




Personal Security Manager in Mozilla

By
Yun Zhou

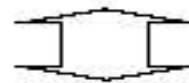


Table of Content

- Overall Structure of Mozilla's Crypto System
- PSM (Personal Security Manager)
 - Overview
 - UI
 - Some package details
- NSS (Network Security Services)
 - A brief overview



Structure of Mozilla's Crypto System



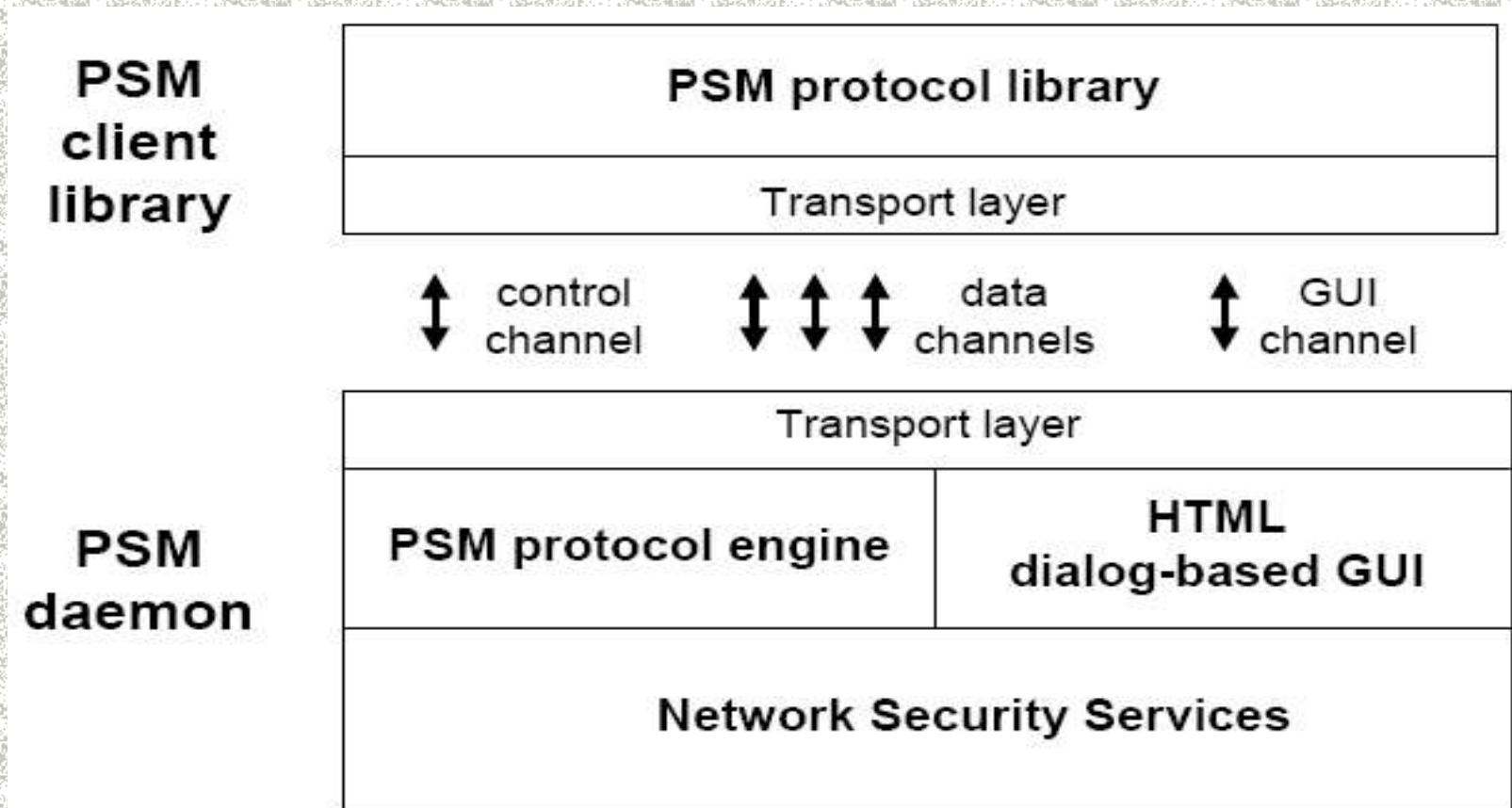


Overview of PSM

- PSM provides solutions to the security of the client application.
 - Supports SSLv2, v3 and TLS.
