Network and Services Integration Forum

NSIF-037-2000

(NSIF Document #NSIF-CA-9910-110R3)

NSIF APPROVED DOCUMENT

WORK GROUP: Security

TITLE: Common Applications Requirements for SONET NE Security System

---

DATE: April 13, 2000

EDITOR: **Name:** Ron Roman
Voice: (732) 758-5631
email: rroman@telcordia.com

ABSTRACT: This is an NSIF approved document that identifies the need for a security server and specifies requirements from users of management systems for the security server function. It is expected that NSIF will specify an implementable solution to these functional requirements in a future NSIF document.

This document has received the approval of the Network Services and Integration Forum (NSIF).

Table of Contents

1. Introduction

This is an NSIF working document that identifies the need for a security server and specifies requirements from users of management systems for the security server function. It is expected that NSIF will specify an implementable solution to these functional requirements in a future NSIF document.

1.1 Problem Statement for Secure SONET NE Access

A major cornerstone for service provider security efforts is accountability and traceability. From a NE access perspective, this means that every user, regardless of their activity, must have a unique login and password for any NE they require access (a user could have the same login and password on every NE they require access). Without careful planning, this could result in the field personnel having to deal with multiple passwords and sometimes multiple logins for multiple technologies, including multiple SONET technologies. This could result in the field personnel having difficulty with SONET NE access security standards while attempting to address the pressing needs of the business in their daily work activities.

SONET service providers will require very comprehensive NE security requirements. The security requirements specified in Section 2 of this document are basically common for most service providers.

1.2 Proposed Solutions

Service providers need to protect their corporate information resources and the information stored, transmitted, and/or processed on those resources. However, these same resources must be accessible by their personnel to help met the needs of the business.

If the security arrangements for NE access are too stringent and/or haphazard, it could interfere with the personnel ability to complete tasks or in worse cases be bypassed in part or whole. Yet, security must be comprehensive enough to protect the assets of the corporation.

1.2.1 Present Mode of Operation (PMO)

Currently the above requirements are expected to be provided by an OS for remote access and directly by the NE for local access. It is anticipated that OSs will continue to meet the need of remote operation center users. However, the need to be able to verify and authenticate every user, both “regular/full-time” and “Tier 1-2/part-time” access, has exceeded the NE’s ability to provide all of the above functions. In other words, for large metro offices with large number of overlapping work forces and multiple operations centers (maintenance, provisioning, Tier 2, etc), each NE must be able to manage several hundred users.

1.2.2 Future Mode of Operation (FMO) Options

To address the above need, there are several possible solutions of which the top three are listed below:

1. Greatly enhance the network element,
2. Develop a password manager or

3. Develop an account manager (or for the purposes of this document a security server).

Option 1 at a minimum involves enhancing the NE to support several hundred users plus keeping track of up to five old passwords (due to password aging). Option 1 is doable for new NEs, however it is expected to be a costly solution for the embedded base, both as a cost to enhance the software/hardware and to actually perform the work.

With a quick analysis, Option 2 appears to be a possible solution. However, it has the same problems as Option 1 in addition to addressing restrictions regarding the handling of passwords.

Option 3 details that any user that requires access to any NE must first be verified and authenticated by the security server. The security server will know all NEs that a user can access and that user's access level for each class of NE. This option will require that the embedded base of SONET NEs will have minimum to no impact to meet all security standards and allow future NEs to provide more features at some lower cost per unit. In addition the cost of security management for a SONET network will be lower due to the ability to manage security from a central location.

1.3 References

1. *Generic Requirements for Network Element/Network System (NE/NS) Security,* GR-815-CORE (November 1997).
2. *Proposed Common Applications Requirements Development for SONET NE Security Server,* SIF-CA-9905-050 (BellSouth Telecommunications).
3. *Proposed Additional Security Requirements to Requirements Defined by Contribution "SIF-CA-9905-050 – Attachment 1",* SIF-CA-9907-083 (Fujitsu Network Communications, Inc.).

