Ceylan's HOWTO

HOW-TO

Contact: about (dash) howtos (at) esperide (dot) com

Creation date: Wednesday, November 17, 2021

Lastly updated: Wednesday, February 2, 2022

Version: 0.0.2

Status: In progress

Dedication: Users of these HOWTOs

Abstract: The role of these `HOW-TOs` is, akin to a cookbook, to share a collection of (technical) recipes ("how-to do this task?) regarding various topics.

These elements are part of the Ceylan umbrella project.

The latest version of this documentation is to be found at the official Ceylan-HOWTOs website (`http://howtos.esperide.org`).

> **Note**
>
> This PDF document includes cross-references between HOWTOs, yet these links make sense only in the context of its HTML counterpart.

Table of Contents

Using the GNU/Linux Operating System

Contact: about (dash) howtos (at) esperide (dot) com

Creation date: Sunday, December 19, 2021

Lastly updated: Wednesday, February 2, 2022

Overview

GNU/Linux is our operating system of choice, for many reasons: it is in free software, it is efficient, trustable, reliable and controllable, its mode of operation does not change much over time so any time invested on it is well spent.

Over the years we tried many distributions, including Ubuntu, Debian, Gentoo, Mint.

Our personal all-time favorite is clearly Arch Linux, because it leaves much control to its end user (not attempting to hide details that have to be mastered anyway), it is a "clean" one, driven by a skilled and knowledgeable community, and also because it is a rolling distribution: it updates constantly its packages *without needing to regularly upgrade the whole system*, which would jeopardise it in the same movement (global system updates rarely complete successfully and tend to be postponed because of the many problems they trigger; we found preferable to deal with issues incrementally on a live system - rather than on one that may fail to reboot properly).

It ends up with a very stable, hassle-free distribution, with cutting-edge packages and higher uptimes (several months without needing to reboot), which is desirable for server-like usages.

Software Update

The setup that we use is to perform **automatic nightly updates**. For that we use our update-distro.sh script, run through root's crontab as:

```
$ crontab -l
# Each day at 5:17 AM, update the distro:
17  05   *   *  * /usr/local/bin/update-distro.sh -q
```

As a result, all packages, libraries, executables, etc. are transparently updated, for the best.

However, for a proper management of modules[3], the kernel-related packages shall be special-cased; otherwise after the first kernel update no more modules can be loaded (they will expect to link to that latest installed kernel version, not to the older one being running).

A first line of defense is to force the loading of the modules known to be of interest directly at boot-time, so that they can be for sure loaded and linked to the right kernel.

This may be done by populating `/etc/modules-load.d/` with as many files listing the modules to auto-load, like in:

[3] We tried to rely on DKMS for that, but had still issues with some graphic-related modules, so we preferred managing updates by ourselves.

```
::::::::::::::
/etc/modules-load.d/for-3g-keys.conf
::::::::::::::
option
usb_wwan

::::::::::::::
/etc/modules-load.d/for-all-usb-keys.conf
::::::::::::::
# To be able to mount all kinds of USB keys:
vfat
uas
dm_crypt

::::::::::::::
/etc/modules-load.d/for-mobile-file-transfer.conf
::::::::::::::
# To be able to transfer files between this hosts and mobile phones by MTP:
nls_utf8
isofs
sr_mod
cdrom
# Maybe also: agpgart ahci wdat_wdt wmi_bmof xts

::::::::::::::
/etc/modules-load.d/for-tty-serial-on-usb.conf
::::::::::::::
# To be able to connect tty-like interfaces through a USB port:
ftdi_sio
usbserial

::::::::::::::
/etc/modules-load.d/for-usb-tethering.conf
::::::::::::::
# To enable an Internet access thanks to a smartphone via USB:
usbnet
# Implies:
#rndis_host
#cdc_ether

::::::::::::::
/etc/modules-load.d/for-vlan-support.conf
::::::::::::::
# To be able to manage VLANs:
8021q
```

This is not sufficient though (ex: one cannot anticipate all modules needed after a while); disabling the *automatic* updates of kernels is also key to reduce issues; this can be done by specifying in `/etc/pacman.conf`:

```
IgnorePkg = linux linux-headers
```

LTS (*Long Term Support*) kernels are intentionally *not* listed here, as we prefer having them regularly updated in order to minimise the risk that the base and LTS kernels belong to too close versions (as then a problem in terms of hardware support is more likely to arise at the same time with both).

At least users of NVidia graphic cards may also list there their drivers, as apparently an hardware acceleration supported at boot may be lost after some time, presumably because of an update of its drivers (knowing that the update of the kernel itself was already disabled in that case) - so, if appropriate, better be safe than sorry:

```
IgnorePkg = linux linux-headers nvidia nvidia-utils
```

See also our section about operating system support for 3D.

Updating all packages but kernel-related ones is fine, but of course the latters shall still be also updated appropriately. The best moment for that is just prior to rebooting (knowing that your Linux box never crashes, isn't it?), so for that we use (as root) our shutdown-local-host.sh script, like in:

```
$ shutdown-local-host.sh --reboot
```

The kernel packages, and possibly driver-related ones, will then only be properly updated before the host is rebooted.

