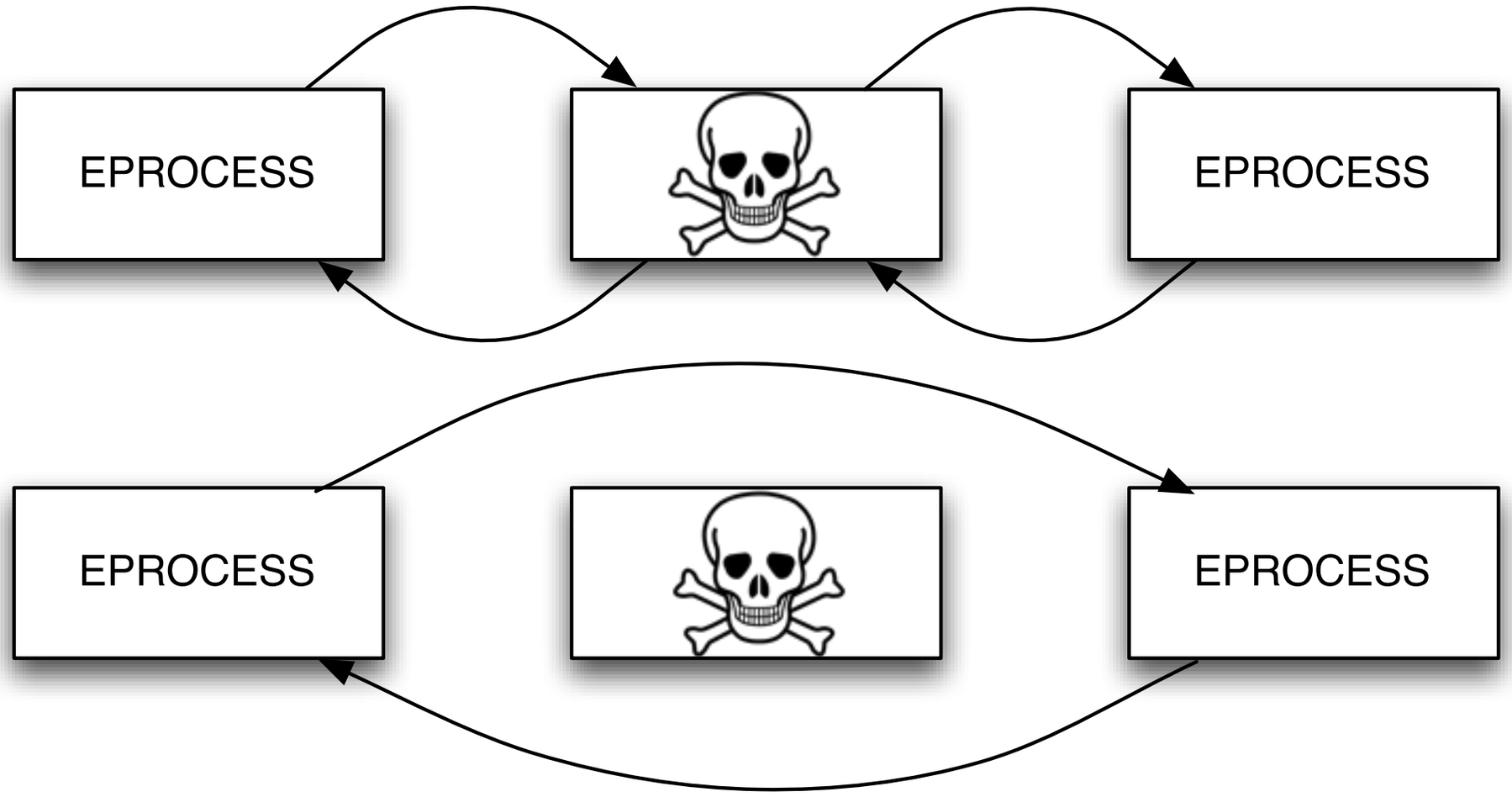

SUBVERTING THE WINDOWS KERNEL
ROOTKITS
知識
GREG HOGLUND
JAMES BUTLER

Attacks

- Objective: conceal presence of an object from the user
  - Hooking: modify code, make the APIs lie
  - DKOM: manipulate kernel data structures instead of code

DKOM Example

Before



After

Signature Scans

- Some new tools (PTFinder, Volatility) use *signature scans* to find hidden objects in memory
- Identify a set of invariants for the object
- Perform a linear scan through memory
- Report regions of data where the fields match your invariants

Signature Evasion

- What if an attacker can modify some of those fields?
- False negative for a signature
- Attacker can hide his object from scanners

Contributions

- Explore effectiveness of signature evasion attacks
- Develop robust signatures that resist evasion
- Automate the process to keep up with OS development

Signature Example

```
typedef struct _EPROCESS {
   UCHAR Type;
   UCHAR Size;
   ULONG DirectoryTableBase;
   LIST_ENTRY ThreadListHead;
   UCHAR WorkingSetLock.Type;
   UCHAR WorkingSetLock.Size;
   UCHAR AddressCreationLock.Type;
   UCHAR AddressCreationLock.Size;
} EPROCESS;
```

0x03

0x1b

page-aligned

Kernel

0x01

0x04

0x01

0x04

```
4f00 500a 5072 6fe3 ef00 0000 0500 0000  O.P.Pro.........
388e 3c82 0000 0020 a036 1e82 af30 61e2  8.<.... .6...0a.
0300 1b00 0000 0000 68e8 4681 68e8 4681  ........h.F.h.F.
70e8 4681 70e8 4681 00f0 b717 0080 c117  p.F.p.F.........
0000 0000 0000 0000 0000 0000 0000 0000  ................
ac20 0000 0000 0000 6e07 0000 e001 0000  . ......n.......
a0e8 4681 a0e8 4681 0000 0000 0000 0000  ..F...F.........
18e4 4681 587f 86ff 0000 0000 0100 0000  ..F.X...........
0a00 0806 0000 0000 0000 0000 0000 0000  ................
70b5 afb7 c480 c501 0000 0000 0000 0000  p...............
0000 0000 5809 0000 881b 0d82 28c7 0282  ....X.......(...
884a 0000 4466 0100 160e 0000 d85a 0000  .J..Df.......Z..
3096 0100 c20e 0000 160e 0000 00a0 cd06  0...............
0060 e305 b41b 0d82 54c7 0282 0000 0000  .`......T.......
683f 02e1 88a3 cfe1 4cd7 c9e1 0100 0000  h?......L.......
3ce4 d6f5 0000 0000 0100 0400 0000 0000  <...............
40e9 4681 40e9 4681 0100 0000 1a7b 0100  @.F.@.F......{..
0100 0000 0000 0000 0000 0000 0100 0400  ................
0000 0000 64e9 4681 64e9 4681 0000 0000  ....d.F.d.F.....
0000 0000 0000 0000 0000 0000 2843 1b82  ............(C..
2843 1b82 0000 0000 0a0b 0000 0000 0000  (C..............
08b0 c9e1 0000 0000 a874 cbe1 0000 0001  .........t......
a036 1e82 0000 0000 3000 0000 fc08 0000  .6......0.......
0000 0000 0000 0000 0000 0000 a815 f3e1  ................
c0e9 4681 c0e9 4681 0000 0000 0000 0000  ..F...F.........
0030 a9f8 6578 706c 6f72 6572 2e65 7865  .0..explorer.exe
0000 0000 0000 0000 0000 0000 0000 0000  ................
94e4 4681 d47f 86ff 0000 0000 0000 0000  ..F.............
1200 0000 ff0f 1f00 0000 0000 0000 0000  ................
```

Type == 0x03

```
4f00 500a 5072 6fe3 ef00 0000 0500 0000  O.P.Pro.........
388e 3c82 0000 0020 a036 1e82 af30 61e2  8.<.... .6...0a.
0300 1b00 0000 0000 68e8 4681 68e8 4681  ........h.F.h.F.
70e8 4681 70e8 4681 00f0 b717 0080 c117  p.F.p.F.........
0000 0000 0000 0000 0000 0000 0000 0000  ................
ac20 0000 0000 0000 6e07 0000 e001 0000  . ......n.......
a0e8 4681 a0e8 4681 0000 0000 0000 0000  ..F...F.........
18e4 4681 587f 86ff 0000 0000 0100 0000  ..F.X...........
0a00 0806 0000 0000 0000 0000 0000 0000  ................
70b5 afb7 c480 c501 0000 0000 0000 0000  p...............
0000 0000 5809 0000 881b 0d82 28c7 0282  ....X.......(...
884a 0000 4466 0100 160e 0000 d85a 0000  .J..Df.......Z..
3096 0100 c20e 0000 160e 0000 00a0 cd06  0...............
0060 e305 b41b 0d82 54c7 0282 0000 0000  .`......T.......
683f 02e1 88a3 cfe1 4cd7 c9e1 0100 0000  h?......L.......
3ce4 d6f5 0000 0000 0100 0400 0000 0000  <...............
40e9 4681 40e9 4681 0100 0000 1a7b 0100  @.F.@.F......{..
0100 0000 0000 0000 0000 0000 0100 0400  ................
0000 0000 64e9 4681 64e9 4681 0000 0000  ....d.F.d.F.....
0000 0000 0000 0000 0000 0000 2843 1b82  ............(C..
2843 1b82 0000 0000 0a0b 0000 0000 0000  (C..............
08b0 c9e1 0000 0000 a874 cbe1 0000 0001  .........t......
a036 1e82 0000 0000 3000 0000 fc08 0000  .6......0.......
0000 0000 0000 0000 0000 0000 a815 f3e1  ................
c0e9 4681 c0e9 4681 0000 0000 0000 0000  ..F...F.........
0030 a9f8 6578 706c 6f72 6572 2e65 7865  .0..explorer.exe
0000 0000 0000 0000 0000 0000 0000 0000  ................
94e4 4681 d47f 86ff 0000 0000 0000 0000  ..F.............
1200 0000 ff0f 1f00 0000 0000 0000 0000  ................
```

Size == 0x1b

Type == 0x03

```
4f00 500a 5072 61e3 ef00 0000 0500 0000  O.P.Pro.........
388e 3c82 0000 0020 a036 1e82 af30 61e2  8.<.... .6...0a.
0300 1b00 0000 0000 68e8 4681 68e8 4681  ........h.F.h.F.
70e8 4681 70e8 4681 00f0 b717 0080 c117  p.F.p.F.........
0000 0000 0000 0000 0000 0000 0000 0000  ................
ac20 0000 0000 0000 6e07 0000 e001 0000  . ......n.......
a0e8 4681 a0e8 4681 0000 0000 0000 0000  ..F...F.........
18e4 4681 587f 86ff 0000 0000 0100 0000  ..F.X...........
0a00 0806 0000 0000 0000 0000 0000 0000  ................
70b5 afb7 c480 c501 0000 0000 0000 0000  p...............
0000 0000 5809 0000 881b 0d82 28c7 0282  ....X.......(...
884a 0000 4466 0100 160e 0000 d85a 0000  .J..Df.......Z..
3096 0100 c20e 0000 160e 0000 00a0 cd06  0...............
0060 e305 b41b 0d82 54c7 0282 0000 0000  .`......T.......
683f 02e1 88a3 cfe1 4cd7 c9e1 0100 0000  h?......L.......
3ce4 d6f5 0000 0000 0100 0400 0000 0000  <...............
40e9 4681 40e9 4681 0100 0000 1a7b 0100  @.F.@.F......{..
0100 0000 0000 0000 0000 0000 0100 0400  ................
0000 0000 64e9 4681 64e9 4681 0000 0000  ....d.F.d.F.....
0000 0000 0000 0000 0000 0000 2843 1b82  ............(C..
2843 1b82 0000 0000 0a0b 0000 0000 0000  (C..............
08b0 c9e1 0000 0000 a874 cbe1 0000 0001  .........t......
a036 1e82 0000 0000 3000 0000 fc08 0000  .6......0.......
0000 0000 0000 0000 0000 0000 a815 f3e1  ................
c0e9 4681 c0e9 4681 0000 0000 0000 0000  ..F...F.........
0030 a9f8 6578 706c 6f72 6572 2e65 7865  .0..explorer.exe
0000 0000 0000 0000 0000 0000 0000 0000  ................
94e4 4681 d47f 86ff 0000 0000 0000 0000  ..F.............
1200 0000 ff0f 1f00 0000 0000 0000 0000  ................
```

