

# How to compile Linux kernel and IPsec-tools using Camellia

Nippon Telegraph and Telephone Corporation

Version 1.0, Nov. 8<sup>th</sup>, 2006

## (1) Getting the Linux kernel sources and “Camellia additional to Linux-2.6.18”

Download “linux-2.6.18.tar.bz2” from the sites such as ftp. kernel.org. Then download “Camellia additional to Linux-2.6.18” from this web site. Save the downloaded file as” camellia-linux-2.6.18.patch.gz”.

## (2) Patches for the Linux kernel sources

```
$ tar xvfj linux-2.6.18.tar.bz2
$ cd uncompressed directory
$ zcat ../camellia-linux-2.6.18.patch.gz | patch -p0
```

## (3) Compile and install of the Linux kernel

By inputting the following command, compile and install the Linux kernel. Because some commands and parameters are different depending on your environment, please adjust to your environment accordingly. As to the details of the commands, see manuals and so on.

```
$ make menuconfig
```

(3.1) Select the item of “Load an Alternate Configuration File” in the menu and load the running config file of the kernel.

\*You can check the kernel version you are using by the following command.

```
$ uname -a
```

If the result of the above command is 2.6.9-34.EL, set as;

```
/boot/config-2.6.9-34.EL
```

(3.2) Select the following item in order to use Camellia;

```
Cryptographic options --->
```

Next, select the following indicated item and enable it.

```
Camellia cipher algorithms
```

If the <M> mark is put to the left side of the item name, it is enabled.

```
$ make
```

```
$ make modules_install
```

```
$ make install
```

This is the end of the install. Reboot and run with the kernel version you have

installed.

- (4) Getting OpenSSL sources which have corresponded to Camellia

Download “openssl-0.9.8c.tar.gz“ from <http://www.openssl.org/source/>.

- (5) Compile and install of OpenSSL

```
$ tar xvfz openssl-0.9.8c.tar.gz
```

```
$ cd uncompressed directory
```

```
./config enable-camellia shared
```

```
$ make depend
```

```
$ make
```

```
$ make install
```

OpenSSL is installed under `usr/local/ssl`.

- (6) Getting the ipsec-tools sources and “Camellia additional to ipsec-tools CVS HEAD 20061002”

Check out the ipsec-tools sources from CVS HEAD.

```
$ cvs -d anoncvs@anoncvs.netbsd.org:/cvsroot co ipsec-tools
```

Download “Camellia additional to ipsec-tools CVS HEAD 20061002” from this web site in the same directory. Save the downloaded file as “camellia-ipsec-tools-cvs-20061002.patch.gz”.

- (7) Patches for ipsec-tools sources

```
$ cd ipsec-tools
```

```
$ zcat ../camellia-ipsec-tools-cvs-20061002.patch.gz | patch -p0
```

- (8) Compile and install of ipsec-tools

```
$ bootstrap
```

```
$ ./configure --with-openssl=/usr/local/ssl
```

```
$ make
```

```
$ make install
```

This is the end of the install of ipsec-tools.

Don't forget to set the paths of `usr/local/bin/setkey` and `usr/local/sbin/racoon`.

- (9) Communication of IPsec

Add “camellia” to “proposal” and “sainfo” of `racoon.conf`. As to the other details of the settings about IPsec, see manuals and so on.