NAME

au_fetch_tok, **au_print_tok**, **au_print_flags_tok**, **au_read_rec -** perform I/O involving an audit record

LIBRARY

Basic Security Module Library (libbsm, -lbsm)

SYNOPSIS

#include <bsm/libbsm.h>

int
au_fetch_tok(*tokenstr_t *tok*, *u_char *buf*, *int len*);

void
au_print_tok(*FILE *outfp*, *tokenstr_t *tok*, *char *del*, *char raw*, *char sfrm*);

void
au_print_flags_tok(*FILE *outfp*, *tokenstr_t *tok*, *char *del*, *int oflags*);

int
au_read_rec(*FILE *fp*, *u_char **buf*);

DESCRIPTION

These interfaces support input and output (I/O) involving audit records, internalizing an audit record from a byte stream, converting a token to either a raw or default string, and reading a single record from a file.

The **au_fetch_tok**() function reads a token from the passed buffer *buf* of length *len* bytes, and returns a pointer to the token via *tok*.

The **au_print_tok**() function prints a string form of the token *tok* to the file output stream *outfp*, either in default mode, or raw mode if *raw* is set non-zero. The delimiter *del* is used when printing. The **au_print_flags_tok**() function is a replacement for **au_print_tok**(). The *oflags* controls how the output should be formatted and is specified by or'ing the following flags:

AU_OFLAG_NONE	Use the default form.
AU_OFLAG_NORESOLVE	Leave user and group IDs in their numeric form.
AU_OFLAG_RAW	Use the raw, numeric form.
AU_OFLAG_SHORT	Use the short form.
AU_OFLAG_XML	Use the XML form.

The flags options AU_OFLAG_SHORT and AU_OFLAG_RAW are exclusive and should not be used together.

The **au_read_rec**() function reads an audit record from the file stream *fp*, and returns an allocated memory buffer containing the record via **buf*, which must be freed by the caller using free(3).

A typical use of these routines might open a file with fopen(3), then read records from the file sequentially by calling **au_read_rec**(). Each record would be broken down into components tokens through sequential calls to **au_fetch_tok**() on the buffer, and then invoking **au_print_flags_tok**() to print each token to an output stream such as stdout. On completion of the processing of each record, a call to free(3) would be used to free the record buffer. Finally, the source stream would be closed by a call to fclose(3).

RETURN VALUES

On success, **au_fetch_tok**() returns 0 while **au_read_rec**() returns the number of bytes read. Both functions return -1 on failure with *errno* set appropriately.

SEE ALSO

free(3), libbsm(3)

HISTORY

The OpenBSM implementation was created by McAfee Research, the security division of McAfee Inc., under contract to Apple Computer, Inc., in 2004. It was subsequently adopted by the TrustedBSD Project as the foundation for the OpenBSM distribution.

The **au_print_flags_tok**() function was added by Stacey Son as a replacement for the **au_print_tok**() so new output formatting flags can be easily added without changing the API. The **au_print_tok**() is obsolete but remains in the API to support legacy code.

AUTHORS

This software was created by Robert Watson, Wayne Salamon, and Suresh Krishnaswamy for McAfee Research, the security research division of McAfee, Inc., under contract to Apple Computer, Inc.

The Basic Security Module (BSM) interface to audit records and audit event stream format were defined by Sun Microsystems.

BUGS

The *errno* variable may not always be properly set in the event of an error.