xmlrpcssl Documentation

Release 0.1.3

Jonatan Dellagostin

December 07, 2016

Contents

CHAPTER 1

xmlrpcssl

xmlprcssl is a Python library that provides secure communication (TLS) beetween clients and servers through xmlrpc protocol. It supports plugable handlers to provide user authentication. For now, it has as an example a ldap based authentication handler.

1.1 Server configuration

```
>>> from xmlrpcssl import SecureAuthenticatedXMLRPCServer
>>> from xmlrpcssl.handlers import LdapVerifyingRequestHandler
>>> from datetime import datetime
>>> KEY_SSL = '/tmp/server.key'
>>> CRT_SSL = '/tmp/server.crt'
>>> TCP_PORT = 433
>>> SERVER_IP = '10.0.0.1'
>>> LDAP_HOST = 'ldapHost' # User must have access granted to this host in ldap
>>> LDAP_SERVER = 'ldapServer' # ip or name of ldap server
>>> GIDNUMBER = 111 # User must be in this group in order to be authenticated
>>> IS_MASTER_USER = False # True if the user has write permissions in the ldap server
>>> BASE_USR_LOGIN_DN = 'o=Organization,c=US' # user base DN to perform login in
 # the ldap server
>>> BASE_SEARCH_DN = 'o=Organization,c=US' # search base DN to perform a search in
 # the ldap server base
>>> RequestHandler = LdapVerifyingRequestHandler # a handler that inherits from
 # BaseRequestHandler and performs user authentication
>>> OPT_ARGS = {'isMasterUser': IS_MASTER_USER, 'baseUsrLoginDn': BASE_USR_LOGIN_DN,
...  'ldapServer': LDAP_SERVER, 'gidNumber': GIDNUMBER, 'baseSearchDn': BASE_SEARCH_DN,
...  'host': LDAP_HOST, 'RequestHandler': RequestHandler}
>>> server_ssl = SecureAuthenticatedXMLRPCServer((SERVER_IP, TCP_PORT), KEY_SSL,CRT_SSL,
...  **OPT_ARGS)
>>> def test():
...  # toy test function
...  return datetime.now().strftime("%H:%M:%S")
>>> server_ssl.register_function(test)
>>> server_ssl.serve_forever()
```

1.2 Client configuration

```
>>> import ssl
>>> from xmlrpclib import ServerProxy
>>> USERNAME = 'ldapUser'
>>> PASSWORD = 'ldapUserPassword'
>>> TCP_PORT = 433
>>> SERVER_IP = '10.0.0.1'
>>> client_xml = ServerProxy('https://'+USERNAME+':'+PASSWORD+'@'+SERVER_IP+':'+str(TCP_PORT),
    context=ssl.SSLContext(ssl.PROTOCOL_TLSv1))
>>> response = client_xml.test()
>>> print·response
```

1.3 Installation

To install xmlrpcssl, simply run:

```
$ pip install xmlrpcssl
```

xmlrpcssl is compatible with Python 2.6+

1.4 Documentation

https://xmlrpcssl.readthedocs.io

1.5 Source Code

Feel free to fork, evaluate and contribute to this project.

Source: https://github.com/jonDel/xmlrpcssl

1.6 License

GPLv3 licensed.

1.7 Credits

Credits go to http://code.activestate.com/recipes/496786-simple-xml-rpc-server-over-https and https://github.com/nosmo/python-xmlrpcssl for inspiration.

CHAPTER 2

xmlrpcssl package contents:

2.1 xmlrpcssl package

2.1.1 Subpackages

xmlrpcssl.handlers package

Submodules

xmlrpcssl.handlers.ldap_handler module

Module contents

2.1.2 Submodules

2.1.3 xmlrpcssl.xmlrpcssl module

Xmlrpc server with SSL and configurable authentication plugin method

class xmlrpcssl.xmlrpcssl.**BaseRequestHandler**(*req*, *addr*, *server*)

Bases: *xmlrpcssl.xmlrpcssl.SecureXMLRPCRequestHandler*

Base Handler providing methods to handle xmlrpc incoming requests

authenticate(*headers*)

Performs user authentication

Parameters **headers** (str) – http/https headers received from client

Returns True if user successfully authenticated, False otherwise

Return type ret (bool)

Returns Error message if authentication failed, None otherwise

Return type error_msg (str)

Returns Error code if authentication failed, None otherwise

Return type error_code (str)

parse_request()

Parses incoming requests and perform user authentication

verify_user_credentials()
Verify the user credentials

Returns True if user successfully authenticated, False otherwise

Return type ret (bool)

Returns Error message if authentication failed, None otherwise

Return type error_msg (str)

Returns Error code if authentication failed, None otherwise

Return type error_code (str)

OBS: Must be overwritten with a proper authentication method in the child class

class xmlrpcssl.xmlrpcssl.**SecureAuthenticatedXMLRPCServer**(*server_address*, *keyfile*, *certfile*, ***kwargs*)
Bases: BaseHTTPServer.HTTPServer, SocketServer.BaseServer, SimpleXMLRPCServer.SimpleXMLRPCDispatcher

Xmlrpc server secured with ssl

Parameters

- **server_address** (str) – ip address of the xmlrpc server
- **keyfile** (str) – path of the ssl/tls private keyfile generated for the xmlrpc server
- **certfile** (str) – path of the ssl/tls certificate file signed by the Certification Authority

Keyword Arguments

- **log_requests** (str,optional, *default* =True) – enable log all requests
- **path** (str,optional, *default* ='/') – server http path
- **RequestHandler** (class,optional, *default* =BaseRequestHandler) – class to handle client requests
- **ssl_version** (int, optional, *default* = ssl.PROTOCOL_TLSv1) – ssl protocol version code

class xmlrpcssl.xmlrpcssl.**SecureXMLRPCRequestHandler**(*req*, *addr*, *server*)
Bases: SimpleXMLRPCServer.SimpleXMLRPCRequestHandler

Provides a ssl secured handler class for xmlrpc requests

do_POST()
Send POST responses with proper xml content

setup()
Perform prior base class initializations

2.1.4 Module contents

CHAPTER 3

Indices and tables

- genindex
- modindex
- search

X

A

B

D

P

S

V

X