Package Management

Configuration One may enable the multilib repository, which is useful to run 32-bit software on 64-bit hardware. This is useful for example if needing `wine`, knowing that its build from the AUR may fail.

To enable multilib, uncomment in `/etc/pacman.conf`:

```
[multilib]
Include = /etc/pacman.d/mirrorlist
```

then upgrade your system with `pacman -Syu`.

Package-related Commands

- to get information about a package (installed or not): `pacman -Si MY_PACKAGE`
- to list all packages explicitly installed and not required as dependencies: `pacman -Qet`
- to determine which package installed a specified file:
  - on Arch: `pkgfile SOME_FILE`; `pkgfile` itself must have been installed beforehand, with `pacman -S pkgfile`, and be updated, with `pkgfile --update` (still as root)
  - on Debian: `apt-file search SOME_FILE` after a similar initial install thanks to: `sudo apt-get install apt-file && sudo apt-file update`
  - for many distros, one may rely on the command-not-found website

See this page for many more Arch-related commands.

Interesting Packages They might be lesser known:

- `cpulimit`: the way of limiting CPU usage of a given process, for example to avoid overheat (`nice` just defines respective process priorities)
- `inotify-tools`: to be able to monitor filesystem events (ex: with `inotifywait`) from scripts
- `jq`: for command-line JSON processing (ex: `jq . myfile.json` to display it properly on a terminal)
- `mathjax`: to generate LaTeX-like images for the web
- `most`: a replacement for `more`
- `pdftk`: to transform PDF files
- `pkgfile`: to retrieve file information about packages

Post-Mortem Investigations

Sometimes a UNIX process crashes and, typically if one developed it, one wants to investigate the issue, based on a core dump produced by the operating system.

This Arch Linux article will give all relevant details.

In short, `coredumpctl list` will list all known core dumps from oldest to most recent, such as in:

```
$ coredumpctl list
TIME                          PID   UID  GID SIG     COREFILE EXE                SIZE
[...]
Tue 2021-12-21 20:53:02 CET 73873 1007 988 SIGSEGV present  [...]/bin/beam.smp 14.6M
```

The last core dump produced may be studied directly, thanks to `coredumpctl debug`, relying on `gdb` to fetch much lower-level information:

```
$ coredumpctl debug
           PID: 73873 (beam.smp)
           UID: 1007 (xxx)
           GID: 988 (users)
        Signal: 11 (SEGV)
     Timestamp: Tue 2021-12-21 20:53:01 CET (38min ago)
  Command Line: /home/xxx/Software/Erlang/Erlang-24.2/lib/erlang/erts-12.2/bin/beam.smp
    Executable: /home/xxx/Software/Erlang/Erlang-24.2/lib/erlang/erts-12.2/bin/beam.smp
 Control Group: /user.slice/user-1007.slice/session-2.scope
          Unit: session-2.scope
         Slice: user-1007.slice
       Session: 2
     Owner UID: 1007 (xxx)
       Boot ID: f8abe9473f7e4fea8ba24944e35ce7d9
    Machine ID: c9413a71e7b4498f831e2df7a08e5f33
      Hostname: xxx
       Storage: /var/lib/systemd/coredump/core.beam\x2esmp.1007.f8abe9473f7e4fea8ba2494
     Disk Size: 14.6M
```

```
       Message: Process 73873 (beam.smp) of user 1007 dumped core.

                Found module /home/xxx/Software/Erlang/Erlang-24.2/lib/erlang/erts-12.2
                Found module /home/xxx/Software/Erlang/Erlang-24.2/lib/erlang/lib/wx-2
[...]
   Stack trace of thread 74039:
   #0  0x00007f6e5461a74b __memmove_avx_unaligned_erms (libc.so.6 + 0x16374b)
   #1  0x00007f6d8a204428 n/a (iris_dri.so + 0xd12428)
   #2  0x00007f6d89733207 n/a (iris_dri.so + 0x241207)
   #3  0x00007f6d89733c97 n/a (iris_dri.so + 0x241c97)
   #4  0x00007f6d898d8b0d n/a (iris_dri.so + 0x3e6b0d)
   #5  0x00007f6d898d8bf2 n/a (iris_dri.so + 0x3e6bf2)
   #6  0x00007f6d8b2f241c n/a (/home/xxx/Software/Erlang/Erlang-24.2/lib/erlang/lib/wx
[New LWP 74039]
[New LWP 73873]
[...]
Core was generated by `/home/xxx/Software/Erlang/Erlang-24.2/lib/erlang/erts-12.2/bin/
Program terminated with signal SIGSEGV, Segmentation fault.
#0  0x00007f6e5461a74b in __memmove_avx_unaligned_erms () from /usr/lib/libc.so.6
[Current thread is 1 (Thread 0x7f6d900aa640 (LWP 74039))]
```

