Seminario 5
El protocolo XMPP

IGNACIO CORDÓN,
MARIO ROMÁN
Universidad de Granada
19 de octubre de 2014

Resumen

Índice

1. Introducción al XMPP

El protocolo XMPP (Extensible Messaging and Presence Protocol) se usa para la mensajería instantánea, así como para las llamadas de voz y vídeo. El desarrollo del protocolo fue iniciado por **Jeremie Miller** en el 1998, continuado por la comunidad de código abierto Jabber y finalmente formalizado en 2002 por la IETF.

En 2004 se publicaron los RFCs del protocolo. Han vuelto a ser actualizados en 2011, y, aunque la base del protocolo continúa estable, la **XMPP Standards Foundation** sigue definiendo extensiones al protocolo.

2. Estructura del XMPP

XMPP sigue una estructura cliente/servidor. El cliente y el servidor se comunican a través de una conexión TCP en el puerto 5222. Y la información que se envía sobre XMPP va contenida en un streaming de objetos XML.

2.1. Proceso de entrega de mensajes

2.1.1. Inicio de la sesión

La sesión se inicia con la etiqueta `<stream>` y se finalizará con la etiqueta `</stream>`. Por razones de seguridad, a la apertura de la comunicación le sigue negociación por TLS y SASL. Después de la negociación, se abre un nuevo canal de comunicación más seguro.

Más detalladamente, para requerir un nuevo inicio de sesión, el cliente envía un paquete para la apertura:

```
<stream:stream to='example.com'
        xmlns='jabber:client'
        xmlns:stream='http://etherx.jabber.org/streams'
        version='1.0'>
```

Donde `example.com` es la URL del servidor XMPP al que se conecta. El servidor devolverá entonces un paquete con los requisitos para la negociación TLS o SASL.

```
<stream:features>
```

```
  <starttls xmlns='urn:ietf:params:xml:ns:xmpp-tls'>
    <required/>
  </starttls>
  <mechanisms xmlns='urn:ietf:params:xml:ns:xmpp-sasl'>
    <mechanism>DIGEST-MD5</mechanism>
    <mechanism>PLAIN</mechanism>
    <mechanism>EXTERNAL</mechanism>
  </mechanisms>
</stream:features>
```

2.1.2. Encriptación y autorización

Si el servidor necesita una negociación TLS, el cliente enviará un `STARTTLS` al servidor:

```
<starttls xmlns='urn:ietf:params:xml:ns:xmpp-tls'/>
```

A lo que el servidor responderá en función de si el TLS está permitido o si causa error:

```
<!-- Aceptado -->
<proceed xmlns='urn:ietf:params:xml:ns:xmpp-tls'/>
<!-- Error -->
<failure xmlns='urn:ietf:params:xml:ns:xmpp-tls'/>
```

Cuando es procesada la solicitud TLS, el cliente solicitará una nueva sesión, a la que el servidor responderá con la necesidad de una negociación SASL.

Para la negociación SASL, el cliente debe elegir un método de autenticación entre los disponibles (DIGEST-MD5, PLAIN y EXTERNAL). En el caso de autorización más simple (PLAIN), se envía una cadena codificada como "`\0User\0Pass`". El servidor responderá a esto en función de si acepta o no la petición:

```
<!-- Aceptado -->
<success xmlns='urn:ietf:params:xml:ns:xmpp-sasl'/>
<!-- Error -->
<failure xmlns='urn:ietf:params:xml:ns:xmpp-sasl'/>
```

3. Conexión a otros protocolos. Pasarelas

3.1. Protocolos base de XMPP

3.2. Extensiones a XMPP

3.3. XMPP y HTTP

Referencias

1. XMPP Standards Foundation. October, 2007.
`http://xmpp.org/2007/10/what-is-xmpp/`.