 - Provides a large variety of cipher suites for key exchange, digital signatures, bulk encryption, and data integrity.
 - Manages certificates for mutual authentication.
 - Manages passwords and cookies.
 - Very user-friendly UI for the users to customize their security settings. Easy to understand if you have some basic knowledge about Internet security
 - Easy access to the security info of a particular page
 - Other PKI functions.



Structure of PSM

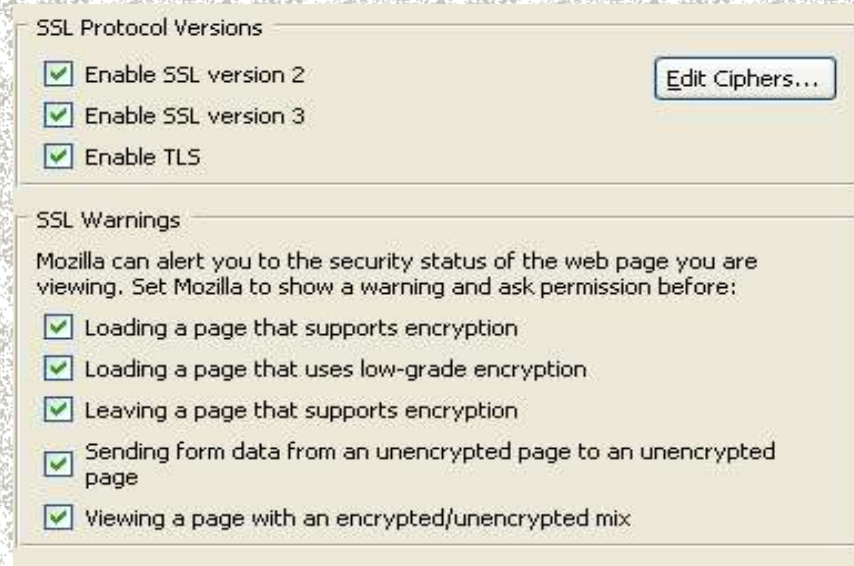
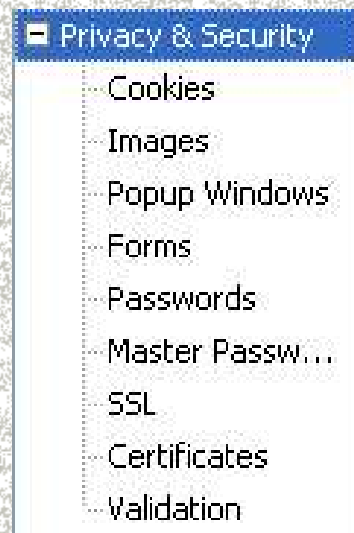




