AUTHENTICATION, AUTHORIZATION, AND ACCOUNTING (AAA) SERVICES SECURITY REQUIREMENTS GUIDE (SRG) TECHNOLOGY OVERVIEW

Version 1, Release 2

24 January 2020

Developed by DISA for the DoD

Trademark Information

Names, products, and services referenced within this document may be the trade names, trademarks, or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our users, and do not constitute or imply endorsement by DISA of any non-Federal entity, event, product, service, or enterprise.

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

1. INTRODUCTION

1.1 Executive Summary

This Authentication, Authorization, and Accounting (AAA) Services Security Requirements Guide (SRG) provides the technical guidance for configuring the AAA Services securely and the framework for vendors to develop product-specific Security Technical Implementation Guides (STIGs).

The guidance includes protocols used for AAA Services interaction, including RADIUS, TACACS+, Kerberos, and other supporting protocols (e.g., LDAPS). The AAA Services SRG includes interaction with directory services, such as the maintenance of user accounts, disablement of inactive accounts, and multifactor authentication (MFA) implementation. This SRG will support risk mitigation for the Network Device Management (NDM) SRG and derived STIGs. However, directory services, policy, and architecture are out of the scope of this AAA Services SRG.

1.1.1 Security Requirements Guides (SRGs)

SRGs are collections of requirements applicable to a given technology family. SRGs represent an intermediate step between Control Correlation Identifiers (CCIs) and STIGs. CCIs represent discrete, measurable, and actionable items sourced from Information Assurance (IA) controls defined in a policy, such as the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53. STIGs provide product-specific information for validating and attaining compliance with requirements defined in the SRG for that product's technology area.

There are four core SRGs: Application, Network, Operating System, and Policy. Each addresses the applicable CCIs in the context of the technology family. Subordinate to the core SRGs, there are Technology SRGs developed to address the technologies at a more granular level.

This AAA Services SRG is based on the Application SRG. This AAA Services SRG contains general check and fix information that can be used for products for which STIGs do not exist.

The STIGs based on this SRG will provide the product-specific technical implementation guidance for that product. The STIG will contain the specific check and fix information for the product it covers.

SRG Hierarchy example:

Application SRG
|__Database SRG
|__MS SQL Server 2005 STIG

The SRG relationship and structure provides the ability to identify requirements that may be considered not applicable for a given technology family and provide appropriate justification. It also provides the structure to identify variations in specific values based on the technology

family. These variations will be captured once and will propagate down to the Technology SRGs and then to the STIGs. This will eliminate the need for each product-specific STIG to address items that are not applicable.

1.1.2 SRG Naming Standards

In an effort to establish consistency across the SRGs, a naming standard for the Group Title and STIGIDs has been established.

Technology SRG Naming Standards

For Technology SRG Group Title and STIGIDs the following applies:

{Core SRG value}-{*Technology SRG*}-{5- or *6-digit numeric sequence number*}

Examples:

SRG-NET-000001-RTR-000001
SRG-APP-000001-COL-000001
SRG-NET-000001-VVSM-00001
SRG-OS-000001-UNIX-000001

Checks/fixes will be included at this level in a general form. These checks and fixes will apply for any STIGs that are created for products that do not have product-specific check and fix guidance.

1.2 Authority

DoD Instruction (DoDI) 8500.01 requires that "all IT that receives, processes, stores, displays, or transmits DoD information will be […] configured […] consistent with applicable DoD cybersecurity policies, standards, and architectures" and tasks that Defense Information Systems Agency (DISA) "develops and maintains control correlation identifiers (CCIs), security requirements guides (SRGs), security technical implementation guides (STIGs), and mobile code risk categories and usage guides that implement and are consistent with DoD cybersecurity policies, standards, architectures, security controls, and validation procedures, with the support of the NSA/CSS, using input from stakeholders, and using automation whenever possible." This document is provided under the authority of DoDI 8500.01.

Although the use of the principles and guidelines in these SRGs/STIGs provides an environment that contributes to the security requirements of DoD systems, applicable NIST SP 800-53 cybersecurity controls need to be applied to all systems and architectures based on the Committee on National Security Systems (CNSS) Instruction (CNSSI) 1253.

1.2.1 Relationship to STIGs

The SRG defines the requirements for various technology families, and the STIGs are the technical implementation guidelines for specific products. A single SRG/STIG is not all-inclusive for a given system, which may include but is not limited to: Database, Web Server, and Domain Name System (DNS) SRGs/STIGs. For a given system, compliance with all (multiple) SRGs/STIGs applicable to a system is required.

