NAME

audit_submit - general purpose audit record submission

LIBRARY

Basic Security Module Library (libbsm, -lbsm)

SYNOPSIS

#include <bsm/libbsm.h>

int
audit_submit(*short au_event, au_id_t auid, char status, int reterr, const char * restrict format, ...*);

DESCRIPTION

The **audit_submit**() function provides a generic programming interface for audit record submission. This audit record will contain a header, subject token, an optional text token, return token, and a trailer. The header will contain the event class specified by *au_event*. The subject token will be generated based on *auid*. The return token is dependent on the *status* and *reterr* arguments; unlike the argument to au_to_return, *reterr* should be a local rather than BSM error number. Optionally, a text token will be created as a part of this record.

Text token output is under the control of a *format* string that specifies how subsequent arguments (or arguments accessed via the variable-length argument facilities of stdarg(3)) are converted for output. If *format* is NULL, then no text token is created in the audit record.

It should be noted that **audit_submit**() assumes that setaudit(2), or setaudit_addr(2) has already been called. As a direct result, the terminal ID for the subject will be retrieved from the kernel via getaudit(2), or getaudit_addr(2).

RETURN VALUES

If successful, **audit_submit** will return zero. Otherwise a -1 is returned and the global variable *errno* is set to indicate the error.

EXAMPLES

```
#include <bsm/audit.h>
#include <bsm/libbsm.h>
#include <bsm/audit_uevents.h>

#include <stdio.h>
#include <stdarg.h>
#include <errno.h>
```

```
void
audit_bad_su(char *from_login, char *to_login)
{
        struct auditinfo_addr aia;
        struct auditinfo ai;
        au_id_t aid;
        int error;

        error = getaudit_addr(&aia, sizeof(aia));
        if (error < 0 && errno == ENOSYS) {
                error = getaudit(&ai);
                if (error < 0)
                        err(1, "getaudit");
                aid = ai.ai_auid;
        } else if (error < 0)
                err(1, "getaudit_addr");
        else
                aid = aia.ai_auid;
        error = audit_submit(AUE_su, aid, EPERM, 1,
           "bad su from %s to %s", from_login, to_login);
        if (error != 0)
                err(1, "audit_submit");
}
```

Will generate the following audit record:

```
header,94,1,su(1),0,Mon Apr 17 23:23:59 2006, + 271 msec
subject,root,root,wheel,root,wheel,652,652,0,0.0.0.0
text,bad su from from csjp to root
return,failure : Operation not permitted,1
trailer,94
```

SEE ALSO

auditon(2), getaudit(2), libbsm(3), stdarg(3)

HISTORY

The **audit_submit**() function first appeared in OpenBSM version 1.0. OpenBSM 1.0 was introduced in FreeBSD 7.0.

AUTHORS

The **audit_submit**() function was written by Christian S.J. Peron <csjp@FreeBSD.org>.