Agenda

- What is GnuTLS?
- What's going on? (v2.2.x)
- Software Patent Blues
- Hands-on GnuTLS: gnutls-cli, certtool, ...
What is GnuTLS?
GnuTLS is an implementation of the SSL/TLS standard

- HTTP, IMAP, SMTP, POP3, ...
What is GnuTLS?

Implements X.509/PKIX and PKCS standards
A successful free software project

What is GnuTLS?
A successful free software project

<table>
<thead>
<tr>
<th>rank</th>
<th>name</th>
<th>inst</th>
<th>vote</th>
<th>old</th>
<th>recent</th>
<th>no-files</th>
</tr>
</thead>
<tbody>
<tr>
<td>103</td>
<td>libssl0.9.8</td>
<td>68202</td>
<td>54738</td>
<td>2143</td>
<td>11317</td>
<td>4</td>
</tr>
<tr>
<td>112</td>
<td>libgnutls13</td>
<td>67966</td>
<td>53525</td>
<td>2809</td>
<td>11623</td>
<td>9</td>
</tr>
<tr>
<td>12165</td>
<td>libmatrixssl1.7</td>
<td>150</td>
<td>1</td>
<td>9</td>
<td>0</td>
<td>140</td>
</tr>
<tr>
<td>19482</td>
<td>libmatrixssl1.8</td>
<td>44</td>
<td>19</td>
<td>22</td>
<td>3</td>
<td>0</td>
</tr>
</tbody>
</table>
Written in C
Object Oriented Design
What is GnuTLS?
Official API bindings in Guile (scheme) and C++

What is GnuTLS?
What is GnuTLS?

Started early months of 2000
What is GnuTLS?

Written by Nikos Mavrogiannopoulos
I maintain it since August 2004
What is GnuTLS?

Reference manual

3.1 TLS Layers

TLS is a layered protocol, and consists of the Record Protocol, the Handshake Protocol and the Alert Protocol. The Record Protocol is to serve all other protocols and is above the transport layer. The Record protocol offers symmetric encryption, data authenticity, and optionally compression.

The Alert protocol offers some signaling to the other protocols. It can help informing the peer for the cause of failures and other error conditions. See the Alert Protocol for more information. The alert protocol is above the record protocol.

The Handshake protocol is responsible for the security parameters' negotiation, the initial key exchange and authentication. See the Handshake Protocol, for more information about the handshake protocol. The protocol layering in TLS is shown in the figure below.
What is GnuTLS?

Documented source code

```c
#include <gnutls/x509.c>

int gnutls_certificate_set_x509_simplePkcs12_file
(gnutls_certificate_credentials_t res,
 const char *cert_file,
 gnutls_x509_crt_type_t type,
 const char *password);
```

This function sets a certificate/private key pair and/or a CRL in the gnutls_certificate_credentials_t structure. This function may be called more than once (in case multiple keys/certificates exist for the server).

MACed PKCS12 files are supported. Encrypted PKCS12 bags are supported. Encrypted PKCS8 private keys are supported. However, only password based security and the same password for all operations, are supported.

The private keys may be RSA PKCS1 or DSA private keys encoded in the OpenSSL way.
What is GnuTLS?

Official GNU project
libtasn1, libgcrypt, opencdk, libz, liblzo
Version control: Git
(before May 2007: CVS)
What is GnuTLS?
savannah.gnu.org
What is GnuTLS?
September 2007: Version 2.0
What's Going On?
(v2.2.x)
Use your OpenPGP key during handshake
Verify server OpenPGP key via web-of-trust
Apache mod_gnutls work in progress

http://www.outoforder.cc/projects/apache/mod_gnutls/
mod_ssl 15kLOC
mod_gnutls 3kLOC
Support for Server Name Indication
Please write cool applications!

(any Debian Developers out there?)
RFC 5054
(November 2007)
Strong password-based authentication inside the TLS handshake
- Working mod_gnutls v.0.4.1
What’s Going On?

TLS v1.2

- We implemented early drafts, but the protocol has changed since then...
Opaque PRF Input

- Allows systems to provide additional randomness for master key generation
External RSA/DSA signing

- No need to have RSA/DSA keys in same process
- OpenPGP Scute PKCS#11 engine tested
- Upcoming GNOME integration with SeaHorse
uClinux port

- Embedded platforms
- http://josefsson.org/uclinux/
Software Patent Blues
TLS Authorization Extension
Implemented in v2.0
Patent Application
filed September 2005
IETF Last Call in May 2006
Approved June 2006
IETF notified about patent in November 2006
IETF policy on patents:

RFC 3979: Intellectual Property Rights in IETF Technology

6.1. Who Must Make an IPR Disclosure?

6.1.1. A Contributor's IPR in his or her Contribution

Any Contributor who reasonably and personally knows of IPR [...] must make a disclosure in accordance with this Section 6. [...] Contributors must disclose IPR meeting the description in this section; there are no exceptions to this rule.
We have removed our implementation

“This technique may be patented in the future, and it is not of crucial importance for the Internet community. After deliberation we have concluded that the best thing we can do in this situation is to encourage society not to adopt this technique. We have decided to lead the way with our own actions.”

Please develop a free alternative!
Hands-on GnuTLS
• certtool
• gnutls-cli
• gnutls-serv
- Generating private key
- Generating CA
- Generating server certificate
- Starting a test HTTPS server
- Generating client certificate
- Creating PKCS#12 blob
- Import into browser
- Connect to server
Questions?

Answers?

Thank you for listening!