Size == 0x1b

Type == 0x03

DirectoryTableBase
page-aligned

```
4f00 500a 5072 61e3 ef00 0000 0500 0000  O.P.Pro.........
388e 3c82 0000 0020 a036 1e82 af30 61e2  8.<.... .6...0a.
0300 1b00 0000 0000 68e8 4681 68e8 4681  ........h.F.h.F.
70e8 4681 70e8 4681 00f0 b717 0080 c117  p.F.p.F.........
0000 0000 0000 0000 0000 0000 0000 0000  ................
ac20 0000 0000 0000 6e07 0000 e001 0000  . ......n.......
a0e8 4681 a0e8 4681 0000 0000 0000 0000  ..F...F.........
18e4 4681 587f 86ff 000                  ..F.X..........
0a00 0806 0000 0000 000                  ...............
70b5 afb7 c480 c501 0000 0000 0000 0000  p...............
0000 0000 5809 0000 881b 0d82 28c7 0282  ....X.......(...
884a 0000 4466 0100 160e 0000 d85a 0000  .J..Df.......Z..
3096 0100 c20e 0000 160e 0000 00a0 cd06  0...............
0060 e305 b41b 0d82 54c7 0282 0000 0000  .`......T.......
683f 02e1 88a3 cfe1 4cd7 c9e1 0100 0000  h?......L.......
3ce4 d6f5 0000 0000 0100 0400 0000 0000  <...............
40e9 4681 40e9 4681 0100 0000 1a7b 0100  @.F.@.F......{..
0100 0000 0000 0000 0000 0000 0100 0400  ................
0000 0000 64e9 4681 64e9 4681 0000 0000  ....d.F.d.F.....
0000 0000 0000 0000 0000 0000 2843 1b82  ............(C..
2843 1b82 0000 0000 0a0b 0000 0000 0000  (C..............
08b0 c9e1 0000 0000 a874 cbe1 0000 0001  .........t......
a036 1e82 0000 0000 3000 0000 fc08 0000  .6......0.......
0000 0000 0000 0000 0000 0000 a815 f3e1  ................
c0e9 4681 c0e9 4681 0000 0000 0000 0000  ..F...F.........
0030 a9f8 6578 706c 6f72 6572 2e65 7865  .0..explorer.exe
0000 0000 0000 0000 0000 0000 0000 0000  ................
94e4 4681 d47f 86ff 0000 0000 0000 0000  ..F.............
1200 0000 ff0f 1f00 0000 0000 0000 0000  ................
```

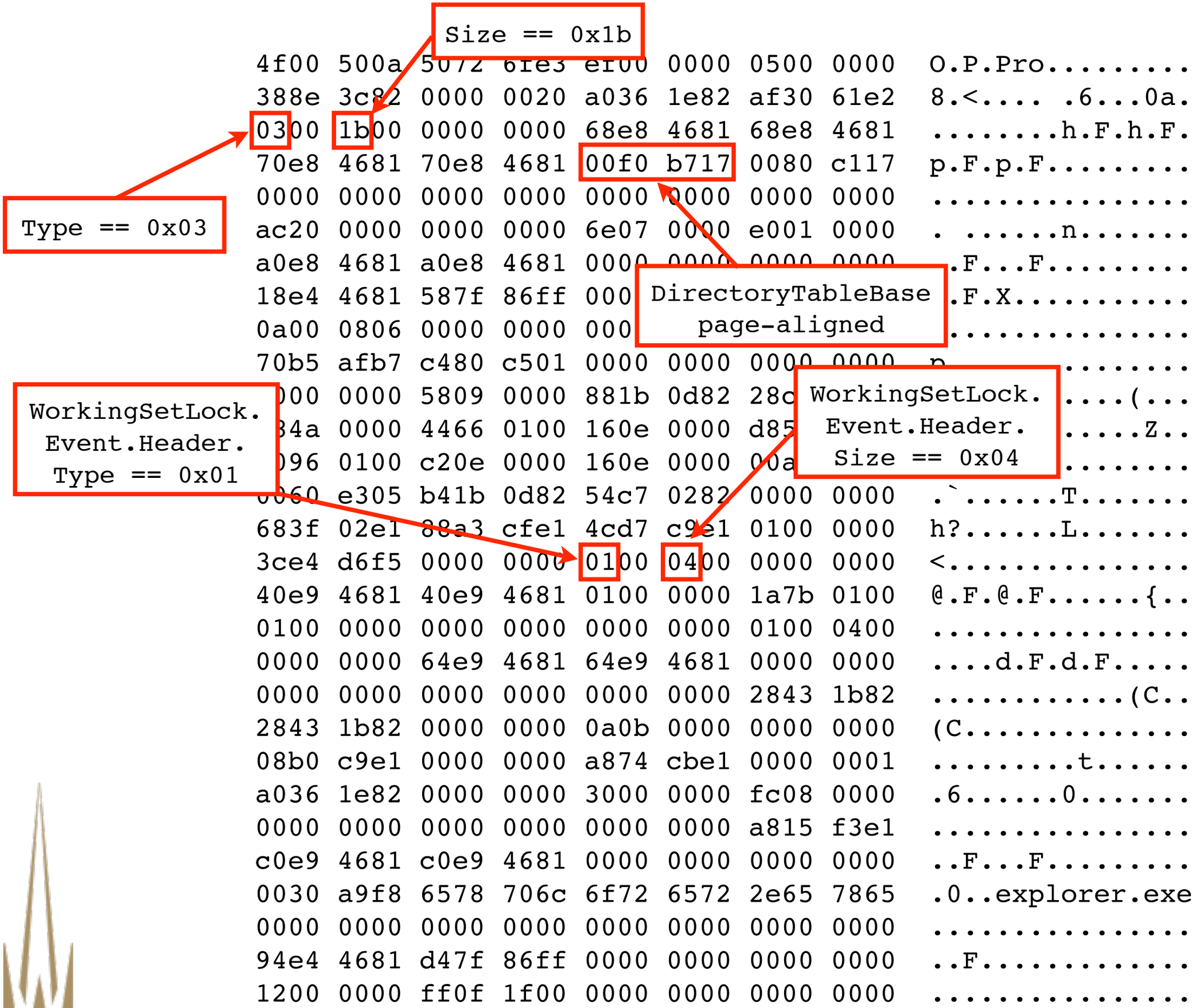
Size == 0x1b

Type == 0x03

DirectoryTableBase
page-aligned

WorkingSetLock.
Event.Header.
Type == 0x01

```
4f00 500a 5072 61e3 ef00 0000 0500 0000  O.P.Pro.........
388e 3c82 0000 0020 a036 1e82 af30 61e2  8.<.... .6...0a.
0300 1b00 0000 0000 68e8 4681 68e8 4681  ........h.F.h.F.
70e8 4681 70e8 4681 00f0 b717 0080 c117  p.F.p.F.........
0000 0000 0000 0000 0000 0000 0000 0000  ................
ac20 0000 0000 0000 6e07 0000 e001 0000  . ......n.......
a0e8 4681 a0e8 4681 0000 0000 0000 0000  ..F...F.........
18e4 4681 587f 86ff 000                  .F.X...........
0a00 0806 0000 0000 000                  ...............
70b5 afb7 c480 c501 0000 0000 0000 0000  p...............
000 0000 5809 0000 881b 0d82 28c7 0282   ....X.......(...
34a 0000 4466 0100 160e 0000 d85a 0000   .J..Df.......Z..
096 0100 c20e 0000 160e 0000 00a0 cd06   0...............
060 e305 b41b 0d82 54c7 0282 0000 0000   .`......T.......
683f 02e1 88a3 cfe1 4cd7 c9e1 0100 0000  h?......L.......
3ce4 d6f5 0000 0000 0100 0400 0000 0000  <...............
40e9 4681 40e9 4681 0100 0000 1a7b 0100  @.F.@.F......{..
0100 0000 0000 0000 0000 0000 0100 0400  ................
0000 0000 64e9 4681 64e9 4681 0000 0000  ....d.F.d.F.....
0000 0000 0000 0000 0000 0000 2843 1b82  ............(C..
2843 1b82 0000 0000 0a0b 0000 0000 0000  (C..............
08b0 c9e1 0000 0000 a874 cbe1 0000 0001  .........t......
a036 1e82 0000 0000 3000 0000 fc08 0000  .6......0.......
0000 0000 0000 0000 0000 0000 a815 f3e1  ................
c0e9 4681 c0e9 4681 0000 0000 0000 0000  ..F...F.........
0030 a9f8 6578 706c 6f72 6572 2e65 7865  .0..explorer.exe
0000 0000 0000 0000 0000 0000 0000 0000  ................
94e4 4681 d47f 86ff 0000 0000 0000 0000  ..F.............
1200 0000 ff0f 1f00 0000 0000 0000 0000  ................
```


Size == 0x1b
Type == 0x03
DirectoryTableBase
page-aligned
WorkingSetLock.
Event.Header.
Type == 0x01
WorkingSetLock.
Event.Header.
Size == 0x04
4f00 500a 5072 61e3 ef00 0000 0500 0000 O.P.Pro.....
388e 3c82 0000 0020 a036 1e82 af30 61e2 8.<.... .6...0a.
0300 1b00 0000 0000 68e8 4681 68e8 4681 ....h.F.h.F.
70e8 4681 70e8 4681 00f0 b717 0080 c117 p.F.p.F.....
0000 0000 0000 0000 0000 0000 0000 0000 ....
ac20 0000 0000 0000 6e07 0000 e001 0000 . ...n.....
a0e8 4681 a0e8 4681 0000 0000 0000 0000 .F...F.....
18e4 4681 587f 86ff 000 .F.X.....
0a00 0806 0000 0000 000 ....
70b5 afb7 c480 c501 0000 0000 0000 0000 p.....
000 0000 5809 0000 881b 0d82 28c ....(...
34a 0000 4466 0100 160e 0000 d85 .....Z..
096 0100 c20e 0000 160e 0000 00a .....
060 e305 b41b 0d82 54c7 0282 0000 0000 .`.....T.....
683f 02e1 88a3 cfe1 4cd7 c9e1 0100 0000 h?.....L.....
3ce4 d6f5 0000 0000 0100 0400 0000 0000 <.....
40e9 4681 40e9 4681 0100 0000 1a7b 0100 @.F.@.F.....{..
0100 0000 0000 0000 0000 0000 0100 0400 ....
0000 0000 64e9 4681 64e9 4681 0000 0000 ....d.F.d.F.....
0000 0000 0000 0000 0000 0000 2843 1b82 ....(C..
2843 1b82 0000 0000 0a0b 0000 0000 0000 (C.....
08b0 c9e1 0000 0000 a874 cbe1 0000 0001 .....t.....
a036 1e82 0000 0000 3000 0000 fc08 0000 .6.....0.....
0000 0000 0000 0000 0000 0000 a815 f3e1 ....
c0e9 4681 c0e9 4681 0000 0000 0000 0000 ..F...F.....
0030 a9f8 6578 706c 6f72 6572 2e65 7865 .0..explorer.exe
0000 0000 0000 0000 0000 0000 0000 0000 ....
94e4 4681 d47f 86ff 0000 0000 0000 0000 ..F.....
1200 0000 ff0f 1f00 0000 0000 0000 0000 ....

Size == 0x1b

Type == 0x03

DirectoryTableBase
page-aligned

WorkingSetLock.
Event.Header.
Type == 0x01

WorkingSetLock.
Event.Header.
Size == 0x04

AddressCreation
Lock.Event.
Header.Type
== 0x01

```
4f00 500a 5072 61e3 ef00 0000 0500 0000  O.P.Pro.........
388e 3c82 0000 0020 a036 1e82 af30 61e2  8.<.... .6...0a.
0300 1b00 0000 0000 68e8 4681 68e8 4681  ........h.F.h.F.
70e8 4681 70e8 4681 00f0 b717 0080 c117  p.F.p.F.........
0000 0000 0000 0000 0000 0000 0000 0000  ................
ac20 0000 0000 0000 6e07 0000 e001 0000  . ......n.......
a0e8 4681 a0e8 4681 0000 0000 0000 0000  ..F...F.........
18e4 4681 587f 86ff 000                  .F.X...........
0a00 0806 0000 0000 000                  ...............
70b5 afb7 c480 c501 0000 0000 0000 0000  p...............
000 0000 5809 0000 881b 0d82 28c         ....X.....(...
34a 0000 4466 0100 160e 0000 d85         ....Df.....Z..
096 0100 c20e 0000 160e 0000 00a         ................
060 e305 b41b 0d82 54c7 0282 0000 0000   .`......T.......
683f 02e1 88a3 cfe1 4cd7 c9e1 0100 0000  h?......L.......
3ce4 d6f5 0000 0000 0100 0400 0000 0000  <...............
40e9 4681 40e9 4681 0100 0000 1a7b 0100  @.F.@.F......{..
100 0000 0000 0000 0000 0000 0100 0400   ................
000 0000 64e9 4681 64e9 4681 0000 0000   ....d.F.d.F.....
000 0000 0000 0000 0000 0000 2843 1b82   ............(C..
343 1b82 0000 0000 0a0b 0000 0000 0000   (C..............
08b0 c9e1 0000 0000 a874 cbe1 0000 0001  .........t......
a036 1e82 0000 0000 3000 0000 fc08 0000  .6......0.......
0000 0000 0000 0000 0000 0000 a815 f3e1  ................
c0e9 4681 c0e9 4681 0000 0000 0000 0000  ..F...F.........
0030 a9f8 6578 706c 6f72 6572 2e65 7865  .0..explorer.exe
0000 0000 0000 0000 0000 0000 0000 0000  ................
94e4 4681 d47f 86ff 0000 0000 0000 0000  ..F.............
1200 0000 ff0f 1f00 0000 0000 0000 0000  ................
```