Then:

```
(gdb) bt
[...]
#0  0x00007f6e5461a74b in __memmove_avx_unaligned_erms () at /usr/lib/libc.so.6
#1  0x00007f6d8a204428 in  () at /usr/lib/dri/iris_dri.so
#2  0x00007f6d89733207 in  () at /usr/lib/dri/iris_dri.so
#3  0x00007f6d89733c97 in  () at /usr/lib/dri/iris_dri.so
#4  0x00007f6d898d8b0d in  () at /usr/lib/dri/iris_dri.so
#5  0x00007f6d898d8bf2 in  () at /usr/lib/dri/iris_dri.so
#6  0x00007f6d8b2f241c in ecb_glTexImage2D(ErlNifEnv*, ErlNifPid*, ERL_NIF_TERM*) (env
[...]
#29 0x00007f6d92967188 in wxe_main_loop(void*) (_unused=<optimized out>) at wxe_main.c
```

(this example was an Erlang wx/OpenGL-oriented crash)

From there, standard gdb-fu shall be sufficient to give much insight. Once done, use `q` to quit.

Quick Topics

Installing Wine Install it, once enabling multilib has been done, with: `pacman -S wine`.

When run, this may lead `wine-mono` to be auto-installed.

The pseudo-Windows filesystem is then located mostly in `~/.wine/drive_c`.

Invalid PGP Signatures in Packages This happens regularly, symptom being: `File /var/cache/pacman/pkg/xxx.pkg.tar.zst is corrupted (invalid or corrupted package (PGP signature))`.

Solution: `pacman -S archlinux-keyring` is at least often enough. Otherwise `pacman-key --populate archlinux`, or changing mirror might help.

Adding a Locale On some hosts, issues in terms of a lacking locales may be reported, like in the following:

```
bash: warning: setlocale: LC_ALL: cannot change locale (en_US.UTF-8)
```

This can be fixed by uncommenting the corresponding locale (`en_US.UTF-8` here) in `/etc/locale.gen`, and then regenerating the system locales by running (as root) `locale-gen`:

```
$ locale-gen
Generating locales (this might take a while)...
 en_US.UTF-8... done
 fr_FR.UTF-8... done
 fr_FR.ISO-8859-15@euro... done
Generation complete.
```

See Also

One may refer to our other mini-HOWTO regarding:

- Network Management
- Cybersecurity

The Ceylan-Hull section system-related section might also be of interest.

Erlang

Organisation: Copyright (C) 2021-2022 Olivier Boudeville

Contact: about (dash) howtos (at) esperide (dot) com

Creation date: Saturday, November 20, 2021

Lastly updated: Friday, January 28, 2022

Overview

Erlang is a concurrent, functional programming language available as free software; see its official website for more details.

Erlang is dynamically typed, and is executed by the BEAM virtual machine. This VM (*Virtual Machine*) operates on bytecodes and can perform Just-In-Time compilation. It powers also other related languages, such as Elixir and LFE.

Let's Start with some Shameless Advertisement for Erlang and the BEAM VM

Taken from this presentation:

> **Hint**
>
> *What makes Elixir StackOverflow's #4 most-loved language?*
> *What makes Erlang and Elixir StackOverflow's #3 and #4 best-paid languages?*
> *How did WhatsApp scale to billions of users with just dozens of Erlang engineers?*
> *What's so special about Erlang that it powers CouchDB and RabbitMQ?*
> *Why are multi-billion-dollar corporations like Bet365 and Klarna built on Erlang?*
> *Why do PepsiCo, Cars.com, Change.org, Boston's MBTA, and Discord all rely on Elixir?*
> *Why was Elixir chosen to power a bank?*
> *Why does Cisco ship 2 million Erlang devices each year? Why is Erlang used to control 90% of Internet traffic?*

Installation

Erlang can be installed thanks to the various options listed in these guidelines.

Building Erlang from the sources of its latest stable version is certainly the best approach; for more control we prefer relying on our custom procedure.

For a development activity, we recommend also specifying the following options to our `conf/install-erlang.sh` script:

- `--doc-install`, so that the reference documentation can be accessed locally (in `~/Software/Erlang/Erlang-current-documentation/`); creating a bookmark pointing to the module index, located in `doc/man_index.html`, would most probably be useful

- `--generate-plt` in order to generate a PLT file allowing the static type checking that applies to this installation (may be a bit long and processing-intensive, yet it is to be done once per built Erlang version)

Run `./install-erlang.sh --help` for more information.

Once installed, ensure that `~/Software/Erlang/Erlang-current-install/bin/` is in your PATH (ex: by enriching your `~/.bashrc` accordingly), so that you can run `erl` (the Erlang interpreter) from any location, resulting a prompt like:

```
$ erl
Erlang/OTP 24 [erts-12.1.5] [source] [64-bit] [smp:8:8] [ds:8:8:10] [async-threads:1]

Eshell V12.1.5  (abort with ^G)
1>
```

Then enter `CTRL-C` twice in order to come back to the (UNIX) shell.

Congratulations, you have a functional Erlang now!