2. SONET Security Server Requirements

The requirements specified in this document are categorized into basic security services and functions that include: Identification, Authentication, System Access Control, Resource Access Control, Confidentiality, Data and System Integrity, Accountability and Traceability, and Security Administration:

- **Identification** is the process of recognizing a session requester's unambiguous and auditable identity, such as a user-ID. It is a "name" by which a valid user is recognized by the security server without any ambiguity. The user-ID may not be confidential.
- **Authentication** is the process of verifying the claimed identity of the session requester (e.g., a password check).
- **System Access Control** authorizes establishment of a session (i.e., log-on) and continuation of a session until log-off. System access is allowed only to those users that are identified and authenticated.
- **Resource Access Control** provides the capability of denying access to the NE resources in the absence of proper authorization (e.g., user privilege).
- **Confidentiality** is the property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
- **Data and System Integrity** deals with consistency and reliability issues associated with the system and its data and software resources. It also includes being able to maintain an acceptable level of service if and when a security intrusion occurs.
- **Accountability and Traceability** provides the capability to trace user actions (recording who did what, and when it was done) and to log/alarm all security activity of the system
- **Security Administration** manages the mechanisms that allow an appropriate administrator to control the security of the security server/NE/network, and analyzes all appropriate security data.

2.1 Identification

1. The system shall provide an adequate number of UserIDs. The number of UserIDs provided shall be large enough to ensure that each person using the system can have an individual UserID. All authorized users shall have unique user-IDs for identification purposes to support individual accountability, auditability, and access privilege.
2. The system shall provide the capability to individually identify each person including users, and development, maintenance and support persons.
3. The system and/or software shall require each person to identify themselves with their assigned UserID before allowing any actions or access to be accomplished.
4. There shall be no way to bypass identification mechanisms.
5. The system shall support a UserID containing seven characters.

2.2 Authentication

1. Each user-ID shall be authenticated using a password or other authentication mechanism.
2. There shall be no way to bypass the authentication mechanism. No user-ID shall be allowed unauthenticated system access.[1]
3. Authentication mechanisms and/or data shall be protected from unauthorized access or manipulation.
4. Authentication data, e.g., passwords, shall be one-way encrypted in a system's database. The security system shall not store or retain any clear text password in any location. An occurrence of a clear text password in the memory (e.g., during log-on) shall be overwritten immediately after its use.

2.2.1 Password-Related Requirements

If passwords are used, the system or software shall:

A. Not allow anyone other than the owner of the password to know that password.

B. Allow the holder (user) of a password to change it at least daily.

C. Not allow default passwords.[1]

D. Not allow any password to be null.

E. Not display a password on any entry device or associated printer. Passwords in *clear text* shall not be available (i.e., displayed) to any user, including appropriate administrators.

F. Require a password to be at least six characters in length, and not contain the associated user-ID. The security system shall not prevent a user from choosing (e.g., unknowingly) a password that is already associated with another user-ID. (Otherwise, an existing password may be divulged.).

G. Require a password to contain at least one numeric character.

H. Require a password to contain at least one alphabetic character.

2.2.1.1 Password Aging Requirements

The security system shall enforce password aging (i.e., a password is required to be changed after a specified interval).

A. The password aging interval shall be provisionable between 1 and 90 days with an initial default value of 60 days.

B. A notification shall be provided to users requiring them to change their passwords.

C. Allow an appropriate administrator to adjust the "early warning period" (i.e., how early the user shall be notified before the password expiration).

[1] Under special situations, such as during installation of a new security server or a new generic software in an existing security server, a default user-ID and password may be used temporarily**,** however, the defaults shall be modifiable by an appropriate administrator at any time during the installation processes.

D. Prevent reuse of a password for at least six months, three aging periods, or at least five password changes, whichever is feasible and longer. The interval (or equivalent) during which an *expired* password shall be denied if it is selected again as a *new* password by the same user shall be provisionable.