Size == 0x1b

Type == 0x03

DirectoryTableBase
page-aligned

WorkingSetLock.
Event.Header.
Type == 0x01

WorkingSetLock.
Event.Header.
Size == 0x04

AddressCreation
Lock.Event.
Header.Type
== 0x01

AddressCreation
Lock.Event.
Header.Size
== 0x04

```
4f00 500a 5072 61e3 ef00 0000 0500 0000  O.P.Pro.........
388e 3c82 0000 0020 a036 1e82 af30 61e2  8.<.... .6...0a.
0300 1b00 0000 0000 68e8 4681 68e8 4681  ........h.F.h.F.
70e8 4681 70e8 4681 00f0 b717 0080 c117  p.F.p.F.........
0000 0000 0000 0000 0000 0000 0000 0000  ................
ac20 0000 0000 0000 6e07 0000 e001 0000  . ......n.......
a0e8 4681 a0e8 4681 0000 0000 0000 0000  ..F...F.........
18e4 4681 587f 86ff 000                  .F.X...........
0a00 0806 0000 0000 000                  ...............
70b5 afb7 c480 c501 0000 0000 0000 0000  p...............
000 0000 5809 0000 881b 0d82 28c         ....X.....(...
34a 0000 4466 0100 160e 0000 d85         .....F.....Z..
096 0100 c20e 0000 160e 0000 00a         ...............
060 e305 b41b 0d82 54c7 0282 0000 0000   .`......T.......
683f 02e1 88a3 cfe1 4cd7 c9e1 0100 0000  h?......L.......
3ce4 d6f5 0000 0000 0100 0400 0000 0000  <...............
40e9 4681 40e9 4681 0100 0000 1a7b 0100  @.F.@.F......{..
100 0000 0000 0000 0000 0000 0100 0400   ...
000 0000 64e9 4681 64e9 4681 0000 0000   ...
000 0000 0000 0000 0000 0000 2843 1b82   ...
343 1b82 0000 0000 0a0b 0000 0000 0000   (C.
08b0 c9e1 0000 0000 a874 cbe1 0000 0001  ...
a036 1e82 0000 0000 3000 0000 fc08 0000  .6......0.......
0000 0000 0000 0000 0000 0000 a815 f3e1  ................
c0e9 4681 c0e9 4681 0000 0000 0000 0000  ..F...F.........
0030 a9f8 6578 706c 6f72 6572 2e65 7865  .0..explorer.exe
0000 0000 0000 0000 0000 0000 0000 0000  ................
94e4 4681 d47f 86ff 0000 0000 0000 0000  ..F.............
1200 0000 ff0f 1f00 0000 0000 0000 0000  ................
```

Size == 0x1b

Type == 0x03

DirectoryTableBase
page-aligned

WorkingSetLock.
Event.Header.
Type == 0x01

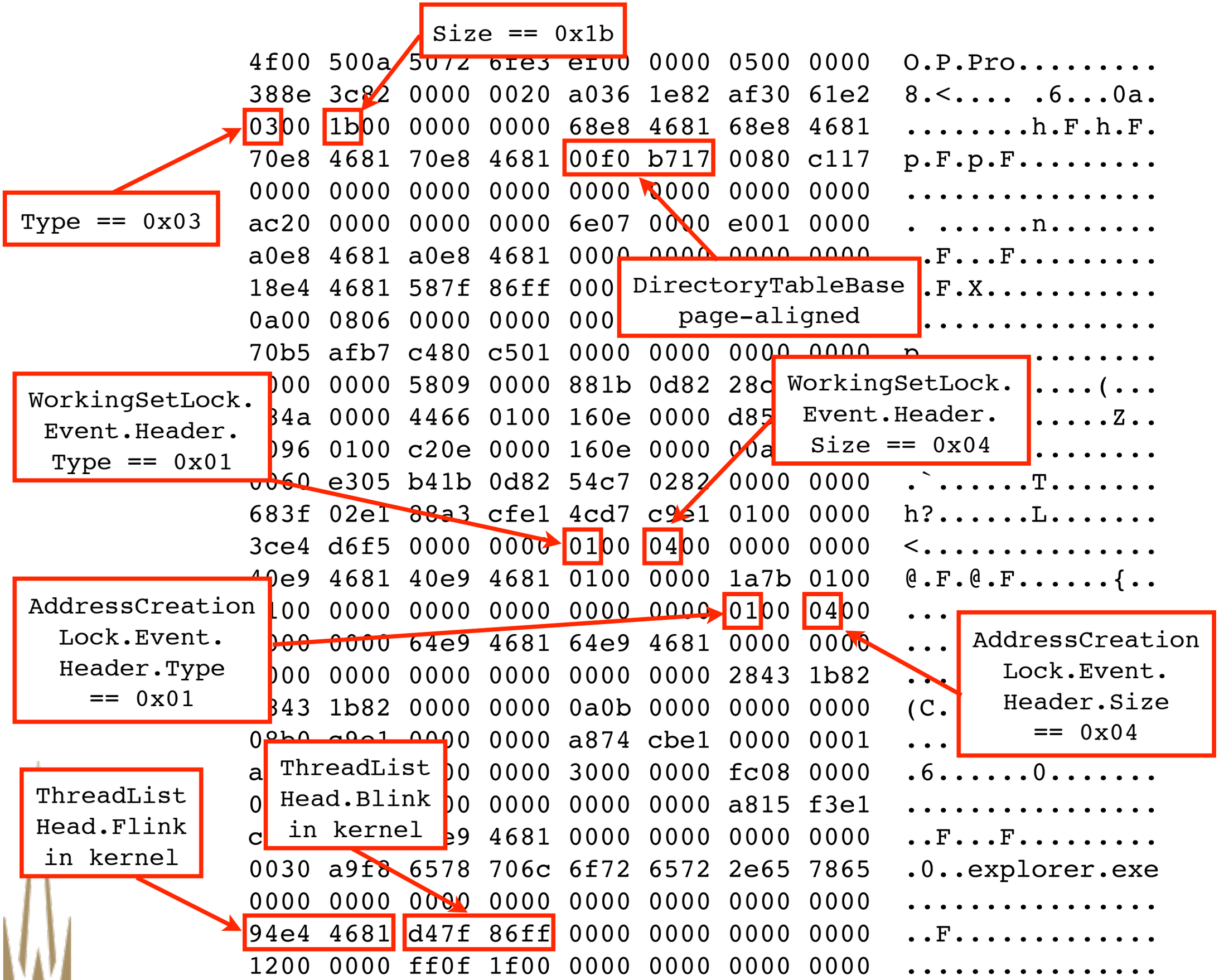
WorkingSetLock.
Event.Header.
Size == 0x04

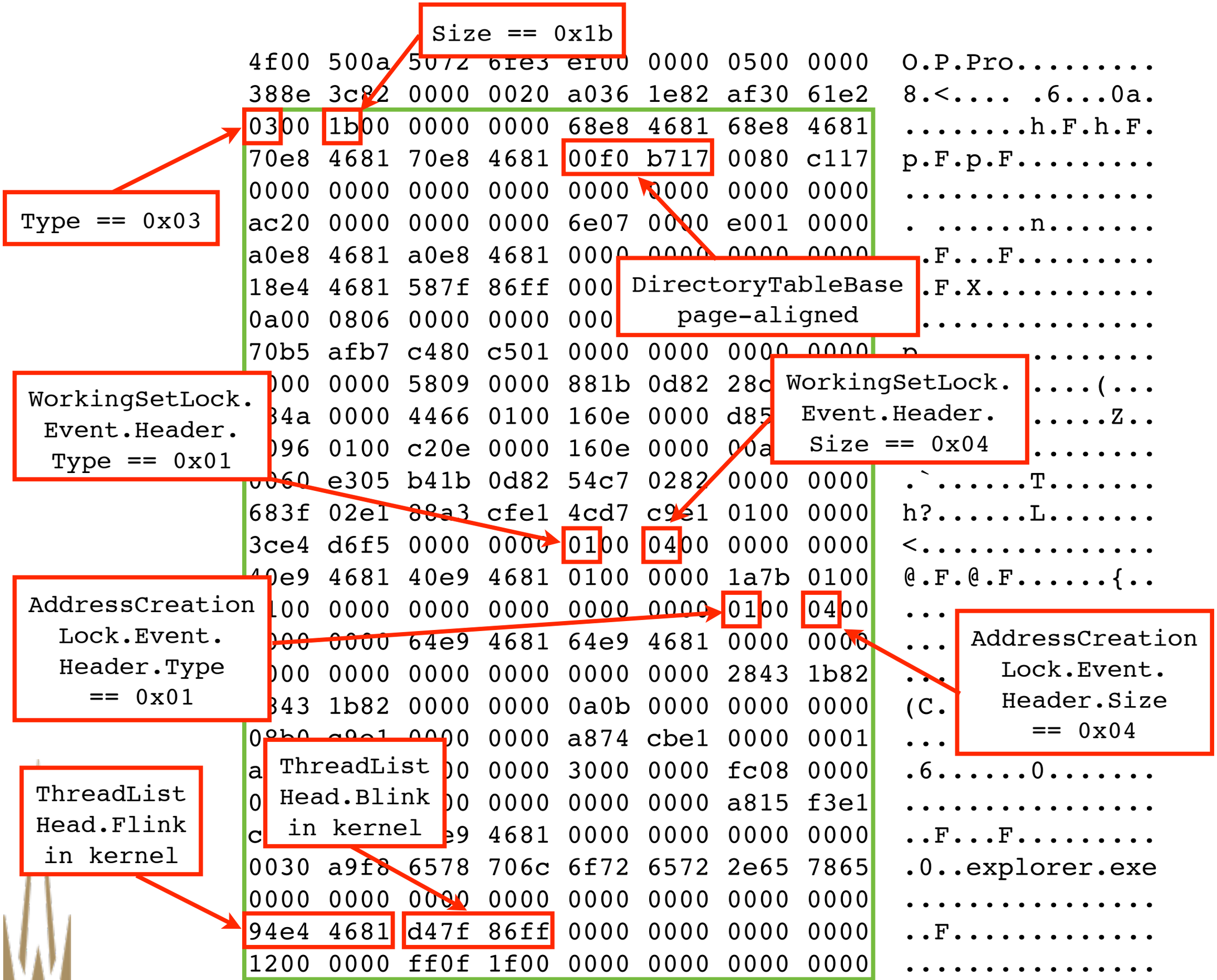
AddressCreation
Lock.Event.
Header.Type
== 0x01

AddressCreation
Lock.Event.
Header.Size
== 0x04

ThreadList
Head.Flink
in kernel

```
4f00 500a 5072 61e3 ef00 0000 0500 0000  O.P.Pro.........
388e 3c82 0000 0020 a036 1e82 af30 61e2  8.<.... .6...0a.
0300 1b00 0000 0000 68e8 4681 68e8 4681  ........h.F.h.F.
70e8 4681 70e8 4681 00f0 b717 0080 c117  p.F.p.F.........
0000 0000 0000 0000 0000 0000 0000 0000  ................
ac20 0000 0000 0000 6e07 0000 e001 0000  . ......n.......
a0e8 4681 a0e8 4681 0000 0000 0000 0000  ..F...F.........
18e4 4681 587f 86ff 000                  .F.X...........
0a00 0806 0000 0000 000                  ...............
70b5 afb7 c480 c501 0000 0000 0000 0000  p...............
   000 0000 5809 0000 881b 0d82 28c      ....X.....(...
   34a 0000 4466 0100 160e 0000 d85      ....Df.........Z..
   096 0100 c20e 0000 160e 0000 00a      ................
   060 e305 b41b 0d82 54c7 0282 0000 0000  .`......T.......
683f 02e1 88a3 cfe1 4cd7 c9e1 0100 0000  h?......L.......
3ce4 d6f5 0000 0000 0100 0400 0000 0000  <...............
40e9 4681 40e9 4681 0100 0000 1a7b 0100  @.F.@.F......{..
   100 0000 0000 0000 0000 0000 0100 0400  ...............
   000 0000 64e9 4681 64e9 4681 0000 0000  ....d.F.d.F.....
   000 0000 0000 0000 0000 0000 2843 1b82  ............(C..
   343 1b82 0000 0000 0a0b 0000 0000 0000  (C..............
08b0 c9e1 0000 0000 a874 cbe1 0000 0001  .........t......
a036 1e82 0000 0000 3000 0000 fc08 0000  .6......0.......
0000 0000 0000 0000 0000 0000 a815 f3e1  ................
c0e9 4681 c0e9 4681 0000 0000 0000 0000  ..F...F.........
0030 a9f8 6578 706c 6f72 6572 2e65 7865  .0..explorer.exe
0000 0000 0000 0000 0000 0000 0000 0000  ................
94e4 4681 d47f 86ff 0000 0000 0000 0000  ..F.............
1200 0000 ff0f 1f00 0000 0000 0000 0000  ................
```


Size == 0x1b
Type == 0x03
DirectoryTableBase
page-aligned
WorkingSetLock.
Event.Header.
Type == 0x01
WorkingSetLock.
Event.Header.
Size == 0x04
AddressCreation
Lock.Event.
Header.Type
== 0x01
AddressCreation
Lock.Event.
Header.Size
== 0x04
ThreadList
Head.Blink
in kernel
ThreadList
Head.Flink
in kernel
4f00 500a 5072 61e3 ef00 0000 0500 0000 O.P.Pro.....
388e 3c82 0000 0020 a036 1e82 af30 61e2 8.<.... .6...0a.
0300 1b00 0000 0000 68e8 4681 68e8 4681 ....h.F.h.F.
70e8 4681 70e8 4681 00f0 b717 0080 c117 p.F.p.F.....
0000 0000 0000 0000 0000 0000 0000 0000 ....
ac20 0000 0000 0000 6e07 0000 e001 0000 . ...n.....
a0e8 4681 a0e8 4681 0000 0000 0000 0000 .F...F.....
18e4 4681 587f 86ff 000 .F.X.....
0a00 0806 0000 0000 000 ....
70b5 afb7 c480 c501 0000 0000 0000 0000 p.....
000 0000 5809 0000 881b 0d82 28c ....(...
34a 0000 4466 0100 160e 0000 d85 .....Z..
096 0100 c20e 0000 160e 0000 00a .....
060 e305 b41b 0d82 54c7 0282 0000 0000 .`.....T.....
683f 02e1 88a3 cfe1 4cd7 c9e1 0100 0000 h?.....L.....
3ce4 d6f5 0000 0000 0100 0400 0000 0000 <.....
40e9 4681 40e9 4681 0100 0000 1a7b 0100 @.F.@.F.....{..
100 0000 0000 0000 0000 0000 0100 0400 ...
000 0000 64e9 4681 64e9 4681 0000 0000 ...
000 0000 0000 0000 0000 0000 2843 1b82 ...
343 1b82 0000 0000 0a0b 0000 0000 0000 (C.
08b0 c9e1 0000 0000 a874 cbe1 0000 0001 ...
a 00 0000 3000 0000 fc08 0000 .6.....0.....
0 00 0000 0000 0000 a815 f3e1 .....
c e9 4681 0000 0000 0000 0000 ..F...F.....
0030 a9f8 6578 706c 6f72 6572 2e65 7865 .0..explorer.exe
0000 0000 0000 0000 0000 0000 0000 0000 .....
94e4 4681 d47f 86ff 0000 0000 0000 0000 ..F.....
1200 0000 ff0f 1f00 0000 0000 0000 0000 .....


