CONGRUENT SOFTWARE, INC.
3998 Whittle Avenue
Oakland, CA 94602
(510) 531-5472
(510) 531-2942 FAX

FROM: Peter Johansson

TO: T10 Plenary

DATE: October 7, 1997

RE: Proposed SBP-2 Annex for Security

As a consequence of the directions agreed in the joint disk boys, SBP-2 and SCSI meeting Wednesday, September 10, in Nashua, NH, and further discussed October 7 in Irvine, CA, the T10 SBP-2 *ad hoc* working group recommends to the plenary that a security model be added to SBP-2 as an optional feature. Most of the model would be contained in a new, normative annex for SBP-2 whose implementation would be optional; one change is required in a stabilized part of the draft.

Stabilized Table 2 in 5.1.4, "Management ORB's," would be modified as shown below:

Table 2 – Management request functions

Value	Management function
0	LOGIN
1	QUERY LOGINS
2	CREATE STREAM
3	RECONNECT
4	SET PASSWORD
5 – 6	Reserved for future standardization
7	LOGOUT
8 – 9	Reserved for future standardization
A_{16}	TERMINATE TASK
B_{16}	ABORT TASK
C_{16}	ABORT TASK SET
D_{16}	CLEAR TASK SET
E_{16}	LOGICAL UNIT RESET
F_{16}	TARGET RESET

The remainder of this document is the proposed normative annex for SBP-2. Although the text that follows is labeled annex X, the editor suggests that it become annex C when added to the draft.

Annex X
(normative)

Security extensions

SBP-2 specifies an access protocol, in section 8, that by itself makes no provisions for security. This annex defines extensions to SBP-2 that may be implemented by targets to provide some measure of security. Targets that implement these security extensions shall conform to all provisions of this annex.

Conformance to this annex does not preclude additional, command set-dependent security facilities.

X.1 Passwords

A target shall implement two passwords:

- The master password, which shall be unchangeable and equal to the target serial number. The target serial number should be in a humanly readable form affixed to the target. The master password shall not be readable *via* the target's Serial Bus interface except by a logged-in initiator; and
- The current password, which shall accommodate 28 bytes of password data and shall be alterable only by the set password function (see X.3).

All password values shall be unchanged by power reset, bus reset or command reset.

The value of the master password shall be obtainable by command set-dependent means.

A target may be manufactured with a current password of all zeros, with the expectation that the user assign a nonzero current password as part of target initialization. If a target is manufactured with a nonzero current password, the target shall be shipped with the current password in a humanly readable form.

X.2 Login

The description of the login protocol below reproduces that specified by section 8 and adds validation of cumulative login attempts and the *password* field from the login request. The target shall implement an internal counter, *login_attempts*, which shall be zeroed upon a power reset or upon a successful login or logout request. The target shall perform the following to process a login request:

a) The target shall reject the login request if *login_attempts* is equal to three;

b) The target shall read the initiator's unique ID, EUI-64, from the bus information block by means of two quadlet read transactions. The *source_ID* from the write transaction used to signal the login ORB to the target's MANAGEMENT_AGENT register shall be used as the *destination_ID* in the quadlet read transactions;

c) The target shall determine whether or not the initiator already owns a login by comparing the EUI-64 just obtained against the *login_owner_EUI_64* for all *login_descriptors*. If the initiator is currently logged-in to the same logical unit, the login request shall be rejected but *login_attempts* shall not be incremented;

d) The target shall validate the password provided by the login request. If *password_length* is zero, the password is eight bytes of immediate data present in the *password* field. Otherwise *password_length* specifies the size of the password addressed by *password*. If password_length is greater than 28 the target shall increment *login_attempts* and reject the login request. When *password_length* is valid,

the password provided is extended to 28 bytes by the addition of least significant bytes of zeros; the result is compared with the target's passwords. If the password provided fails to match either the target's current or master password, the *login_attempts* shall be incremented and the login request shall be rejected;

