BFF Installation Notes

The easiest way to get BFF up and running is to use the UbuFuzz virtual machine. However, if this is not an option for you, it should possible to run BFF on any UNIX-like operating system, as long as the dependencies are met.

Dependencies

For basic fuzzing functionality, the following packages are required:

- Python 2.7
- Python Numpy
- Python Scipy
- Python Yaml
- gdb 7.1 or later
- zzuf (patched by CERT)

In order to build zzuf and the other BFF dependencies, the following packages may be required:

- svn
- gcc
- make
- automake
- libtool
- gcc-c++
- ncurses-devel

For additional analysis tools that can be used during or after a fuzzing campaign, the following packages are required:

- Python hcluster
- Python matplotlib

Filesystem layout

By default, BFF will use the following filesystem locations:
For the location of the scripts (including bff.py):
`~/bff`

For the results:
`~/results`

The default fuzzing target of ImageMagick:
`~/convert`

All of these locations can be symlinks.

Beginning a fuzzing campaign

Simply run `~/bff/batch.sh` to start fuzzing.

Tuning the operating system

UbuFuzz has several optimizations that improve fuzzing performance. If using your own operating system, you may wish to make the following changes:

- The Fluxbox window manager is used instead of the heavy Gnome or KDE desktop environments.
- Fluxbox is configured to not raise or focus new windows. This can help in situations where you may need to interact with the guest OS while a GUI application is being fuzzed.
- Memory randomization is disabled (kernel.randomize_va_space = 0 in `/etc/sysctl.conf`). This helps remove duplicate crashes where the target application does not have debug symbols.
- VMware Tools is installed, which allows the guest OS to share a directory with the host.
- The OS is configured to automatically log in and start X.
- sudo is configured to not prompt for a password.
- strip is symlinked to /bin/true, which prevents symbols from being removed when an application is built.

Example installation on Fedora 16 32-bit

To install BFF on a Fedora 16 32-bit system, for example, the following steps can be performed:

1) Install dependencies present in the package system:

```
yum install numpy scipy python-yaml valgrind svn automake libtool gcc-c++ ncurses-devel
```

2) Install libcaca, which is a dependency for building zzuf:

```
svn co https://github.com/cacalabs/libcaca/trunk libcaca
cd libcaca
./bootstrap
./configure
make
sudo make install
```

3) Install the zzuf version patched by CERT:

```
export PKG_CONFIG_PATH=/usr/local/lib/pkgconfig
unzip zzuf-patched.zip
cd zzuf-patched
./bootstrap
./configure
make
sudo make install
```

4) Install old ImageMagick version as default fuzz target:

```
sudo yum groupinstall "X Software Development"
sudo ln -sf /usr/include/asm/byteorder.h /usr/include/sys/byteorder.h
wget http://downloads.sourceforge.net/project/imagemagick/old-sources/5.x/5.2/ImageMagick-5.2.0.tar.gz
tar xzvf ImageMagick-5.2.0.tar.gz
cd ImageMagick-5.2.0
./configure
make
sudo make install
```

5) Unzip BFF scripts:

```
mkdir ~/bff
unzip scripts.zip -d ~/bff
```

6) Configure symlinks

```
ln -s /usr/local/bin/convert ~/convert
ln -s ~/bff/scripts ~/bff
ln -s ~/bff/results ~/results
```

7) Start fuzzing

```
~/bff/batch.sh
```

System Performance Configurations for Fedora

a) Disable Memory Randomization:
add "`kernel.randomize_va_space=0`" to `/etc/sysctl.conf`
(reboot after this change)

b) Symlink strip to true (to preserve symbols during builds)

```
sudo mv /usr/bin/strip /usr/bin/strip.bak
sudo ln -s /bin/true /usr/bin/strip
```

c) Use Fluxbox Window Manager instead of Metacity
`sudo yum install fluxbox`
(Log out)
(Log in, selecting Fluxbox from drop-down selection)
(Right-click desktop, select "Run")
  (Type in "fluxbox-generate_menu")
(Right-click desktop -> Fluxbox Menu -> Configure -> Focus model)
  (Cick the following options and ensure they are not selected to disable them:)
    (Auto Raise)
    (Focus New Windows)

Example installation on Ubuntu 11.10 32-bit

To install BFF on an Ubuntu 11.10 32-bit system, for example, the following steps
can be performed:

1) Install dependencies present in the package system:

```
sudo apt-get install python-numpy python-scipy python-yaml valgrind subversion automake libtool build-
essential libncurses5-dev
```

