NAME

random_harvest - gather entropy from the kernel for the entropy device

SYNOPSIS

#include <sys/types.h>
#include <sys/random.h>

void
random_harvest_direct(*void *entropy*, *u_int size*, *enum esource source*);

void
random_harvest_fast(*void *entropy*, *u_int size*, *enum esource source*);

void
random_harvest_queue(*void *entropy*, *u_int size*, *enum esource source*);

DESCRIPTION

The **random_harvest_*** functions are used by device drivers and other kernel processes to pass data that is considered (at least partially) stochastic to the entropy device.

The caller should pass a pointer pointing to the "random" data in *entropy*. The argument *size* contains the number of bytes pointed to. The *source* is chosen from one of the values enumerated in *sys/dev/random.h*. and is used to indicate the source of the entropy.

The **random_harvest_direct**() variant is used for early harvesting before any multitasking is enabled.

The **random_harvest_fast**() variant is used by sources that should not take a performance hit from harvesting, as they are high-rate sources. Some entropy is sacrificed, but the high rate of supply will compensate for this.

The **random_harvest_queue**() variant is used for general harvesting and is the default choice for most entropy sources such as interrupts or console events.

Interrupt harvesting has been in part simplified for the kernel programmer. If a device driver registers an interrupt handler with BUS_SETUP_INTR(9) or bus_setup_intr(9), then it is only necessary to include the INTR_ENTROPY bit in the *flags* argument to have that interrupt source be used for entropy harvesting. This should be done wherever practicable.

SEE ALSO

random(4), BUS_SETUP_INTR(9)

AUTHORS

The FreeBSD random(4) entropy device and supporting documentation was written by Mark R V Murray.