PSM User Interface

Select Preferences off the Edit menu. Expand Privacy and Security. You will see

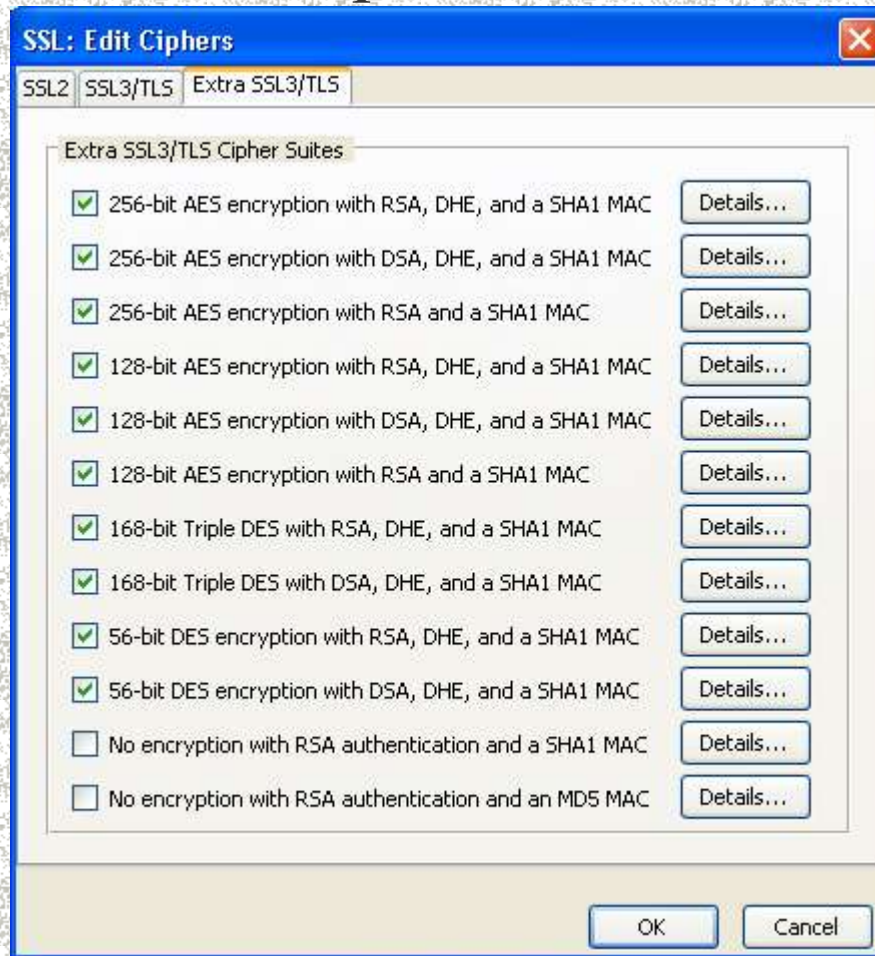
Let's take a look at SSL...



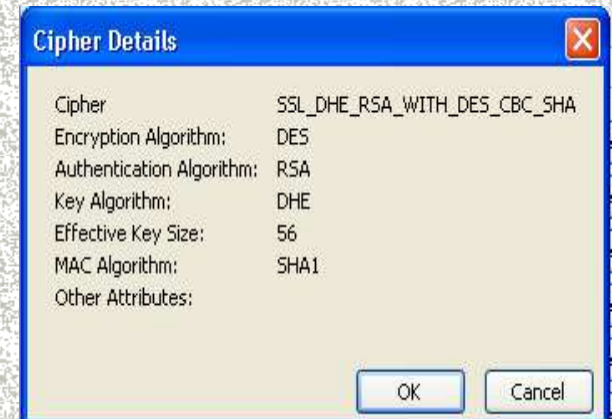
You can enable or disable the protocols or warnings.
Note the warning for low-grade encryption is new in PSM 2.0.

PSM User Interface (cont'd)

Click “Edit Ciphers”...



You can explore the ciphers available in PSM and disable one if you are skeptical about its security. You can see the details such as





Security Info for a Page

Type www.hotmail.com in Mozilla. Click  the lower-right corner of the window, and you will get the page info. Click Security tab...



It shows that the hotmail server is authenticated by Verisign, a certificate authority that your browser trusts.

Furthermore, the connections for this is encrypted by RC4 with a 128-bit key.

If you click “View”, you will access even more details about the hotmail server’s certificate, such as the public key, the issuer, the certificate signature, the algorithms, the time expansion, the finger-prints...



PSM Package Details

Two XPCOM shared libraries: pki and ssl
ssl links to NSS 3.2 and handles all the SSL sockets.

Provides event handlers and appropriate warnings.

Defines and implements IDL interfaces for access to NSS libraries.

Supports embedding systems to use the cryptographic components without the UI.

High performance – fast enough for disk encryption The goal is 1MB per second for both encryption and decryption.

pki implements the UI using XUL and related XPCOM objects.



nsNTLMAuthModule.cpp

This module supports DES and MD5 using NSS API.

```
// set odd parity bit (in least significant bit position)
static PRUint8 des_setkeyparity(PRUint8 x)
// build 64-bit des key from 56-bit raw key
static void des_makekey(const PRUint8 *raw, PRUint8 *key)
// run des encryption algorithm (using NSS)
static void des_encrypt(const PRUint8 *key, const PRUint8
    *src, PRUint8 *hash)
// MD5 support code
static void md5sum(const PRUint8 *input, PRUint32 inputLen,
    PRUint8 *result)
```




Overview of NSS

NSS provides an open-source implementation of security libraries that can be reused by embedding applications.

