JEFRi Authentication

April 8, 2012

Contents

1 Overview

JEFRi Authentication is a JEFRi context and series of guidelines for how JEFRi contexts should handle authentication and session control for handling transactions from remote JEFRi instances. Authentication must provide a way for two JEFRi runtimes to establish a known identity and maintain that trust for the duration of a session. Creating a robust protocol for establishing trust between two computing resources is not a trivial undertaking. To sidestep many of those issues, it is recommended that any communication regarding authentication and authenticated sessions be carried out over some protocol that handles network security; either HTTPS for connections over the internet as a whole or IPsec or some other VPN for an application that functions entirely in an intranet environment. The rest of JEFRi authentication assumes such an encrypted channel is in place, and only deals with establishing identity and sessions between JEFRi runtimes.

2 Authentication Context

The JEFRi authentication extension defines a context with two entities, **User** and **Authsession**. These entities form the core of handling identities during a series of tranactions.

2.1 User

A User is an entity representing any agent that is allowed privileged access to a JEFRi runtime. A User's properties are the user_id, a name, an email address, and a password. The Address is an email address as specified in RFC 5322 section 3.4 and related RFCs. Besides being a canonical representation for an online identity, the address also allows fine-grained organizational-level access control, by separating the address into the Addr-spec's local-part and domain. Since we expect especially the domain to be in dot-atom form, there is an easy mechanism to identify where in an organization hierarchy a user gets its permission. The name is simply a display-name for the user. The user id is a version 5 UUID, using the address as is for the distinguished name. The password should NEVER be sent across a unsecured channel, and a runtime MUST store a hash of a password, not the password itself.

The Authsession entity associates an ongoing series of JEFRi requests with a certain user and a certain device, as well as storing information about the state of those requests. In this way, authentication can guard against session hijacking by only allowing a certain session to originate from a single device (as identified by its IP address). Authentication sessions can time out after a certain period of inactivity, or terminated explicitly following a logout event.

2.2 Shared API

current_user logged_in

2.3 Client API

login(email, password, success[, failure]) logout

2.4 Server API

"meta":, "entities":["name": "User", "key": "user_id", "properties": ["name": "user_id", "type": "int", "attributes": "primary": "true", "name": "name", "type": "string", "attributes": , "name": "address", "type": "string", "attributes": "unique": "true"], "relationships": ["name": "authinfo", "type": "has_a", "to": "type": "Authinfo", "property": "user_id", "vname": "user", "from": "type": "User", "property": "user_id", "vname": "user"], "attributes": "vname": "users", "svname": "user",

"name": "Session", "key": "session_id", "properties": ["name": "session_id", "type": "string", "attributes": "primary": "true", "name": "expires", "type": "string", "attributes": , "name": "ip", "type": "],

"name": "Authinfo", "key": "authinfo_id", "properties": ["name": "authinfo_id", "type": "int", "attributes": "primary": "true", "name": "user_id", "type": "int", "attributes": , "name": "username", "type": "string", "attributes": "length": "45", "name": "password", "type": "string", "attributes": "length": "45", "name": "activated", "type": "string", "attributes": "nullable": "true", "length": "45", "name": "banned", "type": "string", "attributes": "nullable": "true", "length": "45", "name": "ban_reason", "type": "string", "attributes": "nullable": "true", "length": "45", "name": "new_password_key", "type": "string", "attributes": "nullable": "true", "length": "45", "name": "new_password_requested" "type": "string", "attributes": "nullable": "true", "length": "45", "name": "new_email", "type": "string", "attributes": "nullable": "true", "length": "45", "name": "new_email_key", "type": "string", "attributes": "nullable": "true", "length": "45", "name": "last_ip", "type": "string", "attributes": "nullable": "true", "length": "45", "name": "last_login", "type": "string", "attributes": "nullable": "true", "length": "45", "name": "created", "type": "string", "attributes": "nullable": "true", "length": "45", "name": "modified", "type": "string", "attributes": "nullable": "true", "length": "45"], "relationships": ["name": "user", "type": "has_a", "to": "type": "User", "property": "user_id", "vname": "user", "from": "type": "Authinfo", "property": "user_id", "vname": "user"], "attributes": "vname": "authinfo", "svname": "authinfo",

"name": "Loginattempt", "key": "login_attempt_id", "properties": ["name": "login_attempt_id", "type": "int", "attributes": "primary": "true", "name": "ip_address", "type": "string", "attributes": "nullable": "true", "length": "45", "name": "login", "type": "string", "attributes": "nullable": "true", "length": "45", "name": "time", "type": "float", "attributes": "nullable": "true"], "relationships": [], "attributes": "vname": "loginAttempts", "svname": "loginattempt",

"name": "Autologin", "key": "", "properties": ["name": "keyid", "type": "int", "attributes": "nullable": "true", "name": "user_id", "type": "int", "attributes": , "name": "user_agent", "type": "string", "attributes": "nullable": "true", "length": "45", "name": "last_ip", "type": "string", "attributes": "nullable": "true", "length": "45", "name": "last_login", "type": "float", "attributes": "nullable": "true"], "relationships": [], "attributes": "vname": "autologin", "svname": "autologin"]