Size == 0x1b
Type == 0x03
DirectoryTableBase
page-aligned
WorkingSetLock.
Event.Header.
Type == 0x01
WorkingSetLock.
Event.Header.
Size == 0x04
AddressCreation
Lock.Event.
Header.Type
== 0x01
AddressCreation
Lock.Event.
Header.Size
== 0x04
ThreadList
Head.Blink
in kernel
ThreadList
Head.Flink
in kernel
4f00 500a 5072 61e3 ef00 0000 0500 0000 O.P.Pro.....
388e 3c82 0000 0020 a036 1e82 af30 61e2 8.<.... .6...0a.
0300 1b00 0000 0000 68e8 4681 68e8 4681 ....h.F.h.F.
70e8 4681 70e8 4681 00f0 b717 0080 c117 p.F.p.F.....
0000 0000 0000 0000 0000 0000 0000 0000 ....
ac20 0000 0000 0000 6e07 0000 e001 0000 . ...n.....
a0e8 4681 a0e8 4681 0000 0000 0000 0000 .F...F.....
18e4 4681 587f 86ff 000 .F.X.....
0a00 0806 0000 0000 000 ....
70b5 afb7 c480 c501 0000 0000 0000 0000 p.....
000 0000 5809 0000 881b 0d82 28c ....(...
34a 0000 4466 0100 160e 0000 d85 .....Z..
096 0100 c20e 0000 160e 0000 00a .....
060 e305 b41b 0d82 54c7 0282 0000 0000 .`.....T.....
683f 02e1 88a3 cfe1 4cd7 c9e1 0100 0000 h?.....L.....
3ce4 d6f5 0000 0000 0100 0400 0000 0000 <.....
40e9 4681 40e9 4681 0100 0000 1a7b 0100 @.F.@.F.....{..
100 0000 0000 0000 0000 0000 0100 0400 ...
000 0000 64e9 4681 64e9 4681 0000 0000 ...
000 0000 0000 0000 0000 0000 2843 1b82 ...
343 1b82 0000 0000 0a0b 0000 0000 0000 (C.
08b0 c9e1 0000 0000 a874 cbe1 0000 0001 ...
a 00 0000 3000 0000 fc08 0000 .6.....0.....
0 00 0000 0000 0000 a815 f3e1 ....
c e9 4681 0000 0000 0000 0000 ..F...F.....
0030 a9f8 6578 706c 6f72 6572 2e65 7865 .0..explorer.exe
0000 0000 0000 0000 0000 0000 0000 0000 ....
94e4 4681 d47f 86ff 0000 0000 0000 0000 ..F.....
1200 0000 ff0f 1f00 0000 0000 0000 0000 ....

Evasion Example

```
typedef struct _EPROCESS {
   UCHAR Type;
   UCHAR Size;
   ULONG DirectoryTableBase;
   LIST_ENTRY ThreadListHead;
   UCHAR WorkingSetLock.Type;
   UCHAR WorkingSetLock.Size;
   UCHAR AddressCreationLock.Type;
   UCHAR AddressCreationLock.Size;
} EPROCESS;
```

0x00

0x1b

page-aligned

Kernel

0x01

0x04

0x01

0x04

Is Evasion Possible?

Attacker modifying a field could impact system stability if OS relies on the value

```
*** STOP: 0x0000001E (0x80000003,0x80106fc0,0x8025ea21,0xfd6829e8)
Unhandled Kernel exception c0000047 from fa8418b4 (8025ea21,fd6829e8)

Dll Base Date Stamp - Name              Dll Base Date Stamp - Name
80100000 2be154c9 - ntoskrnl.exe        80400000 2bc153b0 - hal.dll
80258000 2bd49628 - ncrc710.sys         8025c000 2bd49688 - SCSIPORT.SYS
80267000 2bd49683 - scsidisk.sys        802a6000 2bd496b9 - Fastfat.sys
fa800000 2bd49666 - Floppy.SYS          fa810000 2bd496db - Hpfs_Rec.SYS
fa820000 2bd49676 - Null.SYS            fa830000 2bd4965a - Beep.SYS
fa840000 2bdaab00 - i8042prt.SYS        fa850000 2bd5a020 - SERMOUSE.SYS
fa860000 2bd4966f - kbdclass.SYS        fa870000 2bd49671 - MOUCLASS.SYS
fa880000 2bd9c0be - Videoprt.SYS        fa890000 2bd49638 - NCC1701E.SYS
fa8a0000 2bd4a4ce - Vga.SYS             fa8b0000 2bd496d0 - Msfs.SYS
fa8c0000 2bd496c3 - Npfs.SYS            fa8e0000 2bd496c9 - Ntfs.SYS
fa940000 2bd496df - NDIS.SYS            fa930000 2bd49707 - wdlan.sys
fa970000 2bd49712 - TDI.SYS             fa950000 2bd5a7fb - nbf.sys
fa980000 2bd72406 - streams.sys         fa9b0000 2bd4975f - ubnb.sys
fa9c0000 2bd5bfd7 - usbser.sys          fa9d0000 2bd4971d - netbios.sys
fa9e0000 2bd49678 - Parallel.sys        fa9f0000 2bd4969f - serial.SYS
faa00000 2bd49739 - mup.sys             faa40000 2bd4971f - SMBTRSUP.SYS
faa10000 2bd6f2a2 - srv.sys             faa50000 2bd4971a - afd.sys
faa60000 2bd6fd80 - rdr.sys             faaa0000 2bd49735 - bowser.sys

Address dword dump Dll Base                                      - Name
801afc20 80106fc0 80106fc0 00000000 00000000 80149905 : fa840000 - i8042prt.SYS
801afc24 80149905 80149905 ff8e6b8c 80129c2c ff8e6b94 : 8025c000 - SCSIPORT.SYS
801afc2c 80129c2c 80129c2c ff8e6b94 00000000 ff8e6b94 : 80100000 - ntoskrnl.exe
801afc34 801240f2 80124f02 ff8e6df4 ff8e6f60 ff8e6c58 : 80100000 - ntoskrnl.exe
801afc54 80124f16 80124f16 ff8e6f60 ff8e6c3c 8015ac7e : 80100000 - ntoskrnl.exe
801afc64 8015ac7e 8015ac7e ff8e6df4 ff8e6f60 ff8e6c58 : 80100000 - ntoskrnl.exe
801afc70 80129bda 80129bda 00000000 80088000 80106fc0 : 80100000 - ntoskrnl.exe

Kernel Debugger Using: COM2 (Port 0x2f8, Baud Rate 19200)
Restart and set the recovery options in the system control panel
or the /CRASHDEBUG system start option. If this message reappears,
contact your system administrator or technical support group.
```

Feature Selection

```
EPROCESS
   +0x000 Pcb                    : _KPROCESS
   +0x078 ExitTime               : _LARGE_INTEGER
   +0x080 RundownProtect         : _EX_RUNDOWN_REF
   +0x084 UniqueProcessId        : Ptr32 Void
   +0x088 ActiveProcessLinks     : _LIST_ENTRY
   +0x090 QuotaUsage             : [3] Uint4B
   +0x0c4 ObjectTable            : Ptr32 _HANDLE_TABLE
   +0x0c8 Token                  : _EX_FAST_REF
   +0x0cc WorkingSetLock         : _FAST_MUTEX
   +0x0ec WorkingSetPage         : Uint4B
   +0x0f0 AddressCreationLock    : _FAST_MUTEX
   +0x110 HyperSpaceLock         : Uint4B
   +0x114 ForkInProgress         : Ptr32 _ETHREAD
   +0x118 HardwareTrigger        : Uint4B
   +0x11c VadRoot                : Ptr32 Void
   +0x120 VadHint                : Ptr32 Void
   +0x12c NumberOfLockedPages    : Uint4B
   +0x130 Win32Process           : Ptr32 Void
   +0x134 Job                    : Ptr32 _EJOB
   +0x140 QuotaBlock             : Ptr32 _EPROCESS_QUOTA_BLOCK
   +0x144 WorkingSetWatch        : Ptr32 _PAGEFAULT_HISTORY
   +0x148 Win32WindowStation     : Ptr32 Void
   +0x154 VadFreeHint            : Ptr32 Void
```

Feature Selection

```
EPROCESS
   +0x000 Pcb                      : _KPROCESS
   +0x078 ExitTime                 : _LARGE_INTEGER
   +0x080 RundownProtect           : _EX_RUNDOWN_REF
   +0x084 UniqueProcessId          : Ptr32 Void
   +0x088 ActiveProcessLinks       : _LIST_ENTRY
   +0x090 QuotaUsage               : [3] Uint4B
   +0x0c4 ObjectTable              : Ptr32 _HANDLE_TABLE
   +0x0c8 Token                    : _EX_FAST_REF
   +0x0cc WorkingSetLock           : _FAST_MUTEX
   +0x0ec WorkingSetPage           : Uint4B
   +0x0f0 AddressCreationLock      : _FAST_MUTEX
   +0x110 HyperSpaceLock           : Uint4B
   +0x114 ForkInProgress           : Ptr32 _ETHREAD
   +0x118 HardwareTrigger          : Uint4B
   +0x11c VadRoot                  : Ptr32 Void
   +0x120 VadHint                  : Ptr32 Void
   +0x12c NumberOfLockedPages      : Uint4B
   +0x130 Win32Process             : Ptr32 Void
   +0x134 Job                      : Ptr32 _EJOB
   +0x140 QuotaBlock               : Ptr32 _EPROCESS_QUOTA_BLOCK
   +0x144 WorkingSetWatch          : Ptr32 _PAGEFAULT_HISTORY
   +0x148 Win32WindowStation       : Ptr32 Void
   +0x154 VadFreeHint              : Ptr32 Void
```

Feature Selection

```
EPROCESS
   +0x000 Pcb                      : _KPROCESS
   +0x078 ExitTime                 : _LARGE_INTEGER
   +0x080 RundownProtect           : _EX_RUNDOWN_REF
   +0x084 UniqueProcessId          : Ptr32 Void
   +0x088 ActiveProcessLinks       : _LIST_ENTRY
   +0x090 QuotaUsage               : [3] Uint4B
   +0x0c4 ObjectTable              : Ptr32 _HANDLE_TABLE
   +0x0c8 Token                    : _EX_FAST_REF
   +0x0cc WorkingSetLock           : _FAST_MUTEX
   +0x0ec WorkingSetPage           : Uint4B
   +0x0f0 AddressCreationLock      : _FAST_MUTEX
   +0x110 HyperSpaceLock           : Uint4B
   +0x114 ForkInProgress           : Ptr32 _ETHREAD
   +0x118 HardwareTrigger          : Uint4B
   +0x11c VadRoot                  : Ptr32 Void
   +0x120 VadHint                  : Ptr32 Void
   +0x12c NumberOfLockedPages      : Uint4B
   +0x130 Win32Process             : Ptr32 Void
   +0x134 Job                      : Ptr32 _EJOB
   +0x140 QuotaBlock               : Ptr32 _EPROCESS_QUOTA_BLOCK
   +0x144 WorkingSetWatch          : Ptr32 _PAGEFAULT_HISTORY
   +0x148 Win32WindowStation       : Ptr32 Void
   +0x154 VadFreeHint              : Ptr32 Void
```

Feature Selection

```
EPROCESS
   +0x000 Pcb                      : _KPROCESS
   +0x078 ExitTime                 : _LARGE_INTEGER
   +0x080 RundownProtect           : _EX_RUNDOWN_REF
   +0x084 UniqueProcessId          : Ptr32 Void
   +0x088 ActiveProcessLinks       : _LIST_ENTRY
   +0x090 QuotaUsage               : [3] Uint4B
   +0x0c4 ObjectTable              : Ptr32 _HANDLE_TABLE
   +0x0c8 Token                    : _EX_FAST_REF
   +0x0cc WorkingSetLock           : _FAST_MUTEX
   +0x0ec WorkingSetPage           : Uint4B
   +0x0f0 AddressCreationLock      : _FAST_MUTEX
   +0x110 HyperSpaceLock           : Uint4B
   +0x114 ForkInProgress           : Ptr32 _ETHREAD
   +0x118 HardwareTrigger          : Uint4B
   +0x11c VadRoot                  : Ptr32 Void
   +0x120 VadHint                  : Ptr32 Void
   +0x12c NumberOfLockedPages      : Uint4B
   +0x130 Win32Process             : Ptr32 Void
   +0x134 Job                      : Ptr32 _EJOB
   +0x140 QuotaBlock               : Ptr32 _EPROCESS_QUOTA_BLOCK
   +0x144 WorkingSetWatch          : Ptr32 _PAGEFAULT_HISTORY
   +0x148 Win32WindowStation       : Ptr32 Void
   +0x154 VadFreeHint              : Ptr32 Void
```