1.3 Vulnerability Severity Category Code Definitions

Severity Category Codes (referred to as CAT) are a measure of vulnerabilities used to assess a facility or system security posture. Each security policy specified in this document is assigned a Severity Category Code of CAT I, II, or III.

Table 1-1: Vulnerability Severity Category Code Definitions

	DISA Category Code Guidelines
CAT I	Any vulnerability, the exploitation of which will **directly and immediately** result in loss of Confidentiality, Availability, or Integrity.
CAT II	Any vulnerability, the exploitation of which **has a potential** to result in loss of Confidentiality, Availability, or Integrity.
CAT III	Any vulnerability, the existence of which **degrades measures** to protect against loss of Confidentiality, Availability, or Integrity.

1.4 SRG and STIG Distribution

Parties within the DoD and Federal Government's computing environments can obtain the applicable STIG from the Cyber Exchange website at https://cyber.mil/. This site contains the latest copies of STIGs, SRGs, and other related security information. Those without a Common Access Card (CAC) that has DoD Certificates can obtain the STIG from https://public.cyber.mil/.

1.5 Document Revisions

Comments or proposed revisions to this document should be sent via email to the following address: disa.stig_spt@mail.mil. DISA will coordinate all change requests with the relevant DoD organizations before inclusion in this document. Approved changes will be made in accordance with the DISA maintenance release schedule.

1.6 Other Considerations

DISA accepts no liability for the consequences of applying specific configuration settings made on the basis of the SRGs/STIGs. It must be noted that the configuration settings specified should be evaluated in a local, representative test environment before implementation in a production environment, especially within large user populations. The extensive variety of environments makes it impossible to test these configuration settings for all potential software configurations.

For some production environments, failure to test before implementation may lead to a loss of required functionality. Evaluating the risks and benefits to a system's particular circumstances and requirements is the system owner's responsibility. The evaluated risks resulting from not applying specified configuration settings must be approved by the responsible Authorizing Official. Furthermore, DISA implies no warranty that the application of all specified configurations will make a system 100 percent secure.

Security guidance is provided for the Department of Defense. While other agencies and organizations are free to use it, care must be given to ensure that all applicable security guidance is applied both at the device hardening level as well as the architectural level due to the fact that some of the settings may not be able to be configured in environments outside the DoD architecture.

1.7 Product Approval Disclaimer

The existence of a STIG does not equate to DoD approval for the procurement or use of a product.

STIGs provide configurable operational security guidance for products being used by the DoD. STIGs, along with vendor confidential documentation, also provide a basis for assessing compliance with Cybersecurity controls/control enhancements, which supports system Assessment and Authorization (A&A) under the DoD Risk Management Framework (RMF). DoD Authorizing Officials (AOs) may request available vendor confidential documentation for a product that has a STIG for product evaluation and RMF purposes from disa.stig_spt@mail.mil. This documentation is not published for general access to protect the vendor's proprietary information.

AOs have the purview to determine product use/approval IAW DoD policy and through RMF risk acceptance. Inputs into acquisition or pre-acquisition product selection include such processes as:

- National Information Assurance Partnership (NIAP) evaluation for National Security Systems (NSS) (http://www.niap-ccevs.org/) IAW CNSSP #11
- National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) (http://csrc.nist.gov/groups/STM/cmvp/) IAW Federal/DoD mandated standards
- DoD Unified Capabilities (UC) Approved Products List (APL) (http://www.disa.mil/network-services/ucco) IAW DoDI 8100.04

2. ASSESSMENT CONSIDERATIONS

2.1 NIST SP 800-53 Requirements

All applicable baseline technical NIST SP 800-53 requirements and security best practice requirements are included in this SRG.

CNSSI 1253 defines the required controls for DoD systems based on confidentiality, integrity, and availability (baseline) of the given information system. In all cases, CNSSI 1253, along with required baselines, will serve as the policy requirement for any given asset or information system.

2.2 General Procedures

This SRG has procedures that are intended to provide appropriate evaluation and remediation functions for a typically configured system. These procedures are not product specific and are intended for use when a product-specific STIG is not available.

2.3 Directory Services and Centralized Account Management

When directory services are used for centralized account management of users and devices by connecting to AAA Services, the directory services assume the risks associated with account management. In this configuration, AAA Services do not perform user account management and those requirements are not applicable, as stated in the Check Content field.

