Debugging.TV

Frame 0x0D

Presenter: Dmitry Vostokov
Topics

• Spiking Thread pattern
• Manual core dump generation
  ✓ Dump and kill:
    kill -s SIGQUIT <PID>
  ✓ Dump and continue:
    http://osxbook.com/book/bonus/chapter8/core/

• Live thread inspection
Spiking Thread

```c
void * thread_one (void *arg)
{
    while (1) { sleep (1); }
    return 0;
}

void * thread_two (void *arg)
{
    while (1) { sleep (2); }
    return 0;
}

void * thread_three (void *arg)
{
    while (1) { *(double*)arg=sqrt(*(double *)arg); }
    return 0;
}

int main(int argc, const char * argv[])
{
    pthread_t threadID_one, threadID_two, threadID_three;
    double result = 0xffffffff;
    pthread_create (&threadID_one, NULL, thread_one, NULL);
    pthread_create (&threadID_two, NULL, thread_two, NULL);
    pthread_create (&threadID_three, NULL, thread_three, &result);
    pthread_join(threadID_three, NULL);
    return 0;
}
```
Crash Report

Crashed Thread:  0  Dispatch queue: com.apple.main-thread

Exception Type:  EXC_CRASH (SIGQUIT)
Exception Codes: 0x0000000000000000, 0x0000000000000000

Thread 0 Crashed:: Dispatch queue: com.apple.main-thread
0  libsystem_kernel.dylib  0x00007fff8616ee42 __semwait_signal + 10
1  libsystem_c.dylib   0x00007fff8fa7c97e pthread_join + 795
2  SpikingThread  0x0000000107ac1e81 main + 161 (main.c:54)
3  SpikingThread  0x0000000107ac1d64 start + 52

Thread 1:
0  libsystem_kernel.dylib  0x00007fff8616ee42 __semwait_signal + 10
1  libsystem_c.dylib   0x00007fff8fa7cdea nanosleep + 164
2  libsystem_c.dylib   0x00007fff8fa7cc2c sleep + 61
3  SpikingThread  0x0000000107ac1d86 thread_one + 22 (main.c:19)
4  libsystem_c.dylib   0x00007fff8fac68bf _pthread_start + 335
5  libsystem_c.dylib   0x00007fff8fac9b75 thread_start + 13

Thread 2:
0  libsystem_kernel.dylib  0x00007fff8616ee42 __semwait_signal + 10
1  libsystem_c.dylib   0x00007fff8fa7cdea nanosleep + 164
2  libsystem_c.dylib   0x00007fff8fa7cc2c sleep + 61
3  SpikingThread  0x0000000107ac1d86 thread_two + 22 (main.c:29)
4  libsystem_c.dylib   0x00007fff8fac68bf _pthread_start + 335
5  libsystem_c.dylib   0x00007fff8fac9b75 thread_start + 13

Thread 3:
0  libSystem.B.dylib   0x00007fff85b542df sqrt + 15
1  SpikingThread  0x0000000107ac1d9 thread_three + 25 (main.c:38)
2  libsystem_c.dylib   0x00007fff8fac68bf _pthread_start + 335
3  libsystem_c.dylib   0x00007fff8fac9b75 thread_start + 13
GDB Output (live)

(gdb) info threads
(gdb) info threads
4 0x00007fff85b542df in sqrt$fenv_access_off ()
3 0x00007fff8616ee42 in __semwait_signal ()
2 0x00007fff8616ee42 in __semwait_signal ()
• 1 "com.apple.main-thread" 0x00007fff8616ee42 in __semwait_signal ()

(gdb) info thread 4
Thread 4 has current state "WAITING"

    total user time: 18446744072923834312
    total system time: 740808000

(gdb) info thread 3
Thread 3 has current state "WAITING"

    total user time: 816000
    total system time: 3579000

(gdb) info thread 1
Thread 1 has current state "WAITING"

    total user time: 635000
    total system time: 5381000
<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>May 11-14, 2012</td>
<td>Accelerated .NET Memory Dump Analysis</td>
</tr>
<tr>
<td>June 22, 2012</td>
<td>Introduction to Pattern-Driven Software Diagnostics (Free Webinar)</td>
</tr>
<tr>
<td>July 11-16, 2012</td>
<td>Accelerated Windows Memory Dump Analysis</td>
</tr>
<tr>
<td>July 20-23, 2012</td>
<td>Advanced Windows Memory Dump Analysis</td>
</tr>
<tr>
<td>July 25-30, 2012</td>
<td>Accelerated Windows Malware Analysis</td>
</tr>
<tr>
<td>October 12-15, 2012</td>
<td>Accelerated Windows Software Trace Analysis</td>
</tr>
<tr>
<td>October 19-22, 2012</td>
<td>Accelerated Mac OS X Core Dump Analysis</td>
</tr>
</tbody>
</table>
Debugging.TV