Feature Selection

```
EPROCESS
   +0x000 Pcb                      : _KPROCESS
   +0x078 ExitTime                 : _LARGE_INTEGER
   +0x080 RundownProtect           : _EX_RUNDOWN_REF
   +0x084 UniqueProcessId          : Ptr32 Void
   +0x088 ActiveProcessLinks       : _LIST_ENTRY
   +0x090 QuotaUsage               : [3] Uint4B
   +0x0c4 ObjectTable              : Ptr32 _HANDLE_TABLE
   +0x0c8 Token                    : _EX_FAST_REF
   +0x0cc WorkingSetLock           : _FAST_MUTEX
   +0x0ec WorkingSetPage           : Uint4B
   +0x0f0 AddressCreationLock      : _FAST_MUTEX
   +0x110 HyperSpaceLock           : Uint4B
   +0x114 ForkInProgress           : Ptr32 _ETHREAD
   +0x118 HardwareTrigger          : Uint4B
   +0x11c VadRoot                  : Ptr32 Void
   +0x120 VadHint                  : Ptr32 Void
   +0x12c NumberOfLockedPages      : Uint4B
   +0x130 Win32Process             : Ptr32 Void
   +0x134 Job                      : Ptr32 _EJOB
   +0x140 QuotaBlock               : Ptr32 _EPROCESS_QUOTA_BLOCK
   +0x144 WorkingSetWatch          : Ptr32 _PAGEFAULT_HISTORY
   +0x148 Win32WindowStation       : Ptr32 Void
   +0x154 VadFreeHint              : Ptr32 Void
```

Feature Selection

```
EPROCESS
   +0x000 Pcb                      : _KPROCESS
   +0x078 ExitTime                 : _LARGE_INTEGER
   +0x080 RundownProtect           : _EX_RUNDOWN_REF
   +0x084 UniqueProcessId          : Ptr32 Void
   +0x088 ActiveProcessLinks       : _LIST_ENTRY
   +0x090 QuotaUsage               : [3] Uint4B
   +0x0c4 ObjectTable              : Ptr32 _HANDLE_TABLE
   +0x0c8 Token                    : _EX_FAST_REF
   +0x0cc WorkingSetLock           : _FAST_MUTEX
   +0x0ec WorkingSetPage           : Uint4B
   +0x0f0 AddressCreationLock      : _FAST_MUTEX
   +0x110 HyperSpaceLock           : Uint4B
   +0x114 ForkInProgress           : Ptr32 _ETHREAD
   +0x118 HardwareTrigger          : Uint4B
   +0x11c VadRoot                  : Ptr32 Void
   +0x120 VadHint                  : Ptr32 Void
   +0x12c NumberOfLockedPages      : Uint4B
   +0x130 Win32Process             : Ptr32 Void
   +0x134 Job                      : Ptr32 _EJOB
   +0x140 QuotaBlock               : Ptr32 _EPROCESS_QUOTA_BLOCK
   +0x144 WorkingSetWatch          : Ptr32 _PAGEFAULT_HISTORY
   +0x148 Win32WindowStation       : Ptr32 Void
   +0x154 VadFreeHint              : Ptr32 Void
```

Feature Selection

```
EPROCESS
   +0x000 Pcb                      : _KPROCESS
   +0x078 ExitTime                 : _LARGE_INTEGER
   +0x080 RundownProtect           : _EX_RUNDOWN_REF
   +0x084 UniqueProcessId          : Ptr32 Void
   +0x088 ActiveProcessLinks       : _LIST_ENTRY
   +0x090 QuotaUsage               : [3] Uint4B
   +0x0c4 ObjectTable              : Ptr32 _HANDLE_TABLE
   +0x0c8 Token                    : _EX_FAST_REF
   +0x0cc WorkingSetLock           : _FAST_MUTEX
   +0x0ec WorkingSetPage           : Uint4B
   +0x0f0 AddressCreationLock      : _FAST_MUTEX
   +0x110 HyperSpaceLock           : Uint4B
   +0x114 ForkInProgress           : Ptr32 _ETHREAD
   +0x118 HardwareTrigger          : Uint4B
   +0x11c VadRoot                  : Ptr32 Void
   +0x120 VadHint                  : Ptr32 Void
   +0x12c NumberOfLockedPages      : Uint4B
   +0x130 Win32Process             : Ptr32 Void
   +0x134 Job                      : Ptr32 _EJOB
   +0x140 QuotaBlock               : Ptr32 _EPROCESS_QUOTA_BLOCK
   +0x144 WorkingSetWatch          : Ptr32 _PAGEFAULT_HISTORY
   +0x148 Win32WindowStation       : Ptr32 Void
   +0x154 VadFreeHint              : Ptr32 Void
```

Feature Selection

```
EPROCESS
   +0x000 Pcb                      : _KPROCESS
   +0x078 ExitTime                 : _LARGE_INTEGER
   +0x080 RundownProtect           : _EX_RUNDOWN_REF
   +0x084 UniqueProcessId          : Ptr32 Void
   +0x088 ActiveProcessLinks       : _LIST_ENTRY
   +0x090 QuotaUsage               : [3] Uint4B
   +0x0c4 ObjectTable              : Ptr32 _HANDLE_TABLE
   +0x0c8 Token                    : _EX_FAST_REF
   +0x0cc WorkingSetLock           : _FAST_MUTEX
   +0x0ec WorkingSetPage           : Uint4B
   +0x0f0 AddressCreationLock      : _FAST_MUTEX
   +0x110 HyperSpaceLock           : Uint4B
   +0x114 ForkInProgress           : Ptr32 _ETHREAD
   +0x118 HardwareTrigger          : Uint4B
   +0x11c VadRoot                  : Ptr32 Void
   +0x120 VadHint                  : Ptr32 Void
   +0x12c NumberOfLockedPages      : Uint4B
   +0x130 Win32Process             : Ptr32 Void
   +0x134 Job                      : Ptr32 _EJOB
   +0x140 QuotaBlock               : Ptr32 _EPROCESS_QUOTA_BLOCK
   +0x144 WorkingSetWatch          : Ptr32 _PAGEFAULT_HISTORY
   +0x148 Win32WindowStation       : Ptr32 Void
   +0x154 VadFreeHint              : Ptr32 Void
```

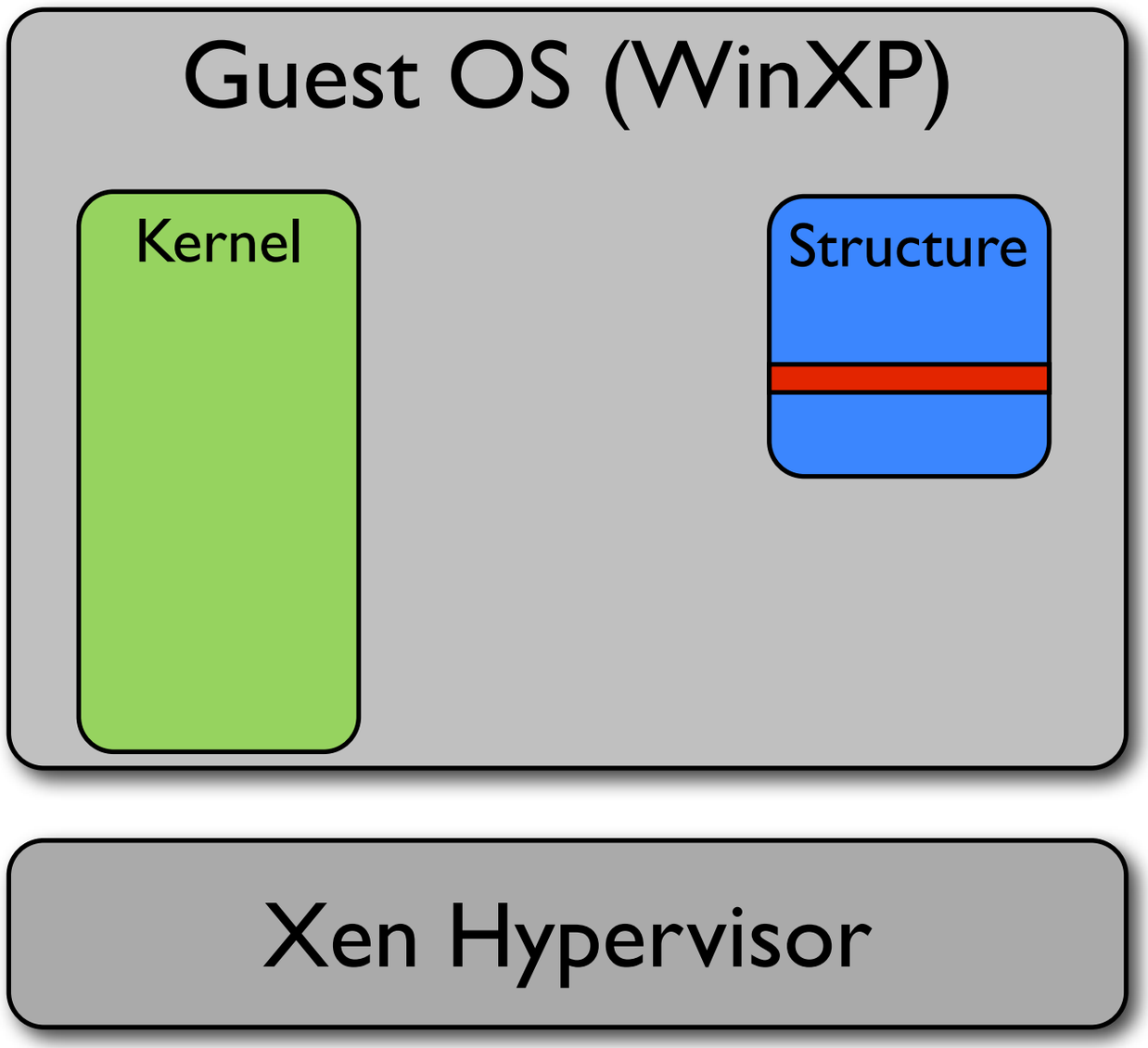
Feature Selection

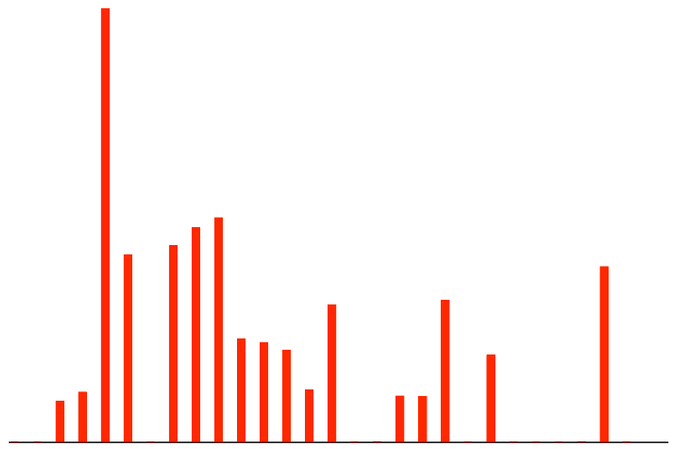
```
EPROCESS
   +0x000 Pcb                    : _KPROCESS
   +0x078 ExitTime               : _LARGE_INTEGER
   +0x080 RundownProtect         : _EX_RUNDOWN_REF
   +0x084 UniqueProcessId        : Ptr32 Void
   +0x088 ActiveProcessLinks     : _LIST_ENTRY
   +0x090 QuotaUsage             : [3] Uint4B
   +0x0c4 ObjectTable            : Ptr32 _HANDLE_TABLE
   +0x0c8 Token                  : _EX_FAST_REF
   +0x0cc WorkingSetLock         : _FAST_MUTEX
   +0x0ec WorkingSetPage         : Uint4B
   +0x0f0 AddressCreationLock    : _FAST_MUTEX
   +0x110 HyperSpaceLock         : Uint4B
   +0x114 ForkInProgress         : Ptr32 _ETHREAD
   +0x118 HardwareTrigger        : Uint4B
   +0x11c VadRoot                : Ptr32 Void
   +0x120 VadHint                : Ptr32 Void
   +0x12c NumberOfLockedPages    : Uint4B
   +0x130 Win32Process           : Ptr32 Void
   +0x134 Job                    : Ptr32 _EJOB
   +0x140 QuotaBlock             : Ptr32 _EPROCESS_QUOTA_BLOCK
   +0x144 WorkingSetWatch        : Ptr32 _PAGEFAULT_HISTORY
   +0x148 Win32WindowStation     : Ptr32 Void
   +0x154 VadFreeHint            : Ptr32 Void
```

Dynamic Profiling

- Idea: watch the structure as OS executes
- If a field is never accessed, attacker can control it
- Monitor OS execution and build histogram of how frequently each field is accessed