3. CONCEPTS AND TERMINOLOGY CONVENTIONS

AAA Services provide a framework for intelligently controlling access to network resources, enforcing policies, auditing usage, and providing the information necessary to bill for services. These combined processes are essential for effective network management and security.

3.1 AAA Functionality

AAA Services provide authentication, authorization, and accounting services.

3.1.1 Authentication

Authentication refers to the process by which an entity's identity is authenticated, typically by providing evidence that it holds a specific digital identity, such as an identifier and the corresponding credentials. Types of credentials include passwords, one-time tokens, digital certificates, digital signatures, and phone numbers (calling/called).

3.1.2 Authorization

The **authorization** function determines whether a particular entity is authorized to perform a given activity, typically inherited from authentication when logging on to an application or service. Authorization may be determined based on a range of restrictions (for example, time-of-day restrictions, physical location restrictions, or restrictions against multiple access by the same entity or user). Typical authorization includes granting read access to a specific file for an authenticated user. Types of service include but are not limited to IP address filtering, address assignment, route assignment, quality of service/differential services, bandwidth control/traffic management, compulsory tunneling to a specific endpoint, and encryption.

3.1.3 Accounting

Accounting refers to the tracking of network resource consumption by users for the purpose of capacity and trend analysis, cost allocation, and billing. In addition, accounting may record events such as authentication and authorization failures as well as audit functionality, verifying that correct procedures were carried out based on accounting data. Information gathered in accounting includes the identity of the user or other entity, the nature of the service delivered, when the service began and when it ended, and if there is a status to report.

3.2 Accounts and Credentials

AAA Services store accounts and credentials for the users being authenticated and authorized and for the service account credentials used to interface with other services. Also, the device or server hosting AAA Services will have an account of last resort, which will also be stored locally. The DoD has mandated that MFA be implemented for all user accounts. However, these user accounts will have passwords associated with them, and these passwords must meet the complexity requirements set forth in this SRG. When MFA is configured, often the password can be randomized, and this is often preferred, but it must meet the minimum complexity standards.

Further, service accounts use passwords, shared secrets, or pre-shared keys, and these must meet the complexity standards. The requirements for password lifetimes, generations, and initial use change do not apply to service account passwords (e.g., shared secrets, pre-shared keys) or the account of last resort.

3.3 Directory Services

A directory service is a shared information infrastructure for locating, managing, administering, and organizing common items and network resources, which can include volumes, folders, files, printers, users, groups, devices, telephone numbers, and other objects. The most commonly implemented directory services are the Microsoft Windows Active Directory (AD) and the X.500 directory service standards.

3.4 AAA Core Components

The core components of AAA Services are described below; each is a logical container of functions and not necessarily dedicated physical devices.

3.4.1 Client

The client is the device attempting to access the network. The client either authenticates itself or acts as a proxy to authenticate the user.

3.4.2 Policy Enforcement Point (Authenticator)

The Policy Enforcement Point (PEP) is sometimes called the authenticator or dial-in server, VPN concentrator, firewall, gateway General Packet Radio Service (GPRS) support node, Ethernet switch, wireless access point, or inline security gateway. The PEP is responsible for enforcing the terms of a client's access.

3.4.3 Policy Information Point

The Policy Information Point (PIP) is a repository of information to help make the access decision. It could be a database of device IDs, a user directory such as the Lightweight Directory Access Protocol (LDAP), a one-time password (OTP) token server, or any other system that houses data relevant to a device or user access request.

3.4.4 Policy Decision Point (AAA Server)

The Policy Decision Point (PDP) is the brain of the AAA Services decision. It collects the access request from the client through the PEP. It also queries any relevant PIPs to gather the information it needs to make the access decision. The PDP, as its name implies, is the entity that makes the final decision around network access. It also can send specific authorizations back to the PEP that apply settings or constraints to the client's network traffic.

3.4.5 Accounting and Reporting System

Whether AAA Services is used on a dedicated system or built as part of a PDP, one of its best features is tracking use of the network with accounting. With all forms of network access now offering controlled access, AAA Services can tell who got on the network, from where, and what that person was granted access to.

3.4.6 Communication Protocols

The most commonly implemented protocols for AAA Services functions are RADIUS, TACACS+, and Kerberos. Often, AAA Services servers use LDAPS to communicate with directory services for user and device management. TACACS+ uses the Transmission Control Protocol (TCP) and RADIUS uses the User Datagram Protocol (UDP) in most implementations. Another significant difference is that RADIUS combines authentication and authorization in a user profile, whereas TACACS+ separates the two operations and can perform authorization to the command line level.