HydroServer Security and Access Control Design

Jeffery S. Horsburgh, John Cullen, Ketan Patil, David G. Tarboton, Kimberly A. T. Schreuders

8-17-2010

# 1. Introduction

# 2. HydroServer Overview

# 3. Architecture of Security and Access Control System

# 4. Design Diagrams

In the following sections, we describe specific processes that have been identified as requirements in the design for HydroServer security. Each of the processes is described by a sequence diagram formulated to identify the key functional requirements that the systems designed for each process will have to support. These diagrams also show the interaction of the system components and help to define the interfaces and messages transmitted between components.

## 4.1. Administrator Creates User

**Goal:** A HydroServer Administrator creates an account on a HydroServer for a user.

**Summary:** When setting up a HydroServer or at any time, a HydroServer Administrator can create user accounts for any number of users on the server. The HydroServer Administrator logs into an Admin tool that may be either a Windows GUI tool or a web application and supplies a new user’s credentials to create an account.

**Actors:** HydroServer Administrator, Admin Tool, HydroServer User List

**Pre-Conditions:** Setup of HydroServer services and databases complete.

**Triggers:** HydroServer Administrator wants to create a user.

**Post Conditions:** A HydroServer user is created in the users list.

**Notes:**

Figure ??. Sequence diagram for creation of users by a HydroServer Administrator

## 4.2. Client Requests User Creation

**Goal:** A data consumer uses a client application like HydroDesktop to request that a user account be created for them on a HydroServer.

**Summary:** Data consumers will want to establish user accounts on HydroServers so that they can access the data resources hosted on those servers. All user account creation must be approved by a HydroServer Administrator, but client applications can request that a new user account be created for a user on a HydroServer. These requests will be queued for and Administrator to review and approve.

**Actors:** Data Consumer, HydroServer Client (HydroDesktop), HydroServer Security Service, HydroServer User List

**Pre-Conditions:** Setup of HydroServer services and databases complete. The Data Consumer has supplied the client application with his/her profile information.

**Triggers:** Data Consumer requests creation of a user account.

**Post Conditions:** A pending HydroServer user is created in the users list for review by the HydroServer Administrator.

**Notes:**

## 4.3. Administrator Manages User Creation Requests

**Goal:** A HydroServer Administrator reviews a list of requests for user account creation and approves or rejects them.

**Summary:** HydroServer client applications like HydroDesktop can request the creation of a user account on a HydroServer for a particular data consumer. The HydroServer Administrator needs to be able to review the pending user account creation requests and approve or deny them.

**Actors:** HydroServer Administrator, HydroServer Admin Tool, HydroServer Security Service, HydroServer User List

**Pre-Conditions:** A potential user has supplied his/her profile information and has requested that a user account be created for them on a HydroServer.

**Triggers:** HydroServer Administrator wants to review pending user requests.

**Post Conditions:** If the request is approved, a HydroServer user is created in the users list.

**Notes:**

## 4.4. Authenticate User

**Goal:** A HydroServer Administrator creates an account on a HydroServer for a user.

**Summary:** When setting up a HydroServer or at any time, a HydroServer Administrator can create user accounts for any number of users on the server. The HydroServer Administrator logs into an Admin tool that may be either a Windows GUI tool or a web application and supplies a new user’s credentials to create an account.

**Actors:** HydroServer Administrator, Admin Tool, HydroServer User List

**Pre-Conditions:** Setup of HydroServer services and databases complete.

**Triggers:** HydroServer Administrator wants to create a user.

**Post Conditions:** A HydroServer user is created in the users list.

**Notes:**

## 4.5. Administrator Authorizes User

**Goal:** A HydroServer Administrator creates an account on a HydroServer for a user.

**Summary:** When setting up a HydroServer or at any time, a HydroServer Administrator can create user accounts for any number of users on the server. The HydroServer Administrator logs into an Admin tool that may be either a Windows GUI tool or a web application and supplies a new user’s credentials to create an account.