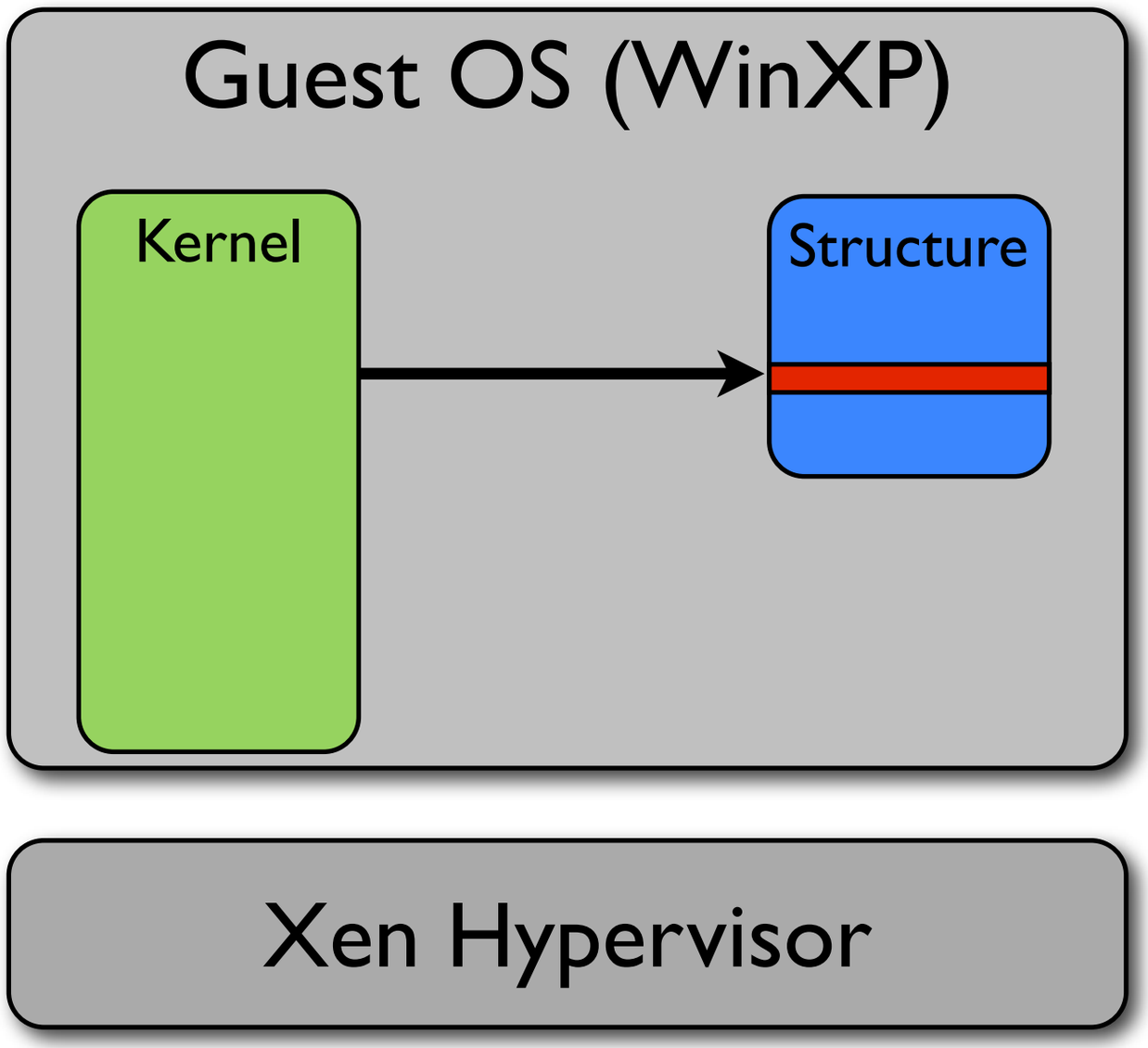
Dynamic Profiling

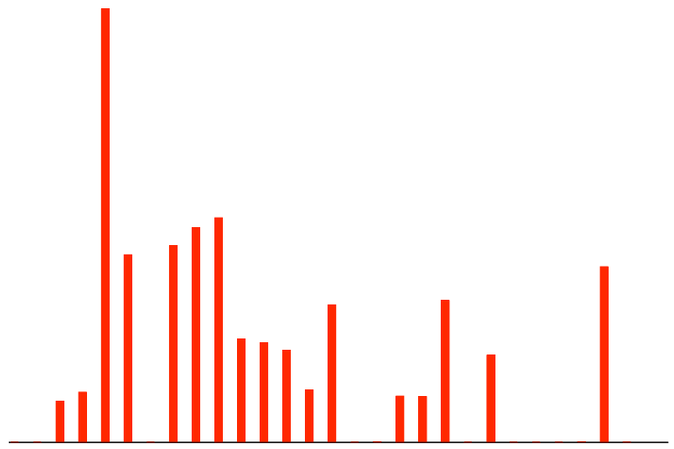




Structure Access Profile

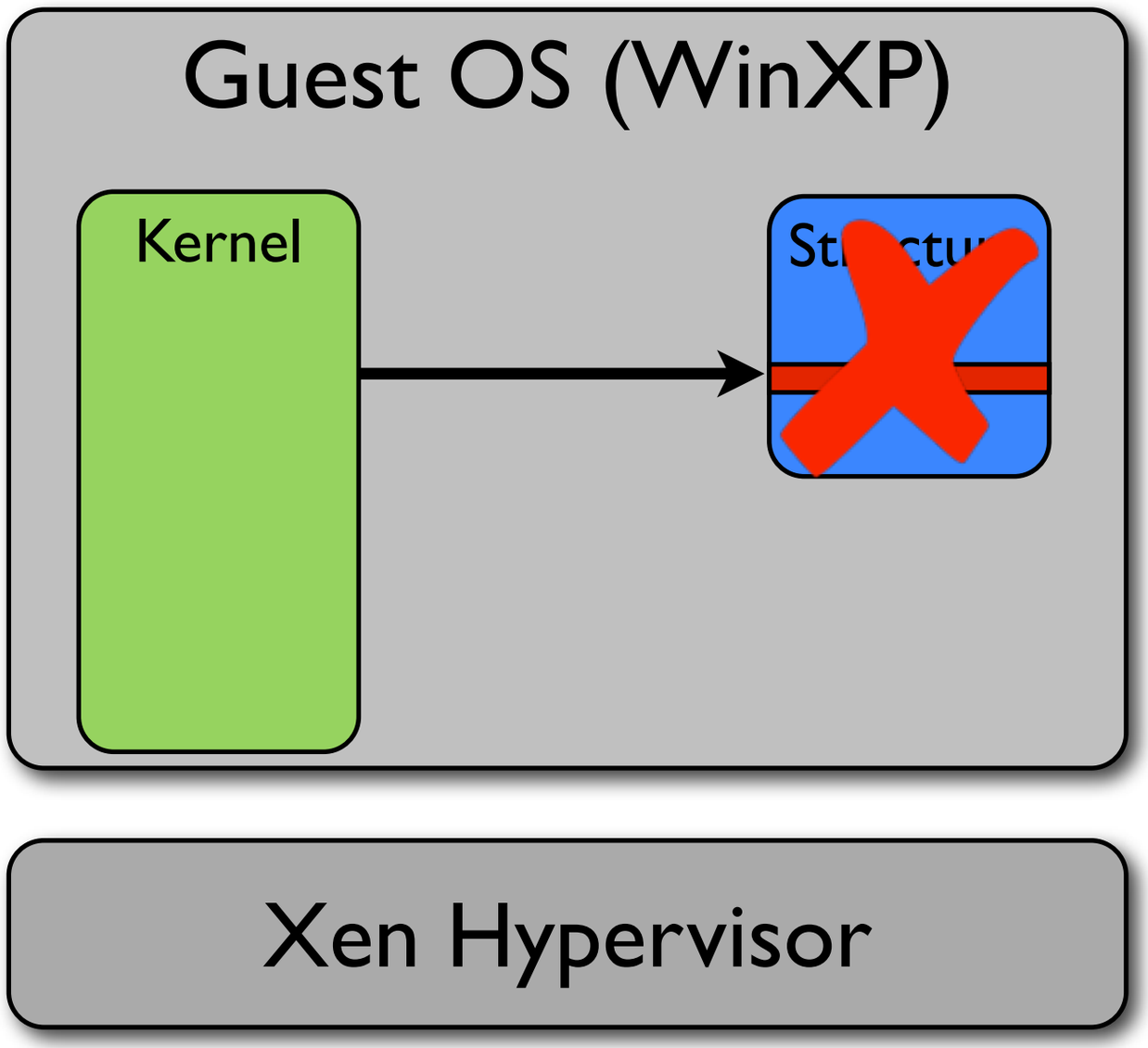
Dynamic Profiling

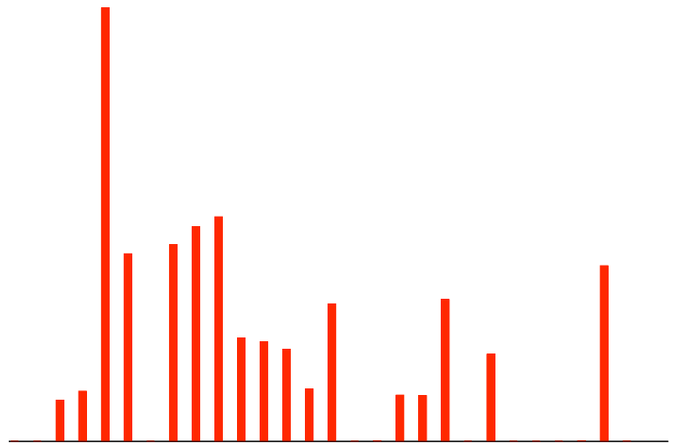




Structure Access Profile

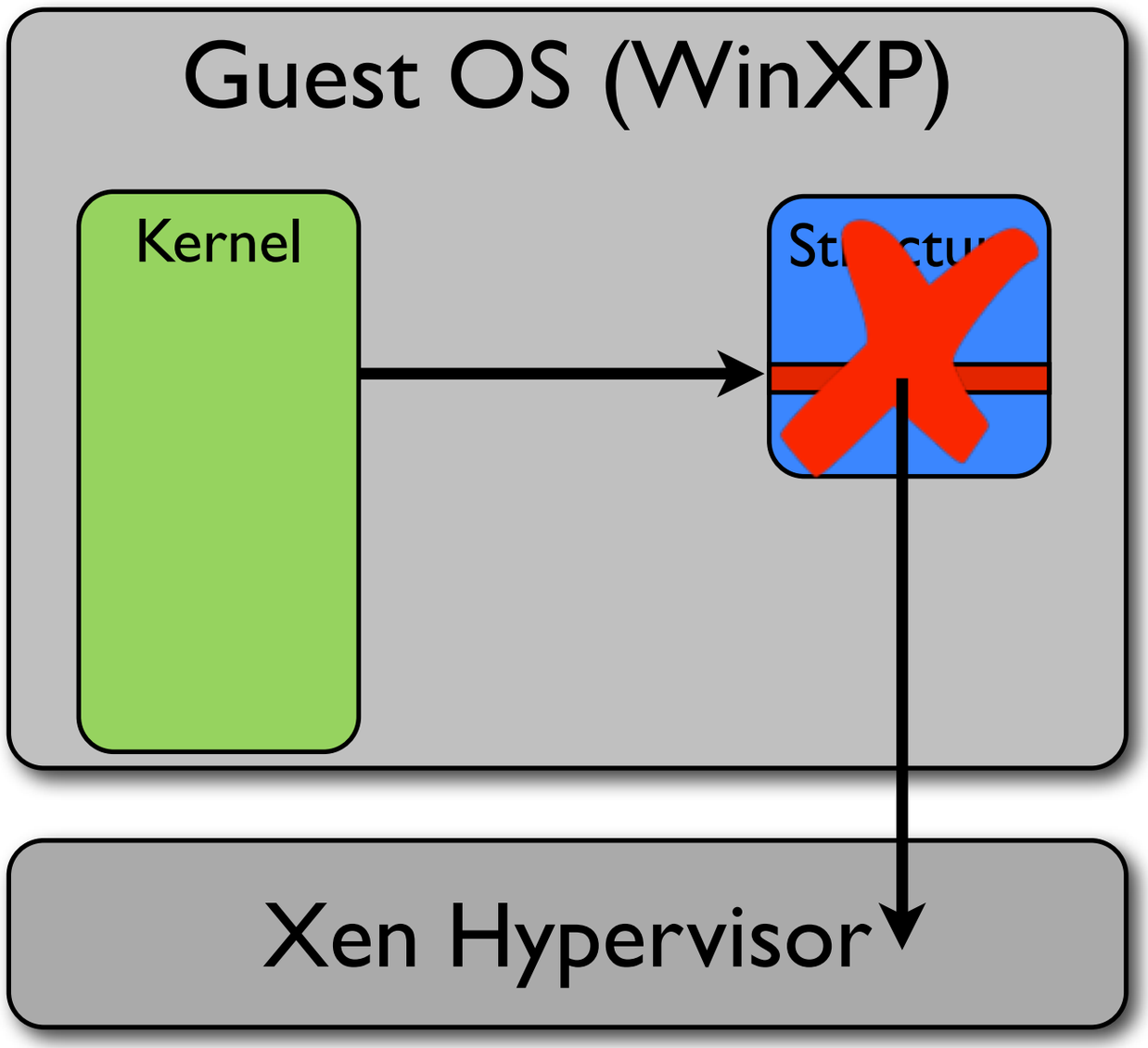
Dynamic Profiling

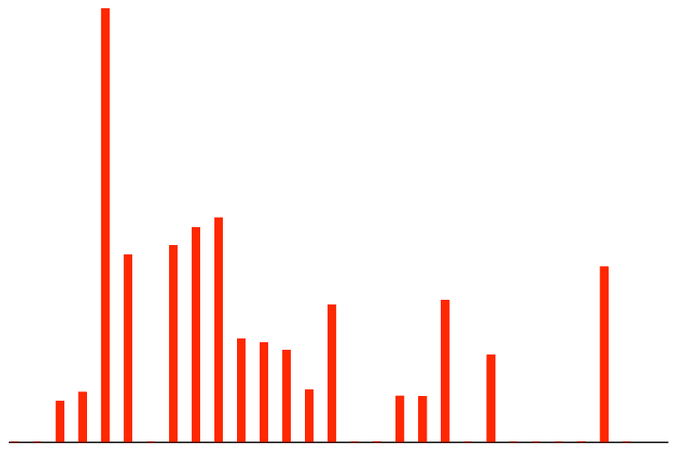




Structure Access Profile

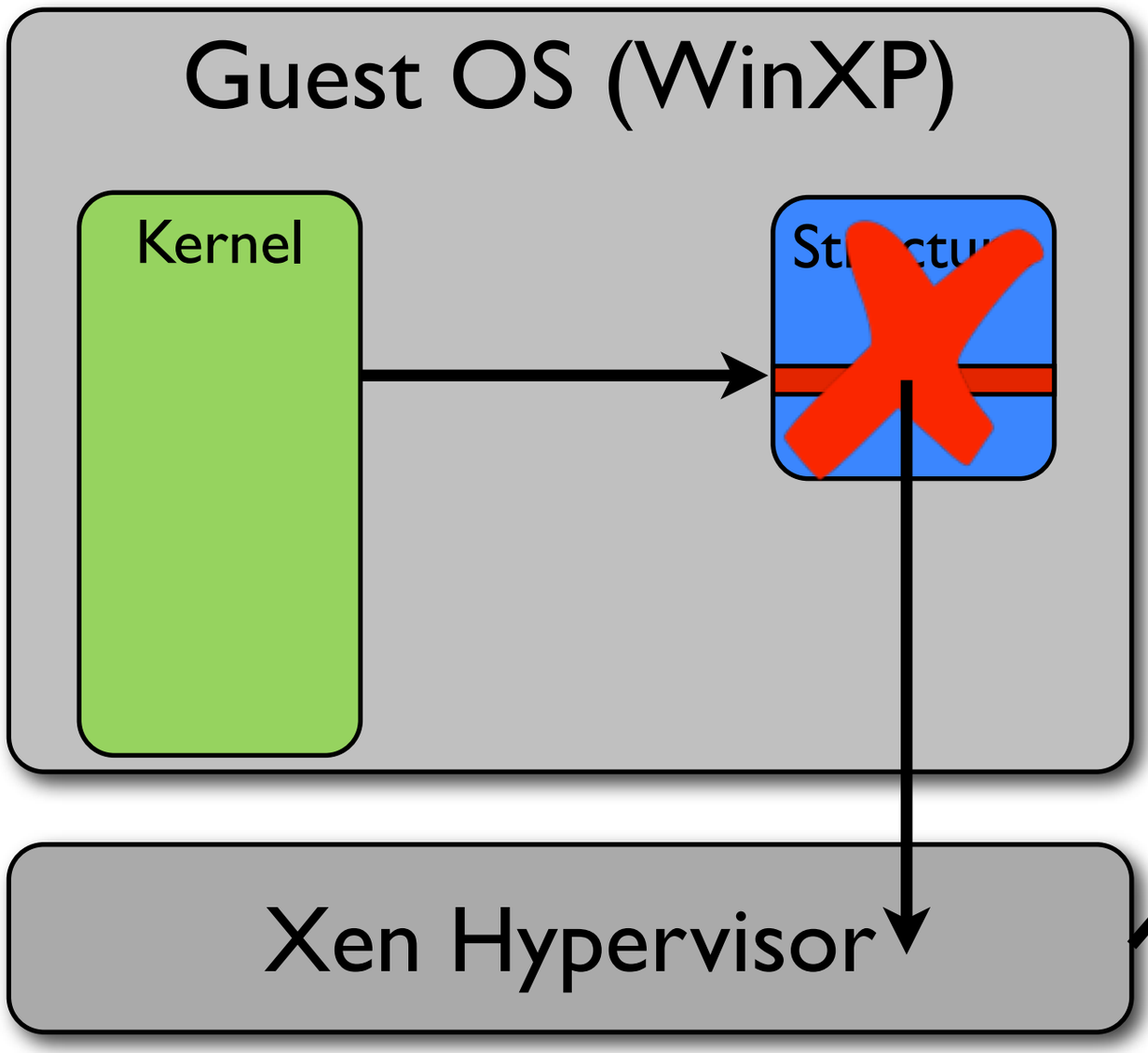
Dynamic Profiling