E. If, after receiving notification that a password has expired, the user does not execute a password change, the system resource will be denied.

F. After a password is assigned to a user, when that user establishes a session for the first time, the security server shall generate a message to the user, instructing the user to change their password.

2.3 System Access Control

1. The security system shall not allow system access to any user unless identified and authenticated. Only authorized users shall be allowed system access.
2. The access control mechanism shall be protected from unauthorized access, modification or destruction.
3. The security server shall perform the entire user authentication procedure even if the user-ID that is entered is not valid.
4. The security server shall provide a mechanism to end a session through a secure log-off procedure.
5. There shall be no way to bypass access control mechanisms. For example, when a subsequent user attempts to log-on, the user shall be required to go through the entire log-on procedure including identification and authentication, and shall not be granted automatic access (i.e., bypassing the log-on procedure) to any process invoked by the previous user.
6. The security system shall terminate a session if the user unplugs from the security system without logging-off.
7. There shall be no mode of entry, for any reason, that is not documented in the material provided with the product.
8. There shall be multiple access control mechanism permission groups.
9. The number of access control mechanism permission groups shall be sufficient to ensure that all persons have access to *only* the data and/or system capabilities necessary to accomplish their jobs. At a minimum, the access control mechanism shall provide one class of permissions for those who administer the system and one or more classes of permissions for those who use the system.
10. It is a requirement that the security system provide a mechanism to include or exclude users based on parameters such as time-of-day, day-of-week, calendar date, and location of entry.

    A. If a user has an active session during which the actual values for these parameters exceed the allowable range, it is an objective that the user be automatically logged-off.

11. Persons using remote, e.g., in-dial, ISDN, wireless or Internet, access shall be individually identified and authenticated by an independent dedicated device such as a network access

controller. The remote authentication process must utilize a dynamic password, such as a *token card*.

12. The ability to authorize or revoke access privileges and grant access to system resources shall be restricted only to appointed system administrators.

2.3.1 Requirements for Handling Incorrect Login Information

The log-on procedure shall exit and end the attempted session if the user-entered information is incorrect.

A. In order to not reveal which part of the user-entered information (user-ID and/or authenticator) is incorrect, the error feedback from the security system after the user authentication procedure has failed, shall provide no information other than "DENY".

B. The default for the specified number of times that the security server log-on procedure shall exit and end the session (due to incorrect user entered information) shall be between two and five (inclusive of both). This number shall be assignable and the initial default value shall be three.

C. When the threshold for incorrect user-entered information has been exceeded, the security server should deny subsequent log-on processes for a specified interval of time on the single use accessible port on the security system where the log-on was attempted. The objective is to interrupt the progress of a mechanized password-cracking algorithm.

    1. The default for the lock-out duration shall not be longer than 60 seconds when the threshold for incorrect user-entered information has been exceeded. (This is because longer delays can be used to temporarily disrupt the service by systematically locking out all single-user accessible ports on the security system.)

    2. The security system shall allow the lock-out duration to be assignable, allowing an appropriate administrator to set durations different from the default setting, including an indefinite lock-out until unlocked by the administrator.

    3. When the threshold for incorrect user-entered information has been exceeded, the security system shall not, as a default arrangement, suspend the associated user-ID. (This is because suspension of user-IDs can be used to systematically disable all user-IDs).

D. The security system shall provide a mechanism to immediately notify (in real time) an appropriate administrator when the threshold for incorrect user-entered information is exceeded. For example, the security system could raise a Security Alarm to notify the administrator of an intrusion attempt.

2.3.2 Requirements for Advisory Warning Messages

After a successful log-on has occurred but before system access is granted, the security server shall provide an advisory warning message regarding unauthorized entry/use and its possible consequences. A warning message is a standard feature for computing environments to explicitly warn intruders and, in certain states, may be a prerequisite for prosecuting them.

