MUD integration with GRASP

Brian Carpenter

November 2019

This document is a quick report on a demonstration of MUD integration with GRASP for the purpose of allowing autonomic nodes to contact a MUD Manager.

If you don't know what GRASP is, please read draft-ietf-anima-grasp, which is approved for publication as a Proposed Standard RFC as soon as its references are also approved. If you don't know what MUD is, please read RFC8520.

There are three modules in this demo. The latest published versions are at https://github.com/becarpenter/graspy, along with this document.

They are coded in Python 3. They need the **`grasp.py`** module and its associated **`acp.py`** module (not yet available on PyPy - see **`graspy.pdf`** in the above GitHub repo).

`Mudlark.py` is an Autonomic Service Agent (ASA) that also acts as a skeleton MUD Manager. It is capable of receiving a MUD URL from another node, retrieving the associated MUD file from the Internet, showing that the JSON is parsable, and if necessary verifying the MUD file's cryptographic signature. It can handle multiple transactions in parallel and is intended to run indefinitely.

`Mudslinger.py` is an ASA that in a final form will be run once on a node joining an Autonomic Network (AN), i.e. a "pledge". It will use GRASP to discover the nearest **`Mudlark`** and then send its MUD URL, using a brief GRASP negotiation session.

`Mudlark` and **`Mudslinger`** communicate using a GRASP synchronization objective **`"411:MUDURL"`** whose value is simply the MUD URL as a string. For further details, please consult the Python source. Since this is demo code, the user enters the MUD URL at the **`Mudslinger`** keyboard. In a real implementation, the URL would be "burned into" the device.

Finally, **`Mudvault.py`** is a utility program (not an ASA) to be run as necessary on the same node as **`Mudlark`**. Its purpose is to install a certificate (a PEM file) in the certificate vault used by **`Mudlark`** for signature verification. This is a primitive process to work around the use of OpenSSL CMS for verification.

OpenSSL must be installed on the **Mudlark** node. The MUD certificate vault is simply a PEM file - the concatenation of all certificates installed by **Mudvault**. It lives in **/OpenSSL/certs/mud-certs.pem** or some such place. I did my best to discover the path in a portable way, but YMMV. It's very possible that **Mudlark** and **Mudvault** will need patching to get that path right.

The code, like the GRASP prototype code, is under the Simplified BSD open source license. No guarantees and no refunds.