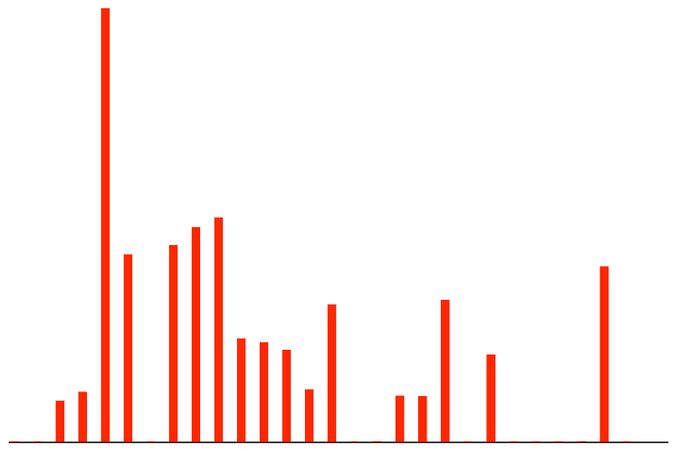




Structure Access Profile

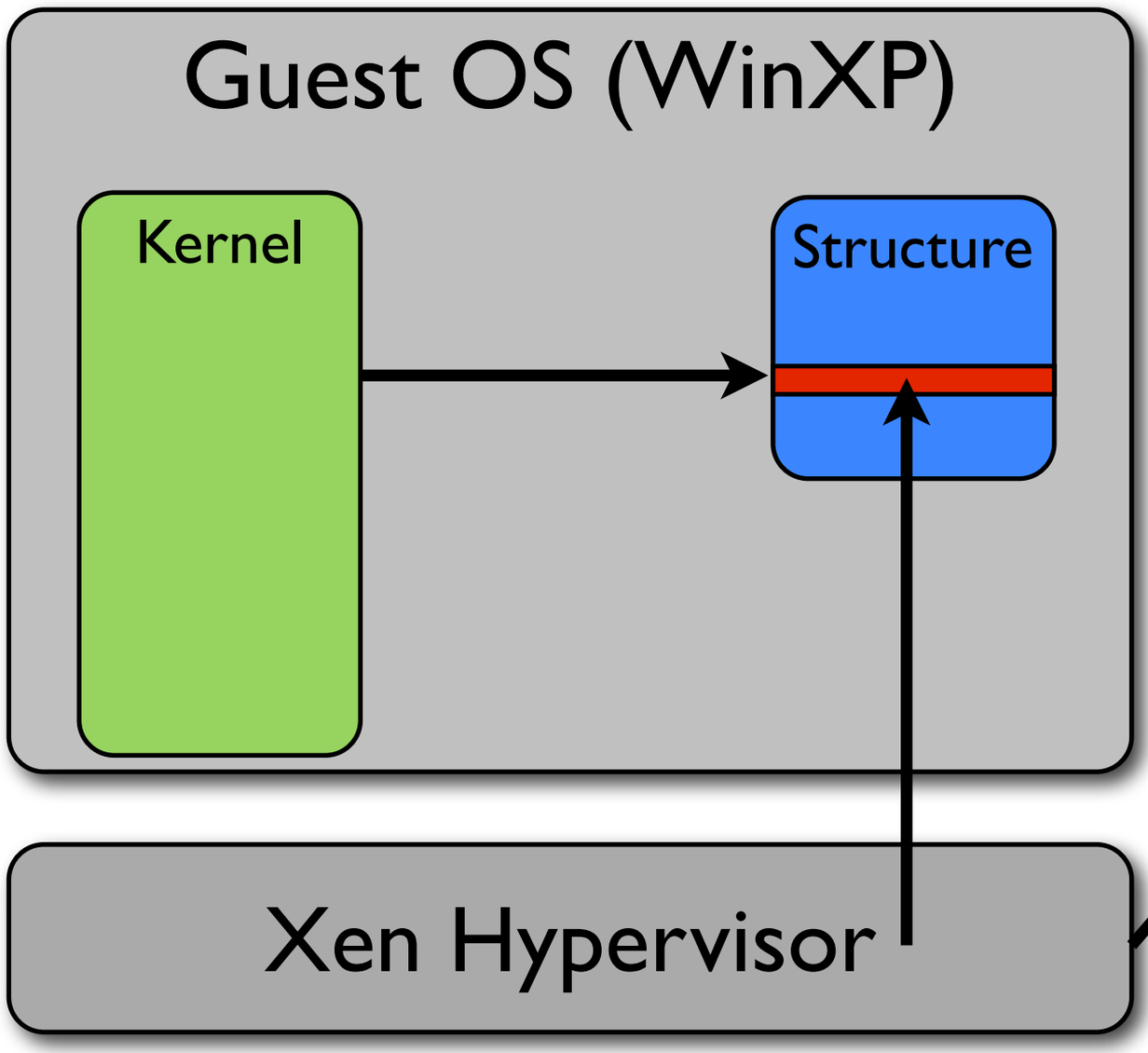
Dynamic Profiling

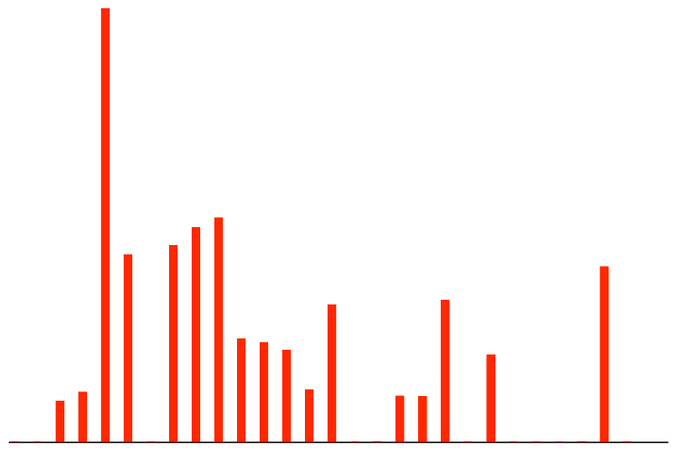




Structure Access Profile

Dynamic Profiling





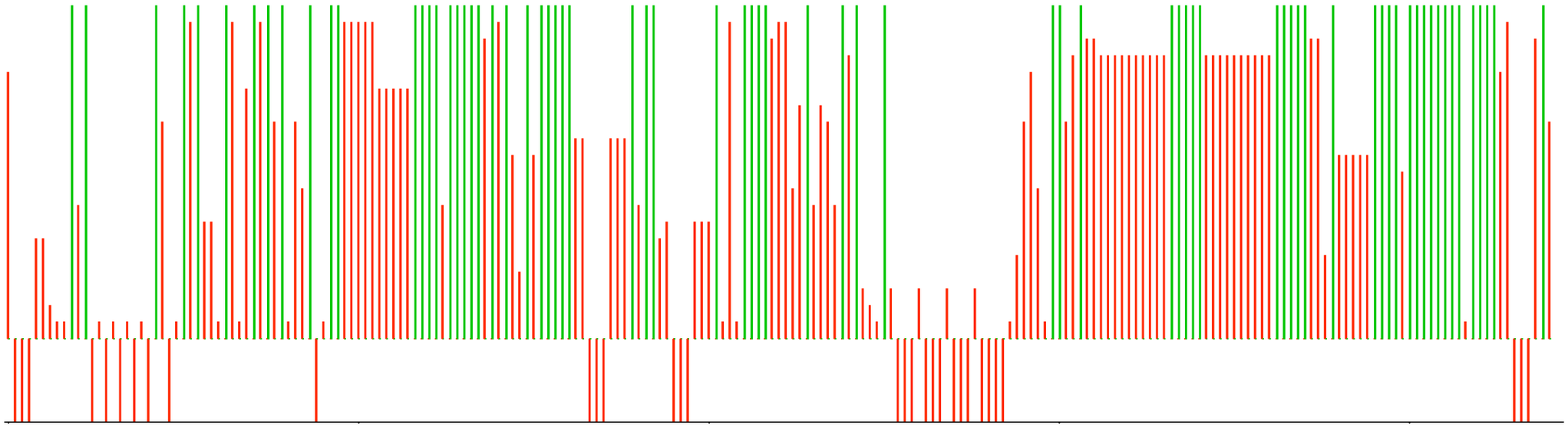
Structure Access Profile

Profiling EPROCESS: Methodology

- Profiled 20 programs. For each:
  1. Find address of EPROCESS using debugger
  2. Log access to data structure
  3. Let each program run for 5 seconds