A. A copyright notice may be required on the initial entry page for any system or software (where appropriate).

B. The security system shall have the capability to display a warning message of up to 20 lines of 80 characters in length.

    1. As part of delivered software, an appropriate default message shall be provided that warns against unauthorized access or use. As an illustration, the default message may be as follows:

    NOTICE: This is a private computer system. Unauthorized access or use may lead to prosecution.

    2. An appropriate administrator shall have the capability to retrieve and provision the advisory warning banner.

2.3.3 Requirements for Time-Out Feature

The security system shall provide a time-out feature. This implies that, if during a session, there has not been any exchange of messages for a specified period of time, the security system shall lockout the user and re-authenticate the user before accepting subsequent inputs.

A. The default for the time-out interval shall be between 5 and 30 minutes, in 1-minute increments. The initial default value shall be 15 minutes.

B. The duration of the time-out interval (inactivity timer) shall be provisionable in 1-minute increments.

C. During time-out, the security system will refrain from transmitting outputs to the timed-out single-user accessible port.

2.4 Resource Access Control

1. The security server shall not allow *resource access* to any user who has not established a *system access* (i.e., a log-on with identification and authentication). This holds for all users.
2. Subsequent to granting a system access to a user, the security server shall not allow the user to access a resource unless that user-ID has an appropriate privilege to access that resource. Access control mechanisms shall provide a default of *"no capability"* for any ID not defined in the access control mechanism.
3. Assigning passwords to specific actions (e.g., operations-related commands) shall not be used.
4. The security system shall provide adequate granularity to deny a user access to potentially damaging processes and transactions that the user does not have to access to be functional.
5. A user shall be able to retrieve the security parameter settings associated with said user.
6. The security system shall provide a level of granularity such that, for any specified resource controlled by the security server, it shall be possible to grant/deny access rights to a specified user or a group of users.
7. The security system shall provide adequate granularity to deny a user access to data files

and/or tables unless the user is authorized for it.

8. The security system shall allow an administrator to define/delete/retrieve privilege levels for security system resources.

2.5 Confidentiality

1. When directed by the service provider, encryption mechanisms shall be employed to protect critical stored or transmitted data.

2.6 Data and System Integrity

1. Modifications shall be allowed by authorized entities only.
2. The origin of data should be identified and maintained.
3. Error detection and correction protocols should be used.

4.The capability shall be provided to back-up or duplicate system software and data.

2.7 Accountability and Traceability

1. An audit mechanism shall provide sufficient information for an after-the-fact investigation of loss or impropriety.
2. The audit mechanism shall provide end-to-end accountability for all significant events.
3. The audit mechanism shall record who did what, and when it was done.
4. The audit mechanism shall be protected from unauthorized access, modification or destruction.
5. The audit mechanism shall be a security log capable of recording:
   a. Invalid authentication attempts.
   b. Valid logins by administrative, special privileged users.
   c. Unauthorized data or transaction access attempts.
   d. Creation, modification or deletion of system resources.
   e. Action taken by administration or special privileged users.
   f. Other security events specified by the service provider.
6. The audit record shall record the following:
   a. Date and time of the event.
   b. The user-ID associated with the event.
   c. The type of event, i.e., read, update, delete.

d. Name of resources accessed.

e. Success or failure of the event.

2.7.1 Security Log

The security system shall generate a security log that contains information to support after-the-fact investigation of loss or impropriety and appropriate management response. *Audit records (as described above) shall be included in the security log.*

A. The list of events that are specified for logging shall be retrievable by a security administrator.

B. The capability for a security administrator to retrieve selected records from the security log shall be provided.

C. Security log entry of any request or activity that is invoked by a user-ID shall include that user-ID, so it becomes possible to establish user accountability.

D. The security log shall be protected from unauthorized access or destruction. The protection shall be provided by access control based on user privilege.

E. It shall not be possible for any user, including an appropriate administrator, to modify or delete a security log.

F. The security log shall have a circular (or equivalent) recording mechanism (i.e., oldest record overwritten by newest).