e) If the *exclusive* bit is set in the login ORB, the target shall reject the login request if there are any active *login_descriptors* for the logical unit but shall not increment *login_attempts*;

f) If an active *login_descriptor* with the *exclusive* attribute exists for the *lun* specified in the login ORB, the target shall reject the login request but shall not increment *login_attempts*; else

g) The target shall determine if a free *login_descriptor* is available. If a *login_descriptor* is free, the initiator's *source_ID* is stored in *login_owner_ID*, the initiator's EUI-64 is stored in *login_owner_EUI_64*, the *lun* from the login ORB is stored in the *login_descriptor*, the *exclusive* variable in the *login_descriptor* is set to the value of the *exclusive* bit from the login ORB and the addresses of the fetch agent(s) are stored in the *login_descriptor*. Lastly the target assigns a unique *login_ID* to this login and stores it in the *login_descriptor*.

If the target is able to satisfy the login request, it shall zero *login_attempts* and return a login response as specified in 5.1.4.1.

X.3 Set password

In order to change a target's current password, an initiator may use a management ORB with the format shown below.

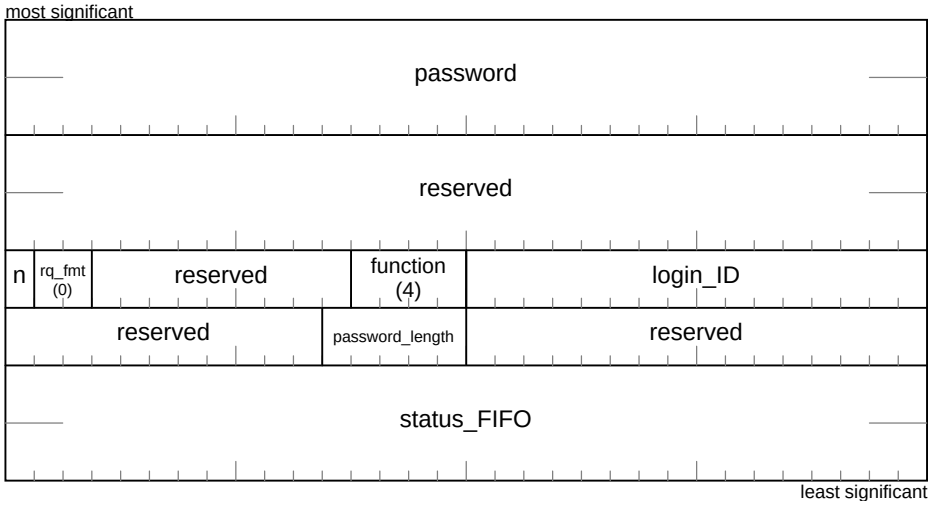

Figure X.1 – Set password ORB

The *password* and *password_length* fields specify the new value for the current password. If *password_length* is zero, the *password* field contains immediate data. When *password_length* is nonzero, the *password* field shall conform to the format for address pointers specified by Figure 11 and shall specify the address of a buffer. The maximum value of *password_length* shall be 28. The buffer shall be in the same node as the initiator and shall be accessible to a Serial Bus block read request with a data transfer length less than or equal to *password_length*.

The *notify* bit and the *rq_fmt* and the *function* fields are as previously defined for management ORB formats.

The *login_ID* field shall specify a login ID value obtained as the result of a successful login.

The *status_FIFO* field shall specify an address allocated for the return of status for the SET PASSWORD request, only. The contents of this field shall not update the status FIFO address established by the successful login that returned *login_ID*.

If *login_ID* specifies a valid current login for the initiator that signaled the SET PASSWORD request to the target's MANAGEMENT_AGENT register, the target shall update the current password to the new value specified by the set password request. The target shall not return completion status for the request unless either the request is rejected or the new password has been successfully stored such that it will not be affected by any subsequent power reset, bus reset or command reset.