EPROCESS Profile

Always



Never

Field

Profiling is not Enough

- We don't know if functionality depends on a given member
- Being accessed is a *necessary* condition, but not *sufficient*
- We need to determine if the access is meaningful

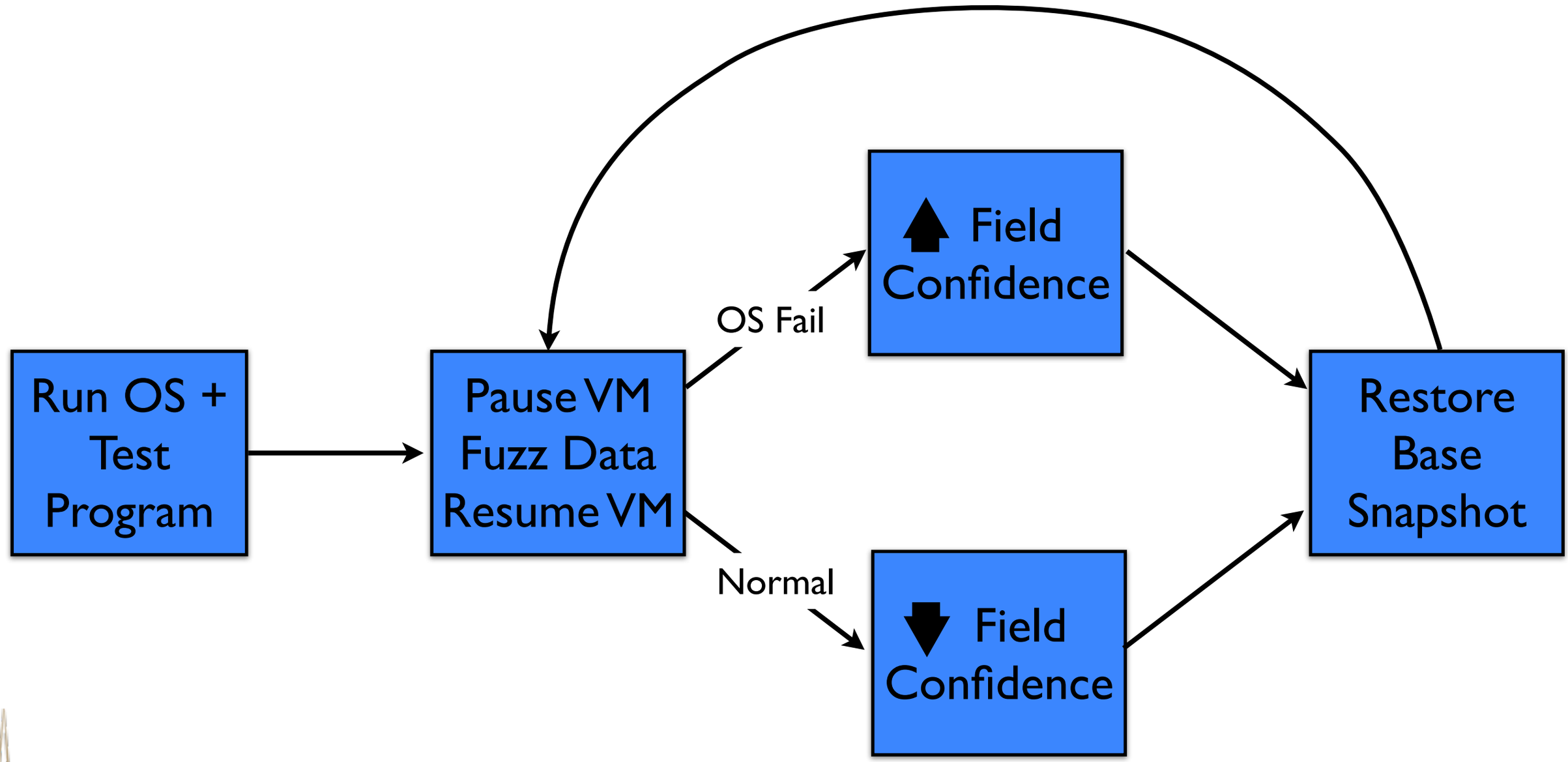
Fuzzing

- Modify field data and see if OS crashes
- If OS consistently crashes, attacker probably can't modify that field
- If we can modify it with impunity, so can an attacker

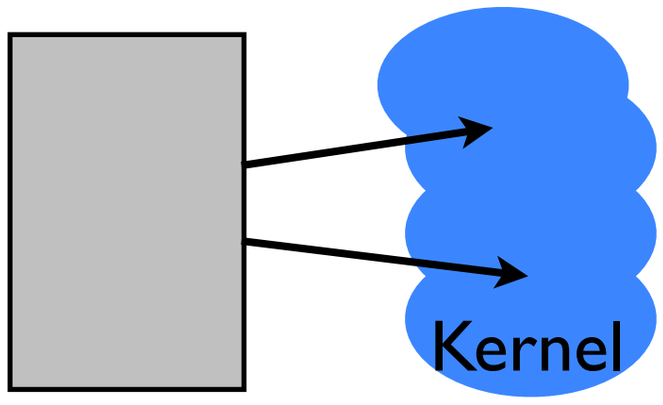
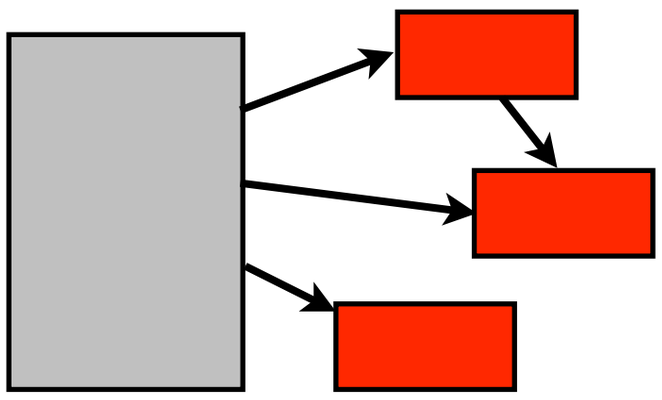
Note: Failure is Good!

- During fuzz testing, *failures* are indications that a feature is robust
- If attackers try to modify these fields, OS instability results
- Good basis for robust signatures

Fuzzing Methodology (1)

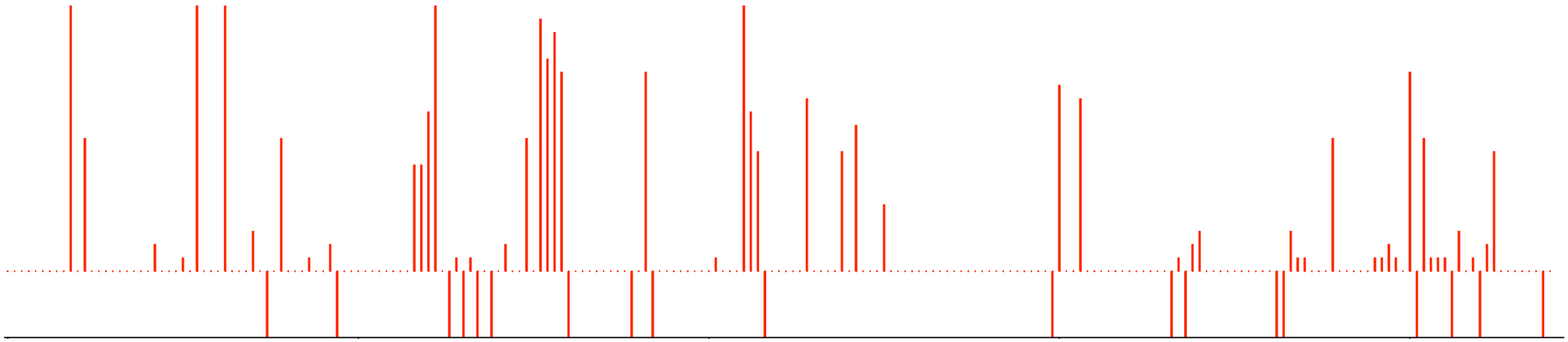


Fuzzing Patterns

Zero	Random
00000000	24601 7669 15151 9272 2 159
	
Random Primitive	Random Aggregate

Fuzzing EPROCESS

Always



Never

Field

Evading Real Signatures

(EPROCESS, PTFinder)

Field	Constraint
Pcb.Header.Type	0x03
Pcb.Header.Size	0x1B
ThreadListHead.Flink	Kernel
ThreadListHead.Blink	Kernel
Pcb.DirectoryTableBase[0]	Aligned
WorkingSetLock.Event.Header.Type	0x01
WorkingSetLock.Event.Header.Size	0x04
AddressCreationLock.Event.Header.Type	0x01
AddressCreationLock.Event.Header.Size	0x04

After Profiling

Field	Constraint
Pcb.Header.Type	0x03
Pcb.Header.Size	0x1B
ThreadListHead.Flink	Kernel
ThreadListHead.Blink	Kernel
Pcb.DirectoryTableBase[0]	Aligned
WorkingSetLock.Event.Header.Type	0x01
WorkingSetLock.Event.Header.Size	0x04
AddressCreationLock.Event.Header.Type	0x01
AddressCreationLock.Event.Header.Size	0x04

After Fuzzing

Field	Constraint
Pcb.Header.Type	0x03
Pcb.Header.Size	0x1B
ThreadListHead.Flink	Kernel
ThreadListHead.Blink	Kernel
Pcb.DirectoryTableBase[0]	Aligned
WorkingSetLock.Event.Header.Type	0x01
WorkingSetLock.Event.Header.Size	0x04
AddressCreationLock.Event.Header.Type	0x01
AddressCreationLock.Event.Header.Size	0x04

Signature Evasion: Takeaway

- Signatures constructed by experts are weak
- Feature selection should be guided by data
- Use information from profiling and fuzzing to generate robust signatures

Signature Generation

- Dynamic invariant detection
- Infer constraints on robust fields
- Check values against invariant templates
  - All values equal some constant?
  - All values aligned?
- Generated constraints on 15 robust fields

Evaluation

- Evaluated new `EPROCESS` signature on real-world memory images
  - Clean: no malicious processes
  - Synthetic attack: custom rootkit running
- In the absence of malware, OS process list serves as ground truth

Synthetic Malware

- Modified version of FU rootkit
- Combines DKOM with signature evasion
- Undetectable by existing scanners
- Does not impair OS stability (tampers with unused fields)

Results

Signature	Image Type	FP	FN
Existing Signatures	Clean		
	Malicious		
Robust Signature	Clean		
	Malicious		

Results

Signature	Image Type	FP	FN
Existing Signatures	Clean	**No**	
	Malicious	**No**	
Robust Signature	Clean	**No**	
	Malicious	**No**	

Results

Signature	Image Type	FP	FN
Existing Signatures	Clean	**No**	**No**
	Malicious	**No**	
Robust Signature	Clean	**No**	**No**
	Malicious	**No**	

Results

Signature	Image Type	FP	FN
Existing Signatures	Clean	**No**	**No**
	Malicious	**No**	**Yes**
Robust Signature	Clean	**No**	**No**
	Malicious	**No**	

Results

Signature	Image Type	FP	FN
Existing Signatures	Clean	**No**	**No**
	Malicious	**No**	**Yes**
Robust Signature	Clean	**No**	**No**
	Malicious	**No**	**No**

Conclusions

- Showed existing signatures weak, vulnerable to evasion
- New systematic method for selecting features for data structure signatures
- Constrains attackers' ability to evade signatures

Questions?

- {brendan,abhinav,traynor,giffin}@cc.gatech.edu
- http://www.cc.gatech.edu/~brendan/

Future Directions

- Smarter profiling: determine whether accessed values affect OS behavior
- Mutation fuzzing: small modifications to existing values
- Iterative fuzzing: repeatedly fuzz with values that break inferred constraints

Robust Signature for EPROCESS

Field	Constraint
Pcb.ReadyListHead.Flink	`val & 0x80000000 == 0x80000000 && val % 0x8 == 0`
Pcb.ThreadListHead.Flink	`val & 0x80000000 == 0x80000000 && val % 0x8 == 0`
WorkingSetLock.Count	`val == 1 && val & 0x1 == 0x1`
Vm.VmWorkingSetList	`val & 0xc0003000 == 0xc0003000 && val % 0x1000 == 0`
VadRoot	`val == 0 || (val & 0x80000000 == 0x80000000 && val % 0x8 == 0)`
Token.Value	`val & 0xe0000000 == 0xe0000000`
AddressCreationLock.Count	`val == 1 && val & 0x1 == 0x1`
VadHint	`val == 0 || (val & 0x80000000 == 0x80000000 && val % 0x8 == 0)`
Token.Object	`val & 0xe0000000 == 0xe0000000`
QuotaBlock	`val & 0x80000000 == 0x80000000 && val % 0x8 == 0`
ObjectTable	`val == 0 || (val & 0xe0000000 == 0xe0000000 && val % 0x8 == 0)`
GrantedAccess	`val & 0x1f07fb == 0x1f07fb`
ActiveProcessLinks.Flink	`val & 0x80000000 == 0x80000000 && val % 0x8 == 0`
Peb	`val == 0 || (val & 0x7ffd0000 == 0x7ffd0000 && val % 0x1000 == 0)`
Pcb.DirectoryTableBase[0]	`val % 0x20 == 0`