To check from the command-line the version of an Erlang install:

```
$ erl -eval '{ok, V} = file:read_file( filename:join([code:root_dir(), "releases", erl
24.2
```

Ceylan's Language Use

Ceylan users shall note that most of our related developments (namely Myriad, WOOPER, Traces, LEEC, Seaplus, Mobile, US-Common, US-Web and US-Main) depart significantly from the general conventions observed by most Erlang applications:

- notably because of their reliance on parse transforms, by default they rely on our own build system based on GNU make (rather than on rebar3)
- they tend not to rely on OTP abstractions such as `gen_server`, as WOOPER offers OOP (*Object-Oriented Programming*) ones that we prefer

Using the Shell

If it is as simple to run `erl`, we prefer, with Ceylan settings, running `make shell` in order to benefit from a well-initialized VM (notably with the full code path of the current layer and the ones below).

Refer then to the shell commands, notably for:

- `f/1`, used as `f(X).` in order to *forget* a variable `X`, i.e. to remove the binding of this variable and be able to (re)assign it afterwards
- `rr/{1,2,3}` (ex: used as `rr(Path).`) to *read records* and have them available on the shell; for example, to be able to use the records defined by xmerl:

```
1> rr(code:lib_dir(xmerl) ++ "/include/xmerl.hrl").
```

See also the JCL mode (for *Job Control Language*) to connect and interact with other Erlang nodes.

About Security

- one should not encrypt messages directly with a key pair (ex: with RSA, only messages up to around 200 bytes long can be encrypted): one should encrypt only a *symmetric key* (generated by a cryptographically-safe random algorithm) that is then used to encrypt one's message(s); ensure an Encrypt-Then-Authenticate scheme to prevent padding oracle attacks (and a secure-compare algorithm for the *Message Authentication Code* verification to prevent timing attacks); using libsodium should make mistakes using the standard crypto primitives less error-prone; see the enacl Erlang binding for that; for more information, refer to the corresponding thread

- relevant sources of information:

  - books:

    * `Cryptography Engineering: Design Principles and Practical Applications`
    * `Practical Cryptography`

  - the Security Working Group of the EEF (*Erlang Ecosystem Foundation*)

More Advanced Topics

Metaprogramming Metaprogramming is to be done in Erlang through **parse transforms**, which are user-defined modules that transform an AST (for *Abstract Syntax Trees*, an Erlang term that represents actual code; see the Abstract Format for more details) into another AST that is fed afterwards to the compiler.

See also:

- this introduction to parse transforms
- Ceylan-Myriad's support for metaprogramming

Improper Lists A proper list is created from the empty one (`[]`, also known as "nil") by appending (with the `|` operator, a.k.a. "cons") elements in turn; for example `[1,2]` is actually `[1 | [2 | []]]`.

However, instead of enriching a list from the empty one, one *can* start a list with any other term than `[]`, for example `my_atom`. Then, instead of `[2|[]]`, `[2|my_atom]` may be specified and will be indeed a list - albeit an improper one.

Many recursive functions expect proper lists, and will fail (typically with a function clause) if given an improper list to process (ex: `lists:flatten/1`).

So, why not banning such construct? Why even standard modules like `digraph` rely on improper lists?

The reason is that improper lists are a way to reduce the memory footprint of some datastructures, by storing a value of interest instead of the empty list.

Indeed, as explained in this post, a (proper) list of 2 elements will consume:

- 1 list cell (2 words of memory) to store the first element and a pointer to second cell

- 1 list cell (2 more words) to store the second element and the empty list

For a total of 4 words of memory (so, on a 64-bit architecture, it is 32 bytes).

As for an improper list of 2 elements, only 1 list cell (2 words of memory) will be consumed to store the first element and then the second one.

Such a solution is even more compact than a pair (a 2-element tuple), which consumes 2+1 = 3 words. Accessing the elements of an improper list is also faster (one handle to be inspected vs also an header to be inspected).

Finally, for sizes expressed in bytes:

```
1> system_utils:get_size([2,my_atom]).
40

2> system_utils:get_size({2,my_atom}).
32

3> system_utils:get_size([2|my_atom]).
24
```

See also the 1, 2 pointers for more information.

Everyone shall decide on whether relying on improper lists is a trick, a hack or a technique to prohibit.

Post-Mortem Investigations Erlang programs may fail, and this may result in mere (Erlang-level) crashes (the VM detects an error, and reports information about it, possibly in the form of a crash dump) or (sometimes, quite infrequently though) in more brutal, lower-level core dumps (the VM crashes as a whole, like any faulty program run by the operating system); this last case happens typically when relying on faulty NIFs.

Erlang Crash Dumps If experiencing "only" an Erlang-level crash, a `erl_crash.dump` file is produced in the directory whence the executable (generally `erl`) was launched. The best way to study it is to use the `cdv` (refer to crash-dump viewer) tool, available, from the Erlang installation, as `lib/erlang/cdv`[4].

Using this debug tool is as easy as:

```
$ cdv erl_crash.dump
```

Then, through the wx-based interface, a rather large number of Erlang-level information will be available (processes, ports, ETS tables, nodes, modules, memory, etc.) to better understand the context of this crash and hopefully diagnose its root cause.

