

4.4 Data Security At Data Storage Level

The AFS is planning to upgrade their network and database systems in the near future. We therefore concentrated our efforts to evaluate the data security on these new types of systems. The final destination of data is planned to reside on the Microsoft SQL Server which is installed on a Windows NT server computer. Therefore, data security at Windows NT Server and SQL Server will be discussed.

It is worth mentioning that the AFS currently is using a Novell

3.1X network that only uses login user ID and Password for controlling access to the network. The new Novell 4.1 adds C2 data security measures in addition to the login user ID and Password though we are not aware of any plans to make this upgrade.

The Windows NT Server offers the storage space for the SQL databases. The databases saved at NT servers are protected by four separate security software components; login process, local security authority, security account manager, and security reference monitor. The login process is required by each user and uses security features such as password encryption, password aging, and minimum length restrictions on passwords. The local security authority is to ensure that the end-user has permission to access the system. The security account manager will maintain the user accounts database to keep all of the security information. The security reference monitor will determine if the user has permission to access an object, such as file directory, and perform whatever action the user is attempting. The NT server administrator can setup the user access permissions and restrict some data storage areas for the specific users. NT servers also support the C2 security feature.

The SQL Server provides several levels of security for stored data. At the outermost layer, SQL Server login security is integrated directly with Windows NT security. The SQL security Manager utility will integrate the login security process between Windows NT Server and SQL. SQL Server administrators can also monitor the login successes and failures of users by checking the monitor screen. All messages will be sent to Windows NT event log updating the user login information.

Moreover, SQL Server has a number of facilities for managing data security. Access privileges (select, insert, update, and delete) can be granted and revoked on objects such as tables, rows, columns, and views to users or groups of users.