SSL v2 and v3, TLS v1, PKCS #1, #3, #5, #7, #8, #9, #10, #11, #12, S/MIME for encrypted MIME data, X.509 v3 certificates, OCSP (The Online Certificate Status Protocol), PKIX Certificate and CRL Profile, and a suite of advanced ciphers such as AES, RSA, DSA, Triple DES, DES, Diffie-Hellman, RC2, RC4, SHA-1, MD2, MD5.

NSS also provides tools to manage keys and security modules, and to debug and diagnose code.



NSS Package

NSS exports the following functions in shared libraries:

- # The SSL library for SSL operations.
- # The S/MIME library for S/MIME operations.
- # The NSS library for crypto operations.



NSS API for Crypto Functions

The following functions are defined in security/nss/lib/pk11wrap

PK11_Authenticate, PK11_ChangePW,
PK11_CheckUserPassword, PK11_CipherOp,
PK11_CloneContext, PK11_ConfigurePKCS11,
PK11_CreateContextBySymKey,
PK11_CreateDigestContext, PK11_DestroyContext,
PK11_DestroyTokenObject, PK11_DigestBegin,
PK11_DigestOp, PK11_DigestFinal, PK11_DoesMechanism,
PK11_Finalize, PK11_FindCertByIssuerAndSN,
PK11_FindCertFromDERCert...

For a complete listing, see

<http://www.mozilla.org/projects/security/pki/nss/ref/nssfunctions.html>



How Does PSM Call PK11_CipherOp

This code shows how des_encrypt function calls PK11_CipherOp to do the actual encryption. (See security/manager/ssl/src/nsNTLMAuthModule.cpp)

```
// run des encryption algorithm (using NSS)
```

```
static void
```

```
des_encrypt(const PRUint8 *key, const PRUint8 *src, PRUint8 *hash)
```

```
{...
```

```
keyItem.data = (PRUint8 *) key;
```

```
keyItem.len = 8;
```

```
symkey = PK11_ImportSymKey(slot, cipherMech, PK11_OriginUnwrap,  
    CKA_ENCRYPT, &keyItem, nsnull);
```

```
if (!symkey) {
```

```
    NS_ERROR("no symkey");
```

```
    goto done;
```

```
}
```

```
...
```

```
rv = PK11_CipherOp(ctxt, hash, (int *) &n, 8, (PRUint8 *) src, 8);
```

```
if (rv != SECSuccess) {
```

```
    NS_ERROR("des failure");
```

```
    goto done;
```

```
}
```

```
rv = PK11_DigestFinal(ctxt, hash+8, &n, 0);
```

```
if (rv != SECSuccess) {
```

```
    NS_ERROR("des failure");
```

```
    goto done;
```

```
}
```




References

Introduction to Network Security Services. Retrieved from

<http://www.mozilla.org/projects/security/pki/nss/intro.html>

NSS 3.2 Public Functions. Retrieved from

<http://www.mozilla.org/projects/security/pki/nss/ref/nssfunctions.html>

Network Security Services (NSS). Retrieved from

<http://www.mozilla.org/projects/security/pki/nss/#Documentation>

NSS Security Tools. Retrieved from <http://www.mozilla.org/projects/security/pki/nss/tools/>

Open Source Crypto and Mozilla. Retrieved from

<http://www.mozilla.org/docs/ora-oss2000/crypto/open-source-crypto-and-mozilla.pdf>.

PSM 2.0 Roadmap - A Technical View. Retrieved from

<http://www.mozilla.org/projects/security/pki/psm/roadmap.html>

Personal Security Manager (PSM). Retrieved from

<http://www.mozilla.org/projects/security/pki/psm/>

PSM 2.0 Plan. Retrieved from http://www.mozilla.org/projects/security/pki/psm/plan_20.html

What's New in Crypto for Netscape 6.1. Retrieved from <http://people.netscape.com/lord/psm/n61/>