



Tech Info Library

AOCE: Authentication and Privacy Services Overview (10/93)

Revised: 9/30/93
Security: Everyone

AOCE: Authentication and Privacy Services Overview (10/93)

=====
Article Created: 4 October 1993

TOPIC -----

This article provides an overview of Authentication and Privacy Services of Apple Open Collaborative Environment (AOCE).

DISCUSSION -----

PowerShare provides authentication and privacy features for users in a server-based environment. Through AOCE's two way authentication service, users and applications can be confident that the network entity with whom they are communicating are who they claim to be. The privacy feature of AOCE refers to a new protocol, AppleTalk Secure Data Stream Protocol (ASDSP) which encrypts data traveling across the wire.

Two Way Authentication

Two way authentication means that both sides are authenticated to each other. To illustrate why this is important, imagine a network application which prompts a user for a password. The user enters the password, thereby authenticating the user to the application. However, the application has not been authenticated to the user. It is possible that there is a password-gathering application loose on the network which, by impersonating a legitimate application, gathers user names and passwords. This situation is an example of one way authentication.

Two way authentication means that both parties are authenticated to each other. There is a mechanism by which each side can be assured that the entity with whom they are communicating is who it claims to be.

Authentication vs. Authorization

AppleTalk Secure Data Stream Protocol (ASDSP) only offers authentication services, not authorization. Authentication answers the questions 'Who am I?' and 'Who am I talking to?,' while authorization answers the questions 'Do I have access to this server?' and 'What are my access

privileges?' ASDSP leaves authorization services up to the individual application.

ASDSP

Some customers are concerned about someone tapping into their physical network with a packet analysis tool and gathering confidential information by reading the packets on the network. Before AOCE, there was no way for customers to protect against wire tapping, other than guarding the physical security of their network.

PowerShare offers protection against wire tapping through the use of a new protocol, AppleTalk Secure Data Stream Protocol (ASDSP). ASDSP is a secure version of AppleTalk Data Stream Protocol (ADSP). ASDSP encrypts the packets traveling across the wire. If a wire tapper does tap into the network, the packets gathered will be encrypted.

ASDSP uses RC4 encryption.

Copyright 1993, Apple Computer, Inc.

Tech Info Library Article Number:13531