Core Dumps In the worst cases, the VM will crash like any other OS-level process, and generic (non Erlang-specific) tools will have to be used. Do not expect to be pointed to line numbers in Erlang source files anymore!

Refer to our general section dedicated to core dumps for that.

[4]Hence, according to the Ceylan-Myriad conventions, in `~/Software/Erlang/Erlang-current-install/lib/erlang/cdv`.

Language Bindings

The two main approaches in order to integrate third-party code to Erlang are to:

- interact with it as if it was another Erlang node; we defined Ceylan-Seaplus for that purpose
- directly link the current Erlang VM to this code, through NIF; it can be done manually, or may be automatised thanks to nifty; this can be especially useful for larger APIs (ex: SDL)

Language Implementation

Message-Passing: Copying vs Sharing Knowing that, in functional languages such as Erlang, terms ("variables") are immutable, why could not they be shared between local processes when sent through messages, instead of being copied in the heap of each of them, as it is actually the case with the Erlang VM?

The reason lies in the fact that, beyond the constness of these terms, their life-cycle has also to be managed. If they are copied, each process can very easily perform its (concurrent, autonomous) garbage collections. On the contrary, if terms were shared, then reference counting would be needed to deallocate them properly (neither too soon nor never at all), which, in a concurrent context, is bound to require locks.

So a trade-off between memory (due to data duplication) and processing (due to lock contention) has to be found and at least for most terms (excepted larger binaries), the sweet spot consists in sacrificing a bit of memory in favour of a lesser CPU load. Solutions like persistent_term may address situations where more specific needs arise.

Just-in-Time Compilation This long-awaited feature, named *BeamAsm* and whose rationale and history have been detailed in these articles, has been introduced in Erlang 24 and shall transparently lead to increased performances for most applications.

Static Typing Static type checking can be performed on Erlang code; the usual course of action is to use Dialyzer - albeit other solutions like Gradualizer exist.

A few statically-typed languages can operate on top of the Erlang VM, even if none has reached yet the popularity of Erlang or Elixir (that are dynamically-typed).

In addition to the increased type safety that statically-typed languages permit (possibly applying to sequential code but also to inter-process messages), it is unsure whether such extra static awareness may also lead to better performances (especially now that the standard compiler supports JIT).

Intermediate Languages To better discover the inner workings of the Erlang compilation, one may look at the eplaypen online demo (whose project is here) and/or at the Compiler Explorer (which supports the Erlang language among others).

Both of them allow to read the intermediate representations involved when compiling Erlang code (BEAM stage, erl_scan, preprocessed sources, abstract code, Core Erlang, Static Single Assignment form, BEAM VM assembler opcodes, x86-64 assembler generated by the JIT, etc.).

Micro-Cheat Sheet

To avoid having to perform a lookup in the documentation:

- Erlang indices start at `1`, except the ones of the `array` module that are zero-based
- for tuples of unknown number of elements:
  - setting an element is to be done with `setelement(positive_index(), tuple(), term()) -> tuple()`
  - extracting an element is to be done with `element(positive_index(), tuple()) -> term()`

(no need for the `erlang` module to be explicitly specified, as both functions are auto-imported)

Erlang Resources

- the reference is the Erlang official website
- for teaching purpose, we would dearly recommend Learn You Some Erlang for Great Good!; many other high-quality Erlang books exist as well; one may also check the Erlang track on Exercism
- in addition to the module index mentioned in the Erlang Installation section, using the online search and/or Erldocs may also be convenient
- the Erlang community is known to be pleasant and welcoming to newcomers; one may visit the Erlang forums, which complement the erlang-questions mailing list (use this mirror in order to search through the past messages of this list)
- for those who are interested in parse transforms (the Erlang way of doing metaprogramming), the section about The Abstract Format is essential (despite not being well known)
- to better understand the inner workings of the VM: The Erlang Runtime System, a.k.a. "the BEAM book", by Erik Stenman
- BEAM Wisdoms, by Dmytro Lytovchenko

About 3D

Contact: about (dash) howtos (at) esperide (dot) com

Creation date: Saturday, November 20, 2021

Lastly updated: Wednesday, February 2, 2022

As usual, these information pertain to a GNU/Linux perspective.

Cross-Platform Game Engines

The big three are Godot, Unreal Engine and Unity3D.

Godot

Godot is our personal favorite engine, notably because it is free software (released under the very permissive MIT license).

See its official website and its asset library.

Godot (version 3.4.1) will not be able to load FBX files that reference formats like PSD or TIF and/or of older versions (ex: FBX 6.1). See for that our section regarding format conversions.

Installation On Arch Linux: `pacman -Sy godot`.

Use Godot logs are stored per-project; ex: `~/.local/share/godot/app_userdata/my-test-project/logs` past log files are kept once timestamped. They tend not to have interesting content.

A configuration tree lies in `.config/godot`, a cache tree in `~/.cache/godot`.

Unreal Engine

Another contender is the Unreal Engine, a C++ game engine developed by Epic Games; we have not used it yet.

Its licence is meant to induce costs only when making large-enough profits.

