TOE Security Environment

Assumptions

The specific conditions below are assumed to exist in a TOE environment.

A.ModerateExposure
The threat of malicious attacks aimed at discovering and exploiting vulnerabilities is moderate.

A.NoMaliciousUser:
Authorized users and administrators are not malicious unless they attempt to exceed their authorized rights. Authorized users and administrators may make errors.

A.PhysicalAccess
The TOE will be placed in a secure physical location which will prevent unauthorized physical access and modification.

A.PhysicalEnvironment
The TOE will be placed in a physical environment that meets the manufacturer's specifications for temperature, humidity, and other environmental factors. The TOE will be provided with power that meets the manufacturer's specifications.

A.ProtectedCredentials
Authorized users and administrators will protect their login credentials from unauthorized disclosure.

Threats

The threats listed below are addressed by Protection Profile compliant TOE's. The threat agents are either unauthorized persons, unauthorized IT devices, or disgruntled insiders exceeding their authorized use of the TOE. All threat agents are jointly described as an 'attacker' in the threats below.

T.CredentialCracking
An attacker may repeatedly try to guess authentication credentials in order to gain unauthorized access to the TOE.

T.DataAlteration
An attacker may intercept and modify communication sent to or from the TOE in an attempt to force an unauthorized action or affect the integrity of the TOE.

T.DataFlooding
An attacker may send a large volume of data to the TOE to restrict the availability of the TOE. This threat may also be used to attempt to cause the TOE to improperly process data due to limited computing resources.

T.Eavesdropping
An attacker may eavesdrop or sniff communication to or from the TOE thereby compromising the confidentiality of the information outside of the TOE.

T.EscalationOfPrivilege
An attacker who has already gained authorized access to the TOE may attempt to increase its authorization rights by attacking the access control configuration.

T.Hijacking

An attacker may attempt to hijack an existing authorized session to gain the privileges of the user or device in the existing session.

T.MalformedData

An attacker may attempt to compromise the availability or integrity of a TOE by sending malformed data to the TOE. Malformed data is data that does not comply with the expected protocol. It could be values outside of the permitted range, random modifications of the protocol, or data generated using protocol fuzzing tools.

T.Reconnaissance

An attacker may attempt to gather information about the TOE, the TOE configuration, or information in the TOE for use in a future attack or to compromise the confidentiality of the TOE information.

T.Replay

An attacker may record valid communication sent to the TOE and replay all or a portion of the communication to attempt to fool the TOE into performing an unauthorized action or response.

T.Spoofing

An attacker may represent itself as a valid user or device by spoofing the IP address or some other identifying parameter to attempt to compromise the integrity or availability of the TOE or the confidentiality of information in the TOE.

T.StoredDataAttack

An attacker may delete or modify information stored in the TOE to prevent proper operation or to destroy evidence of the attack.

T.SystemIntegrity

An attacker may attempt to replace or destroy application code, configuration parameters or system data in the TOE to compromise the availability or integrity of the TOE.

T.UnauthenticatedAccess

An attacker may bypass the authentication mechanism to attempt to compromise the integrity or availability of the TOE or the confidentiality of information in the TOE.

T.UnauthorizedAction

An attacker that has been authenticated may attempt to perform an unauthorized action by circumventing security in the access control mechanisms.

Organizational Security Policies

Protection Profile compliant TOE's must address the organizational security policies described below.

P.ApprovedCrypto

The TOE shall use FIPS-approved security functions and NIST FIPS validated implementations for all cryptographic functions including key management, hashing, encryption, digital signatures, and random number generation.

P.BackgroundCheck

The organization shall insure that users pass a background check prior to having authorized access to the TOE.

P.Communication The organization shall insure communication to and from the TOE is available.