“Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like.”

The Hacker Manifest
The Mentor, 1986

Jify – Enigform + SSL for secure instant messaging

By Arturo 'Buanzo' Busleiman / OWASP Argentina

buanzo@buanzo.com.ar
Http://www.buanzo.com.ar/pro/eng.html

Table of contents

Introduction to OpenPGP

Pretty Good Privacy was created by Phil Zimmerman in 1991.

In July 1997 the OpenPGP Standard was proposed by Phil to the Internet Engineering Task Force.

RFC 2440 got published in November 1998, now obsoleted by RFC 4880 (November 2007).

It's mostly used for secure email exchange, verification of files, encryption in general.

It's four basic operations are: sign/verify, encrypt/decrypt.

Introduction to OpenPGP

It uses two “keys”:

* The Private key, passphrase-protected, used to sign and decrypt messages.

* The Public key, to be shared with the entire world, used to verify and encrypt messages.

The user can define trust levels for a person's public key.

Public keys can be signed!

A web-of-trust is then created.

Introduction to OpenPGP

There are proprietary (closed) and open source implementations of the OpenPGP standard: PGP by PGP Inc. and the GNU Privacy Guard (gnupg / gpg) by Werner Koch.

Of course, they are compatible with each other.

Don't you LOVE standards, and standard-complying companies?

OpenPGP is integrated in KDE, GNOME, propietary OSes, email clients, etc.

Introduction to HTTPS (HTTP + TLS)

HTTP is a cleartext protocol. That means the communication between user and website can be read by a 3rd party.

Transport Layer Security defines a whole set of functions that allow a connection (two connected sockets) to be encrypted.

When you visit an https:// page, server certificates are presented and validated by the browser.

Introduction to Enigform (you WANT the training!)

Enigform is an OWASP Project that uses OpenPGP to enhance HTTP by adding digital signatures to requests and responses.

Taking advantage of it, a secure session initiation protocol was created, using the challenge/response metodology. It might allow ENCRYPTED requests.

It exists as a Firefox Add-on called enigform, an Apache module called mod_openpgp, and a Wordpress enigform-authentication plugin.

Announcing the Just for You! Instant Messenger

Jify uses HTTPS to transport data between users and servers.

Enigform is used for session initiation.

The contact list is loaded from the users key ring, and can use the web-of-trust to add more contacts.

Announcing the Just for You! Instant Messenger

The message is OpenPGP-encrypted in layers:

the inside layer for the message's recipient, and the outside layer for the server.

This way, the server can route the message to the proper recipient, but cannot read the contents.

In combination with HTTPS, it protects the whole transaction against eavesdroppers.

Announcing the Just for You! Instant Messenger

The most basic Jify client can be written in Python very easily, but the first public release will be a Mono and .NET compatible C# application.

For that, a C# OpenPGP implementation is being developed in collaboration with Bryan Slatner.

That implementation will be Mono and .NET compatible as well, making a simple cross-platform OpenPGP library a reality.

Why Jify and not OpenPGP for XMPP/Jabber?

Well, it's an entirely different approach, a completely different protocol, and I think the world of IT appreciates choices.

And I wanted to do it.

There, I said it.

Questions?

Have fun! Thank you!

Arturo 'Buanzo' Busleiman
buanzo@buanzo.com.ar