See its official website and its marketplace.

Assets Purchased assets may be used in one's own shipped products (source) and apparently at least usually no restrictive terms apply.

Assets not created by Epic Games can be used in other engines unless otherwise specified (source).

Unity3D

Unity is most probably the cross-platform game engine that is the most popular.

Regarding the licensing of the engine, various plans apply, depending notably on whether one subscribes as an individual or a team, and on one's profile, revenue and funding.

See its official website and its asset store.

Unity may be installed at least in order to access its asset store, knowing that apparently an asset purchased in this store may be used with any game

engine of choice. Indeed, for the standard licence, it is stipulated in the EULA legal terms that:

Licensor grants to the END-USER a non-exclusive, worldwide, and perpetual license to the Asset to integrate Assets only as incorporated and embedded components of electronic games and interactive media and distribute such electronic game and interactive media.

So, in legal terms, an asset could be bought in the Unity Asset Store and used in Godot, for example - provided that its content can be used there technically without too much effort/constraints (this may happen with prefabs, specific animations, materials or shaders, conventions in use, etc.).

Installation Unity shall now be obtained thanks to the Unity Hub.

On Arch Linux it is available through the AUR, as an AppImage; one may thus use: `yay -Sy unityhub`.

Then, when running (as a non-priviledged user) `unityhub`, a Unity account will be needed, then a licence, then a Unity release will have to be added in order to have it downloaded and installed for good, covering the selected target platforms (ex: Linux and Windows "Build Supports").

We rely here on the Unity version 2021.2.7f1.

Additional information: Unity3D on Arch.

Configuration Configuring Unity so that its interface (mouse, keyboard bindings) behave like, for example, the one of Blender, is not natively supported.

Running Unity Just execute `unityhub`, which requires signing up and activating a licence.

Troubleshooting The log files are stored in `~/.config/unity3d`:

- Unity Editor: `Editor.log` (the most interesting one)
- Unity Package Manager: `upm.log`
- Unity Licensing client: `Unity.Licensing.Client.log`

If the editor is stuck (ex: when importing an asset), one may use as a last resort kill-unity3d.sh.

In term of persistent state, beyond the project trees themselves, there are:

- `~/.config/UnityHub/` and `~/.local/share/UnityHub/`
- `~/.config/unity3d/` and `~/.local/share/unity3d/`

(nothing in `~/.cache` apparently)

Unity Assets Once ordered through the Unity Asset Store, assets can be downloaded through the `Window -> Package Manager` menu, by replacing, in the top `Packages` drop-down, the `In Project` entry by the `My Assets` one. After having selected an asset, use the `Download` button at the bottom-right of the screen.

Then, to gain access to such downloaded assets, of course the simplest approach is to use the Unity editor; this is done by creating a project (ex: `MyProject`), selecting the aforementioned menu option (just above), then clicking on `Import` and selecting the relevant content that will end up in clear form in your project, i.e. in the UNIX filesystem with their actual name and content, for example in `MyProject/Assets/CorrespondingAssetProvider/AssetName`. We experienced reproducible freezes when importing resources.

Yet such Unity packages, once downloaded (whether or not they have been imported in projects afterwards) are files stored typically in the `~/.local/share/unity3d/Asset Store-5.x` directory and whose extension is `.unitypackage`.

Such files are actually `.tar.gz` archives, and thus their content can be listed thanks to:

```
$ tar tvzf Foobar.unitypackage
```

Inside such archives, each individual package resource is located in a directory whose name is probably akin to the checksum of this resource (ex: `167e85f3d750117459ff6199b79166fd`)[5]; such directory generally contains at least 3 files:

- `asset`: the resource itself, renamed to that unique checksum name, yet containing its exact original content (ex: the one of a Targa image)
- `asset.meta`: the metadata about that asset (file format, identifier, timestamp, type-specific settings, etc.), as an ASCII, YAML-like, text
- `pathname`: the path of that asset in the package "virtual" tree (ex: `Assets/Foo/Textures/baz.tga`)

When applicable, a `preview.png` file may also exist.

Some types of content are Unity-specific and thus may not transpose (at least directly) to another game engine. This is the case for example for materials or prefabs (whose file format is relatively simple, based on YAML 1.1).

Tools like AssetStudio (probably Windows-only) strive to automate most of the process of exploring, extracting and exporting Unity assets.

Meshes are typically in the FBX (proprietary) file format, that can nevertheless be imported in Blender and converted to other file formats (ex: gltF 2.0); see blender import and blender convert for that.

3D Data

File Formats

They are designed to store 3D content (scenes, nodes, vertices, normals, meshes, textures, materials, animations, skins, cameras, lights, etc.).

glTF We prefer to rely on the open, well-specified, modern glTF 2.0 format in order to perform import/export operations.

It comes in two forms:

[5] Yet no checksum tool among `md5sum`, `sha1sum`, `sha256sum`, `sha512sum`, `shasum`, `sha224sum`, `sha384sum` seems to correspond; it must a be a different, possibly custom, checksum.