2) Install libcaca, which is a dependency for building zzuf:

```
svn co svn://svn.zoy.org/caca/libcaca/trunk libcaca
cd libcaca
./bootstrap
./configure
make
sudo make install
```

3) Install the zzuf version patched by CERT:

```
unzip zzuf-patched.zip
cd zzuf-patched
./bootstrap
./configure
make
sudo make install
```

4) Install old ImageMagick version as default fuzz target:

```
sudo apt-get install libx11-dev libxt-dev
sudo ln -sf /usr/include/i386-linux-gnu/asm/byteorder.h /usr/include/sys/byteorder.h
wget http://downloads.sourceforge.net/project/imagemagick/old-sources/5.x/5.2/ImageMagick-5.2.0.tar.gz
tar zxf ImageMagick-5.2.0.tar.gz
cd ImageMagick-5.2.0
./configure
make
sudo make install
```

5) Unzip BFF scripts:

```
mkdir ~/bff
unzip scripts.zip -d ~/bff
```

6) Configure symlinks

```
ln -s /usr/local/bin/convert ~/convert
ln -s ~/bff/scripts ~/bff
ln -s ~/bff/results ~/results
```

7) Start fuzzing

```
~/bff/batch.sh
```

System Performance Configurations for Ubuntu

a) Disable Memory Randomization:
add "`kernel.randomize_va_space=0`" to `/etc/sysctl.conf`
(reboot after this change)

b) Symlink strip to true (to preserve symbols during builds)

```
sudo mv /usr/bin/strip /usr/bin/strip.bak
sudo ln -s /bin/true /usr/bin/strip
```

c) Use Fluxbox Window Manager instead of Metacity
`sudo apt-get install fluxbox`
(Log out)
(Log in, selecting Fluxbox from drop-down selection (Gear symbol))
(Right-click desktop -> Fluxbox Menu -> Configure -> Focus model)
(Cick the following options and ensure they are not selected to disable them:)
(Focus New Windows)
(Auto Raise)

Example installation on openSUSE 12 32-bit

To install BFF on an openSUSE 12 32-bit system, for example, the following steps
can be performed:

1) Install dependencies present in the package system:

```
sudo zypper ar -f 'http://download.opensuse.org/repositories/devel:/languages:/python/openSUSE_12.1/'
python
sudo zypper install python-numpy python-scipy valgrind subversion automake libtool gcc-c++ ncurses-devel
make
```

2) Install libcaca, which is a dependency for building zzuf:

```
svn co svn://svn.zoy.org/caca/libcaca/trunk libcaca
cd libcaca
./bootstrap
./configure
make
sudo make install
```

3) Install the zzuf version patched by CERT:

```
unzip zzuf-patched.zip
cd zzuf-patched
./bootstrap
./configure
make
sudo make install
```

4) Install old ImageMagick version as default fuzz target:

```
sudo zypper install xorg-x11-devel
sudo ln -sf /usr/include/asm/byteorder.h /usr/include/sys/byteorder.h
wget http://downloads.sourceforge.net/project/imagemagick/old-sources/5.x/5.2/ImageMagick-5.2.0.tar.gz
tar xzvf ImageMagick-5.2.0.tar.gz
cd ImageMagick-5.2.0
./configure
make
sudo make install
```

5) Unzip BFF scripts:

```
mkdir ~/bff
unzip scripts.zip -d ~/bff
```

6) Configure symlinks

```
ln -s /usr/local/bin/convert ~/convert
ln -s ~/bff/scripts ~/bff
ln -s ~/bff/results ~/results
```

7) Start fuzzing

```
~/bff/batch.sh
```

System Performance Configurations for Fedora

a) Disable Memory Randomization:
add "`kernel.randomize_va_space=0`" to "`/etc/sysctl.conf`"
(reboot after this change)

b) Symlink strip to true (to preserve symbols during builds)

```
sudo mv /usr/bin/strip /usr/bin/strip.bak
sudo ln -s /bin/true /usr/bin/strip
```

c) Use Fluxbox Window Manager instead of Metacity

```
sudo zypper ar -f 'http://download.opensuse.org/repositories/X11:/windowmanagers/openSUSE_12.1/'
windowmanager
sudo zypper install fluxbox
```

(Log out)
(Log in, selecting Fluxbox from drop-down selection (icon with 3 bars))
(Right-click desktop, select "Run command")
  (Type in "fluxbox-generate_menu")
(Right-click desktop -> Fluxbox Menu -> Configure -> Focus model)
  (Cick the following options and ensure they are not selected to disable them:)
    (Focus New Windows)
    (Auto Raise)