**Actors:** HydroServer Administrator, Admin Tool, HydroServer User List

**Pre-Conditions:** Setup of HydroServer services and databases complete.

**Triggers:** HydroServer Administrator wants to create a user.

**Post Conditions:** A HydroServer user is created in the users list.

**Notes:**

## 4.6. Client Requests Authorization for a User

**Goal:** A HydroServer Administrator creates an account on a HydroServer for a user.

**Summary:** When setting up a HydroServer or at any time, a HydroServer Administrator can create user accounts for any number of users on the server. The HydroServer Administrator logs into an Admin tool that may be either a Windows GUI tool or a web application and supplies a new user’s credentials to create an account.

**Actors:** HydroServer Administrator, Admin Tool, HydroServer User List

**Pre-Conditions:** Setup of HydroServer services and databases complete.

**Triggers:** HydroServer Administrator wants to create a user.

**Post Conditions:** A HydroServer user is created in the users list.

**Notes:**

## 4.7. Administrator Manages Authorization Requests

**Goal:** A HydroServer Administrator creates an account on a HydroServer for a user.

**Summary:** When setting up a HydroServer or at any time, a HydroServer Administrator can create user accounts for any number of users on the server. The HydroServer Administrator logs into an Admin tool that may be either a Windows GUI tool or a web application and supplies a new user’s credentials to create an account.

**Actors:** HydroServer Administrator, Admin Tool, HydroServer User List

**Pre-Conditions:** Setup of HydroServer services and databases complete.

**Triggers:** HydroServer Administrator wants to create a user.

**Post Conditions:** A HydroServer user is created in the users list.

**Notes:**

## 4.8. Client Gets Metadata for a User

**Goal:** A HydroServer Administrator creates an account on a HydroServer for a user.

**Summary:** When setting up a HydroServer or at any time, a HydroServer Administrator can create user accounts for any number of users on the server. The HydroServer Administrator logs into an Admin tool that may be either a Windows GUI tool or a web application and supplies a new user’s credentials to create an account.

**Actors:** HydroServer Administrator, Admin Tool, HydroServer User List

**Pre-Conditions:** Setup of HydroServer services and databases complete.

**Triggers:** HydroServer Administrator wants to create a user.

**Post Conditions:** A HydroServer user is created in the users list.

**Notes:**

## 4.9. Client Gets Data for a User

**Goal:** A HydroServer Administrator creates an account on a HydroServer for a user.

**Summary:** When setting up a HydroServer or at any time, a HydroServer Administrator can create user accounts for any number of users on the server. The HydroServer Administrator logs into an Admin tool that may be either a Windows GUI tool or a web application and supplies a new user’s credentials to create an account.

**Actors:** HydroServer Administrator, Admin Tool, HydroServer User List

**Pre-Conditions:** Setup of HydroServer services and databases complete.

**Triggers:** HydroServer Administrator wants to create a user.

**Post Conditions:** A HydroServer user is created in the users list.

**Notes:**

# 5. Application Programming Interfaces

This section details the Application Programming Interfaces (APIs) that will be exposed by a HydroServer via web services. We do not describe the interfaces that may be used internally within each of the HydroServer components. Figure ?? shows an overview of the HydroServer components and the API methods that can be called for each component.

Figure ??. Overview of HydroServer components and API methods.

## 5.1. Security Service

The HydroServer Security Service provides a mechanism for a user to authenticate themselves with the HydroServer and to request authorization to access specific data resources. It also provides the other HydroServer services with a way to determine whether a user is authorized to perform a particular operation on a data resources.

Table ??. Functions defined in the HydroServer Security Service (HS\_Security).

|  |  |
| --- | --- |
| **Function** | **Parameters** |
| AuthorizeRequest() | (OperationType, ResourceType, ResourceParameters, AuthToken) -> boolean |
| CreateUser() | (UserProfile, AuthToken) -> boolean |
| GetAuthorizationInfo() |  |
| GetResourceInfo() |  |
| GetToken() | (EncryptedCredentials) -> AuthToken |
| GetUsers() |  |
| LogOut() | (AuthToken) -> boolean |
| ModifyUser() |  |
| RequestUserAccount() | (Credentials) -> message |
| RequestAuthorization() | (OperationType, ResourceType, ResourceParameters, AuthToken) -> message |
| SetAccess() |  |
|  |  |

**HS\_Security.AuthorizeRequest**(*OperationType, ResourceType, ResourceParameters, AuthToken*) -> Boolean

This method tests to see if the user identified by the provided token has been authorized for operation on a set of data resources identified by the resource parameters.

