VMS AUTHENTICATION MODULE

Application and System Access Controls

Provides an added layer of security for protecting mission-critical applications running on OpenVMS.

Features

- Prevents unauthorized users from accessing sensitive data

- Leverages RADIUS or LDAP infrastructure to protect OpenVMS systems and applications

- Provides a strong, reliable alternative to weak password protection

- Integrates seamlessly with any OpenVMS application using the VMS Authentication Module's API

- Works with any LDAP v3 compliant server including Microsoft Active Directory and OpenLDAP

- Application integration and consulting services are available

- SSH single sign-on access using MultiNet, TCPware, or SSH for OpenVMS

BUSINESS CHALLENGE

For over twenty years, the OpenVMS operating system has been a strategic part of enterprise networks because of its well-deserved reputation for security and reliability. Many industries including government, healthcare, finance, and other sectors rely on OpenVMS systems to run mission critical applications that manage sensitive data such as patient records, social security numbers, bank accounts, and other trade secrets. Access to sensitive data and the applications that store this data needs to be restricted to only authorized personnel. Security built on static, clear text passwords has proven easy for hackers to beat. Additional identity verification is an essential component of many organizations' security policy.

SOLUTION OVERVIEW

Process Software's VMS Authentication Module provides an added layer of security for protecting mission critical applications running on OpenVMS. It supports the most commonly deployed authentication methods used by enterprises today which are secure LDAP and RADIUS. It also allows administrators to implement further access restrictions from the VMS User Authorization File (VMS modals system). Any combination of these authentication methods can be implemented.

AUTHENTICATION OPTIONS

Secure LDAP:

Many organizations are employing LDAP as a centralized repository for storing user information because it simplifies administration: additions and changes to permissions are made only once in a directory and are immediately available to all authorized users, directory-enabled applications, systems, and other devices. By keeping the authentication centralized in a directory, a security administrator will always know who is accessing network resources and can define user/group-based policies to control access. The VMS Authentication Module makes use of an LDAP directory through a login request for access. The username, password, and all data can

PROCESS
SOFTWARE

be encrypted via TLS between the OpenVMS system and any LDAP compliant directory server to protect a user's identity from being compromised. To ease administration, the VMS User Authorization File may be synced with the LDAP server password. An administrator can also specify a login request should perform multiple searches on multiple servers.

RADIUS:

Remote Authentication Dial-In User Service (RADIUS) is an industry de facto standard which allows organizations to maintain user profiles in a central database that all remote servers can share. It provides better security, allowing a company to set up a policy that can be applied at a single administered network point. The VMS Authentication Module provides secure login access using a RADIUS server for authentication information. The login password is encrypted using the MD5 algorithm.
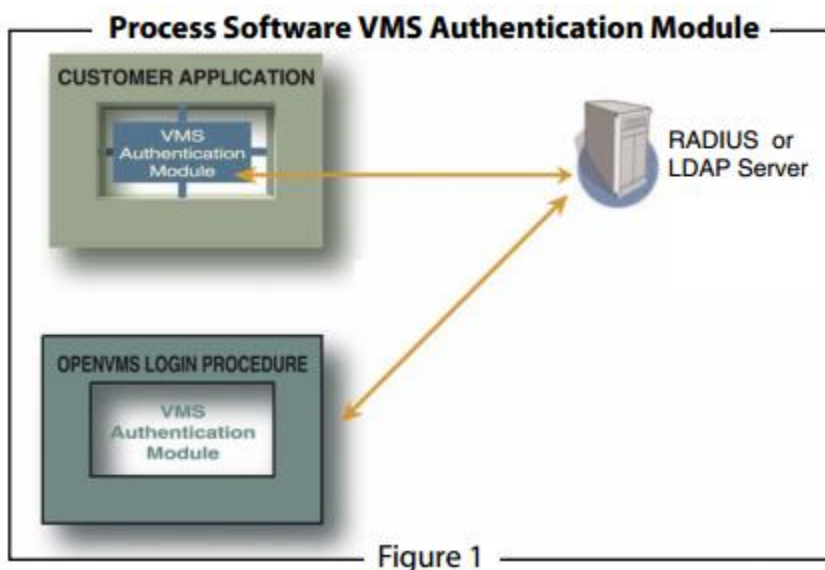
Figure 1

DEPLOYMENT OPTIONS

Process Software's VMS Authentication Module software provides two implementation options (see Figure 1). It can be incorporated into the normal OpenVMS login procedure or used to protect a specific application on the OpenVMS system. Once a user logs into the OpenVMS operating system using normal procedures, access to a specific application is granted with a RADIUS or LDAP login request. The RADIUS or LDAP client can be integrated into third-party applications using the VMS Authentication Module's API.

FREE EVALUATION SOFTWARE!

Please call 800-722-7770 or email sales@process.com to get your free evaluation copy of VMS Authentication Module.

ABOUT PROCESS SOFTWARE
Process Software is a premier supplier of communications software solutions with over 20 years in business. Process Software has grown its customer base to over 3,000 organizations, including Global 2000 and Fortune 1000 companies. Process Software has earned a strong reputation for meeting the stringent reliability and performance requirements of enterprise networks.

PROCESS SOFTWARE'S TECHNICAL SUPPORT PROGRAM
Process Software's Technical Services Program has a well-deserved reputation for excellence. Services include network consulting, training, software maintenance, support, online resources, and 24-hour support. In short, everything you need to keep your mission critical network operating at peak efficiency.

REQUIREMENTS
OpenVMS Alpha 8.2 or higher

OpenVMS Integrity 8.2 or higher

Runs on Process Software's MultiNet or TCPware TCP/IP stacks and TCP/IP Services

Process Software
959 Concord Street
Framingham, MA 01701

Telephone:
U.S./Canada: (800) 722-7770
International: (508) 879-6994
Fax: (508) 879-0042

Web: www.process.com

Email: info@process.com