G. The security log shall be of sufficient size to maintain records for at least thirty days.

H. The security log and its control mechanisms shall survive system restarts (e.g., via reloading).

I. The security log, by default, shall record each user session.

J. The security log, by default, shall record invalid user authentication attempts (equivalently, alarms/events generated due to invalid authentication attempts).

K. The security log, by default, shall record changes made in the security server security configuration.

L. The security log, by default, shall record changes made in a user's security profiles and attributes.

M. The ability for a security administrator to inhibit the security log from recording specified events shall be provided.

N. The ability for a security administrator to allow the security server to resume recording previously inhibited events in the security log shall be provided.

O. Actual or attempted unencrypted passwords shall not be recorded in the security log.

P. The security log, by default, shall record unauthorized attempts to access resources (for example, data, transactions, and processes) in addition to the events recorded by the security log.

Q. For each recorded event, the record in the security log shall include the associated terminal, port, network address or communication device, in addiction to the information recorded for each event.

R. The encryption for the security log shall not employ the password encryption scheme because the security log needs to be decrypted, while encrypted passwords must be protected from decryption.

2.7.2 Security Notifications

1. The security system shall be capable of generating security alarms and security event messages. The alarms and/or messages shall be triggered by specific events as indicated by the security administrator.
2. The security alarms and/or messages shall display the following information and attributes:

- Date and time stamp
- User-ID
- Port of access or network address
- Type of event or condition
- Any other information that is useful such as resource status, proactive action taken, etc.

3. The list of events that generate a security-related alarm or message shall be retrievable by a security administrator.
4. By default, security alarm messages shall be generated by the following:

- Changes to a user-ID privilege profile
- Unauthorized attempts to access resources
- Repeated log-in failures (3 or more)
- Corrupted or tampered security log.

5. By default security event messages shall be generated by the following:

- User-ID created, deleted, enabled, or disabled
- Password expired
- Temporary password assigned
- Session was terminated by a (security) process
- Port of access enabled or disabled
- User authentication failure
- Improper session terminations
- Normal user authentication
- Normal user session termination

- Creation, deletion, and modification of resources
- User execution of actions or other processes
- Changes made in security profiles and attributes associated with a port of access
- Other provisionable or configurable security changes made.

2.8 Security Administration

1. The security system shall support appropriate administrator functions as "separate" from other user functions.
2. There shall be a mechanism such that the execution of administrator functions can be reserved only for an appropriate administrator (i.e., all other users shall be denied this permission).
3. If the option to enable or disable the administrator's account is an installation or run-time option of an security server, the security system shall not require that the account be enabled or activated for the security processes, features, and administrative mechanisms to be operational.
4. There must be at least one administrator user-ID usable at all times.
5. An appropriate administrator shall be able to create and delete users.
6. An appropriate administrator shall be denied creation of a user-ID that is already in use.
7. An appropriate administrator shall be able to create or modify a password.
8. An appropriate administrator shall be able to provision user privilege settings.
9. When a security server needs to be restarted, default user-IDs and passwords, previously modified by an administrator, shall not revert back to the vendor-delivered default user-IDs and passwords.
10. An administrator shall be able to retrieve default settings for all security parameters.
11. At any given instance of time, the security system shall internally maintain and make accessible the identity of all user-IDs logged-in at that time.
12. An appropriate administrator shall be able to Inhibit and Allow users.
13. An appropriate administrator shall be able to identify all resources available to any specific user along with the associated privileges required to access them.
14. An appropriate administrator shall have the capability to retrieve the list of events that are specified for logging.
15. An appropriate administrator shall have the capability to retrieve selected records from the security log.
16. An administrator shall be able to inhibit the security log from recording specified events.
17. An administrator shall be able to allow the security server to resume recording previously inhibited events in the security log.
18. An administrator shall be able to retrieve the list of events that generate a security-related

alarm or message.