



Full credit is given to the above companies including the OS that this PDF file was generated!

Red Hat Enterprise Linux Release 9.2 Manual Pages on 'OPENSSL_instrument_bus2.3oss1' command

\$ man OPENSSL_instrument_bus2.3oss1

OPENSSL_INSTRUMENT_BUS(3oss1) OpenSSL OPENSSL_INSTRUMENT_BUS(3oss1)

NAME

OPENSSL_instrument_bus, OPENSSL_instrument_bus2 - instrument references to memory bus

SYNOPSIS

```
#ifdef OPENSSL_CPUID_OBJ
size_t OPENSSL_instrument_bus(unsigned int *vector, size_t num);
size_t OPENSSL_instrument_bus2(unsigned int *vector, size_t num, size_t max);
#endif
```

DESCRIPTION

It was empirically found that timings of references to primary memory are subject to irregular, apparently non-deterministic variations. The subroutines in question instrument these references for purposes of gathering randomness for random number generator. In order to make it bus-bound a 'flush cache line' instruction is used between probes. In addition probes are added to vector elements in atomic or interlocked manner, which should contribute additional noise on multi-processor systems. This also means that vector[num] should be zeroed upon invocation (if you want to retrieve actual probe values).

OPENSSL_instrument_bus() performs num probes and records the number of oscillator cycles every probe took.

OPENSSL_instrument_bus2() on the other hand accumulates consecutive probes with the same value, i.e. in a way it records duration of

periods when probe values appeared deterministic. The subroutine performs at most max probes in attempt to fill the vector[num], with max value of 0 meaning "as many as it takes."

RETURN VALUES

Return value of 0 indicates that CPU is not capable of performing the benchmark, either because oscillator counter or 'flush cache line' is not available on current platform. For reference, on x86 'flush cache line' was introduced with the SSE2 extensions.

Otherwise number of recorded values is returned.

COPYRIGHT

Copyright 2011-2021 The OpenSSL Project Authors. All Rights Reserved.
Licensed under the Apache License 2.0 (the "License"). You may not use this file except in compliance with the License. You can obtain a copy in the file LICENSE in the source distribution or at <https://www.openssl.org/source/license.html>.

3.0.7 2023-07-13 OPENSSSL_INSTRUMENT_BUS(3ossl)