Upgrading CERT Tapioca 1.0 to Support HTTP/2

Tapioca and HTTP/2

HTTP/2 is a web protocol supported by modern browsers such as Google Chrome. By default, CERT Tapioca and the mitmproxy software that it uses does not support HTTP/2. It is possible to update the OS and the mitmproxy software to enable HTTP/2 support with Tapioca.

Upgrading Ubuntu to 14.04

Upgrading the Tapioca OS, which is Ubuntu 12.04, to version 14.04 is a prerequisite for HTTP/2 support. The upgrade process is relatively straightforward. But before proceeding, create a snapshot of the VM in case something goes wrong. To perform the upgrade, enter the following in a terminal:

```
sudo do-release-upgrade
```

When prompted, accept the default answers to keep the original configuration files. If you do not do this, you will lose the customizations that enable required features such as IPv4 forwarding.

At the end of the upgrade process, you can say yes to the question asking if you'd like to remove obsolete packages. This will save disk space.

You will need to reboot the VM to activate the changes.

Upgrading mitmproxy and the supporting python libraries

After upgrading to Ubuntu 14.04, mitmproxy and the python libraries that it uses should be upgraded. To perform the upgrade, enter the following in a terminal:

```
cd ~/in
wget http://archive.ubuntu.com/ubuntu/pool/main/o/openssl/openssl_1.0.2g-1ubuntu4.5_i386.deb
wget http://archive.ubuntu.com/ubuntu/pool/main/o/openssl/libssl1.0.0_1.0.2g-1ubuntu4.5_i386.deb
wget http://archive.ubuntu.com/ubuntu/pool/main/o/openssl/libssl-dev_1.0.2g-1ubuntu4.5_i386.deb
sudo dpkg -i openssl_1.0.2g-1ubuntu4.5_i386.deb
sudo dpkg -i libssl1.0.0_1.0.2g-1ubuntu4.5_i386.deb
sudo dpkg -i libssl-dev_1.0.2g-1ubuntu4.5_i386.deb
sudo pip install pip --upgrade
sudo pip install pyOpenSSL --upgrade --force
sudo pip install mitmproxy --upgrade
```

CERT Tapioca Tweaks

Now that you've updated both Ubuntu and mitmproxy to support HTTP/2, it is worth performing two other modifications:

Updating the mitmproxy CA certificate

Due to a design flaw in the released version of CERT Tapioca, the CA certificate used to generate website certificates is not trusted after July 10, 2016. This will interfere with testing environments with the mitmproxy CA certificate installed on the client. Please see CERT Tapioca 1.0 and Expired CA Certificates for instructions on how to correct this.

Cleanup on use of "No Proxy"

When pressing the "No Proxy" button, CERT Tapioca leaves the mitmproxy and related windows on the screen. Edit the `~/noproxy.sh` script to add the three `killall` lines at the beginning to perform cleanup:

```
#!/bin/bash

sudo killall -HUP mitmproxy
sudo killall -HUP tcpdump
sudo killall -HUP tail
sudo ~/iptables_noproxy.sh
echo Intercepting proxy disabled
sleep 5
```

Now it will be more obvious when Tapioca is in intercepting mode or in pass-through mode.