**Parameters:** OperationType – the type of operation to be performed, e.g., create, read, update, delete

ResourceType – the type of resource that is to be operated upon, e.g., user, data resource, etc.

ResourceParameters – a string that contains parameters identifying the specific resources that the user wants to operate upon

AuthToken – an encrypted token that identifies the user

**Returns:** True if the user is authorized

**Return Type:** Boolean

**Raises:** Exceptions.TokenDecryptionFailure

Exceptions.NotAuthorized

Exceptions.InvalidToken

Exceptions.InvalidResourceType

Exceptions.InvalidResource

Exceptions.RequestTimeout

Exceptions.InvalidRequest

**HS\_Security.GetToken**(*credentials*) -> AuthToken

This method authenticates a user for interaction with a HydroServer. The returned token is trusted on the HydroServer as a reliable statement of the identity of the authenticated user.

**Parameters:** Credentials (encrypted) – a combination of a user’s email address and password

**Returns:** A composite of the user ID and the authentication token.

**Return Type:** AuthToken (encrypted)

**Raises:** Exceptions.CredentialsDecryptionFailure

Exceptions.InvalidPassword

Exceptions.InvalidCredentials

Exceptions.AuthenticationTimeout

Exceptions.InvalidRequest

## 5.2. WaterOneFlow Web Service

Table ??. Functions defined in the HydroServer WaterOneFlow Service (HS\_WaterOneFlow).

|  |  |
| --- | --- |
| **Function** | **Parameters -> Return** |
| GetSiteInfo() | (SiteCode, AuthToken) -> |
| GetSiteInfoMultipleObject() | (SiteCode(), AuthToken) -> |
| GetSiteInfoObject() | (SiteCode, AuthToken) -> |
| GetSites() | (SiteCode(), AuthToken) -> |
| GetSitesByBoxObject() | (WestLong, SouthLat, EastLong, NorthLat, IncludeSeries, AuthToken) -> |
| GetSitesObject() | (SiteCode(), AuthToken) -> |
| GetValues() | (SiteCode, VariableCode, StartDate, EndDate, AuthToken) -> |
| GetValuesForASiteObject() | (SiteCode, StartDate, EndDate, AuthToken) -> |
| GetValuesObject() | (SiteCode, VariableCode, StartDate, EndDate, AuthToken) -> |
| GetVariableInfo() | (VariableCode, AuthToken) -> |
| GetVariableInfoObject() | (VariableCode, AuthToken) -> |
| GetVariables() | (AuthToken) -> |
| GetVariablesObject() | (AuthToken) -> |
|  |  |
|  |  |

## 5.3. Capabilities Web Service

The HydroServer Capabilities Service is designed to provide information about the services that are hosted on the HydroServer.

Table ??. Functions defined in the HydroServer Capabilities Service (HS\_Capabilities).

|  |  |
| --- | --- |
| **Function** | **Parameters -> Return** |
| GetCapabilities() | () -> CapabilitiesResponse |
| GetMapServices() | () -> |
| GetMapServiceInfo() | (MapServiceID) -> |
| GetRegions() | () -> |
| GetRegionInfo() | (RegionID) -> |
| GetRegionMapServices() | (RegionID) -> |
| GetRegionWaterOneFlowServices() | (RegionID) -> |
| GetWaterOneFlowServices() | () -> |
| GetWaterOneFlowServiceInfo() | (WaterOneFlowServiceID) -> |
|  |  |
|  |  |
|  |  |

## 5.4. State of Health Service

The HydroServer State of Health Service is designed to provide information about the status of a HydroServer and the services that it hosts.

Table ??. Functions defined in the HydroServer Health Service (HS\_Health).

|  |  |
| --- | --- |
| **Function** | **Parameters -> Return** |
| GetMapServiceStatus() | (MapServiceID) -> ServiceStatusResponse |
| GetServerStatus() | () -> ServerStatusResponse |
| GetWaterOneFlowServiceStatus() | (WaterOneFlowServiceID) -> ServiceStatusResponse |
| Ping() | () -> PingResponse |
|  |  |