- either as `*.gltf` when JSON-based, possibly embedding the actual data (vertices, normals, textures, etc.) as ASCII base64-encoded content, or referencing external files
- or as `*.glb` when binary; this is the most compact form, and the one that we recommend especially

See also the glTF 2.0 quick reference guide, the related section of Godot and this standard viewer of predefined glTF samples.

This (generic) online glTF viewer proved lightweight and convenient notably because it displays errors, warnings and information regarding the glTF data that it decodes.

Collada The second best choice that we see is Collada (`*.dae` files), an XML-based counterpart (open as well, yet older and with less validating facilities) to glTF.

FBX, OBJ, etc. Often, assets can be found as FBX of OBJ files and thus may have to be converted (typically to glTF), which is never a riskless task. FBX comes in two flavours: text-based (ASCII) or binary, see this retro-specification for more information.

In General Refer to blender import in order to handle the most common 3D file formats, and the next section about conversions.

The `file` command is able to report the version of at least some formats; for example:

```
# Means FBX 7.3:
$ file foobar.fbx
foobar.fbx: Kaydara FBX model, version 7300
```

Too often, some tool will not be able to load a file and will fail to properly report why. When suspecting that a binary file (ex: a FBX one) references external content either missing or in an unsupported format (ex: PSD or TIFF?), one may peek at their content without any dedicated tool, directly from a terminal, like in:

```
$ strings my_asset.fbx | sort | uniq | grep '\.'
```

This should list, among other elements, the paths that such a binary file is embedding.

Conversions

Due to the larger number of 3D file formats and the role of commercial software, interoperability regarding 3D content is poor and depends on many versions (of tools and formats).

Recommended Option: Relying on Blender Using blender import is the primary solution that we see: a content, once imported in Blender, can be saved in any of the supported formats.

Yet this operation may fail, for example on "older" FBX files, whose FBX version (ex: 6.1) is not supported by Blender ("*Version 6100 unsupported, must be 7100 or later*") or by other tools such as Godot. See also the Media Formats supported by Blender.

Workaround #1: Using Autodesk FBX Converter The simpler approach seems to download the (free) Autodesk FBX Converter and to use wine to run it on GNU/Linux. Just install then this converter with: `wine fbx20133_converter_win_x64.exe`.

A convenient alias (based on default settings, typically to be put in one's `~/.bashrc`) can then be defined to run it:

```
$ alias fbx-converter-ui="$HOME/.wine/drive_c/Program\ Files/Autodesk/FBX/FBX\ Convert
```

Conversions may take place from, for example, FBX 6.1 (also: 3DS, DAE, DXF, OBJ) to a FBX version in: 2006, 2009, 2010, 2011, 2013 (i.e. 7.3 - of course the most interesting one here), but also DXF, OBJ and Collada, with various settings (embedded media, binary/ASCII mode, etc.).

An even better option is to use directly the command-line tool `bin/FbxConverter.exe`, which the previous user interface actually executes. Use its `/?` option to get help, with interesting information.

For example, to update a file in a presumably older FBX into a 7.3 one (that Blender can import):

```
$ cd ~/.wine/drive_c/Program\ Files/Autodesk/FBX/FBX\ Converter/2013.3/bin
$ FbxConverter.exe My-legacy.FBX newer.fbx /v /sffFBX /dffFBX /e /f201300
```

We devised the update-fbx.sh script to automate such an in-place FBX update.

Unfortunately, at least on one FBX sample taken from a Unity package, if the mesh could be imported in Blender, textures and materials were not (having checked `Embed media` in the converter or not).

Workaround #2: Relying on Unity Here the principle is to import a content in Unity (the same could probably be done with Godot), and to export it from there.

Unity does not allow to export for example FBX natively, however a package for that is provided. It shall be installed first, once per project.

One shall select in the menu `Window -> Package Manager`, ensure that the entry `Packages:` points to `Unity Registry`, and search for `FBX Exporter`, then install it (bottom right button).

Afterwards, in the `GameObject` menu, an `Export to FBX` option will be available. Select the `Binary` export format (not `ASCII`) if wanting to be compliant with Blender.

Samples

Here are a few samples of 3D content (useful for testing):

- glTF, notably glTF 2.0; direct: .gltf Buggy example, .glb Fish example (also: a simple cube)
- DAE; direct: Duck example (also: a simple cube)
- FBX; direct: Stylized character
- OBJ
- IFC; direct: Basic house (requires the BlenderBIM add-on for BIM support in Blender)

Asset Providers

Usually, for one's creation, much multimedia artwork has to be secured: typically graphical assets (ex: 2D/3D geometries, animations, textures) and/or audio ones (ex: music, sounds, speech syntheses, special effects).

Instead of creating such content by oneself (not enough time/interest/skill?), it may be more relevant to rely on specialised third-parties.

Hiring a professional or a freelance is then an option. This is of course relatively expensive, involves more efforts (to define requirements and review the results), longer, but it is to provide exactly the artwork that one would like.

Another option is to rely on specialised third-party providers that **sell non-exclusive licences for the content they offer**.

