NAME

Authen::SASL::Perl -- Perl implementation of the SASL Authentication framework

SYNOPSIS

```
use Authen::SASL qw(Perl);

$sasl = Authen::SASL->new(
  mechanism => 'CRAM-MD5 PLAIN ANONYMOUS',
  callback => {
    user => $user,
    pass => \&fetch_password
  }
);
```

DESCRIPTION

Authen::SASL::Perl is the pure Perl implementation of SASL mechanisms in the **Authen::SASL** framework.

At the time of this writing it provides the client part implementation for the following SASL mechanisms:

ANONYMOUS

The Anonymous SASL Mechanism as defined in RFC 2245 resp. in IETF Draft draft-ietf-sasl-anon-03.txt from February 2004 provides a method to anonymously access internet services.

Since it does no authentication it does not need to send any confidential information such as passwords in plain text over the network.

CRAM-MD5

The CRAM-MD5 SASL Mechanism as defined in RFC2195 resp. in IETF Draft draft-ietf-sasl-crammd5-XX.txt offers a simple challenge-response authentication mechanism.

Since it is a challenge-response authentication mechanism no passwords are transferred in clear-text over the wire.

Due to the simplicity of the protocol CRAM-MD5 is susceptible to replay and dictionary attacks, so DIGEST-MD5 should be used in preferrence.

DIGEST-MD5

The DIGEST-MD5 SASL Mechanism as defined in RFC 2831 resp. in IETF Draft draft-ietf-sasl-rfc2831bis-XX.txt offers the HTTP Digest Access Authentication as SASL mechanism.

Like CRAM-MD5 it is a challenge-response authentication method that does not send plain text passwords over the network.

Compared to CRAM-MD5, DIGEST-MD5 prevents chosen plaintext attacks, and permits the use of third party authentication servers, so that it is recommended to use DIGEST-MD5 instead of CRAM-MD5 when possible.

EXTERNAL

The EXTERNAL SASL mechanism as defined in RFC 2222 allows the use of external authentication systems as SASL mechanisms.

GSSAPI

The GSSAPI SASL mechanism as defined in RFC 2222 resp. IETF Draft draft-ietf-sasl-gssapi-XX.txt allows using the Generic Security Service Application Program Interface [GSSAPI] KERBEROS V5 as as SASL mechanism.

Although GSSAPI is a general mechanism for authentication it is almost exlusively used for Kerberos 5.

LOGIN

The LOGIN SASL Mechanism as defined in IETF Draft draft−murchison−sasl−login−XX.txt allows the combination of username and clear-text password to be used in a SASL mechanism.

It does does not provide a security layer and sends the credentials in clear over the wire. Thus this mechanism should not be used without adequate security protection.

PLAIN

The Plain SASL Mechanism as defined in RFC 2595 resp. IETF Draft draft−ietf−sasl−plain−XX.txt is another SASL mechanism that allows username and clear-text password combinations in SASL environments.

Like LOGIN it sends the credentials in clear over the network and should not be used without sufficient security protection.

As for server support, only *PLAIN*, *LOGIN* and *DIGEST−MD5* are supported at the time of this writing.

`server_new` OPTIONS is a hashref that is only relevant for *DIGEST−MD5* for now and it supports the following options:

− no_integrity
− no_confidentiality

which configures how the security layers are negotiated with the client (or rather imposed to the client).

SEE ALSO

Authen::SASL, Authen::SASL::Perl::ANONYMOUS, Authen::SASL::Perl::CRAM_MD5, Authen::SASL::Perl::DIGEST_MD5, Authen::SASL::Perl::EXTERNAL, Authen::SASL::Perl::GSSAPI, Authen::SASL::Perl::LOGIN, Authen::SASL::Perl::PLAIN

AUTHOR

Peter Marschall <peter@adpm.de>

Please report any bugs, or post any suggestions, to the perl-ldap mailing list <perl−ldap@perl.org>

COPYRIGHT