These providers can be either direct **content producers** (companies with staffs of modellers), or **asset aggregators** (marketplaces which federate the offers of many producers of any size) that are often created in link to a given multimedia engine. An interesting point is that assets purchased in these stores generally can be used in any technical context, hence are not meant to be bound to the corresponding engine.

Nowadays, much content is available, in terms of theme/setting (ex: Medieval, Science-Fiction, etc.), of nature (ex: characters, environments, vehicles, etc.), etc. and the overall quality/price ratio is rather good.

The main advantages of these marketplaces is that:

- they favor the competition between content providers: the clients can easily compare assets and share their opinion about them
- they generalised simple, standard, unobtrusive licensing terms; ex: royalty free, allowing content to be used as they are or in a modified form, not limited by types of usage, number of distributed copies, duration of use, number of countries addressed, etc.; the general rule is that much freedom is left to the asset purchasers provided that they use for their own projects (rather than for example selling the artwork as they are)

The main content aggregators that we spotted are (roughly by decreasing order of interest, based on our limited experience):

- the Unity Asset Store, already discussed in the Unity Assets section; websites like this one allow to track the significant discounts that are regularly made on assets
- the UE Marketplace, i.e. the store associated to the Unreal Engine; in terms of licensing and uses:
  - this article states that *When customers purchase Marketplace products, they get a non-exclusive, worldwide, perpetual license to download, use, copy, post, modify, promote, license, sell, publicly perform, publicly display, digitally perform, distribute, or transmit your product's content for personal, promotional, and/or commercial purposes. Distribution of products via the Marketplace is not a sale of the content but the granting of digital rights to the customer.*
  - this one states that *Any Marketplace products that have not been created by Epic Games can be used in other engines unless otherwise specified.*
  - this one states that *All products sold on the Marketplace are licensed to the customer (who may be either an individual or company) for the lifetime right to use the content in developing an unlimited number of products and in shipping those products. The customer is also licensed to make the content available to employees and contractors for the sole purpose of contributing to products controlled by the customer.*
- itch.io
- Turbosquid
- Free3D
- CGtrader
- ArtStation
- Sketchfab
- 3DRT
- Reallusion
- Arteria3D
- the GameDev Market (GDM)
- the Game Creator Store

Many asset providers organise interesting discount offers (at least -50% on a selection of assets, sometimes even more for limited quantities) for the Black Friday (hence end of November) or for Christmas (hence mid-December till the first days of January).

Modelling Software

Blender

Blender is a very powerful open-source 3D toolset.

Blender (version 3.0.0) can import FBX files of version at least 7.1 ("7100"). See for that our section regarding format conversions.

We recommend the use our Blender scripts in order to:

- import conveniently various file formats in Blender, with `blender-import.sh`
- convert directly on the command-line various file formats (still thanks to a non-interactive Blender), with `blender-convert.sh`

Wings3D

Wings3D is a nice, Erlang-based, free software subdivision modeler.

It can be installed on Arch Linux, from the AUR, as `wings3d`.

Other Tools

Draco

Draco is an open-source library for compressing and decompressing 3D geometric meshes and point clouds.

It is intended to improve the storage and transmission of 3D graphics; it can be used with glTF, with Blender, with Compressonator, or separately.

A `draco` AUR package exists, and results notably in creating the `/usr/lib/libdraco.so` shared library file.

Even once this package is installed, when Blender exports a mesh, a message like the following is displayed:

```
'/usr/bin/3.0/python/lib/python3.10/site-packages/libextern_draco.so' does
not exist, draco mesh compression not available, please add it or create
environment variable BLENDER_EXTERN_DRACO_LIBRARY_PATH pointing to the folder
```

Setting the environment prior to running Blender is necessary (and done by our `blender-*.sh` scripts:

```
$ export BLENDER_EXTERN_DRACO_LIBRARY_PATH=/usr/lib
```

but not sufficient, as the built library does not bear the expected name.

So, as root, one shall fix that once for all:

```
$ cd /usr/lib
$ ln -s libdraco.so libextern_draco.so
```

Then the log message will become:

```
'/usr/lib/libextern_draco.so' exists, draco mesh compression is available
```

F3D

f3d (installable from the AUR) is a fast and minimalist VTK-based 3D viewer.

Such a viewer is especially interesting to investigate whether a tool failed to properly export a content or whether it is the next tool that actually failed to properly import, and to gain another chance to have relevant error messages.

OpenGL Corner

Conventions

Code snippets will corresponds to the OpenGL/GLU APIs as they are exposed in Erlang, in the gl and glu modules respectively.

These translate easily for instance in the vanilla C GL/GLU implementations. As an example, gl:ortho/6 (`6` designating here the arity of that function, i.e. the number of the arguments that it takes) corresponds to its C counterpart, glOrtho.

The reference pages for OpenGL (in version 2.1) can be browsed here.

The mentioned tests will be Ceylan-Myriad ones, typically located here.

Basics

- OpenGL is a **software interface to graphics hardware**, i.e. an API of around 150 functions (version 1.1)
- OpenGL concentrates on **hardware-independent 2D/3D rendering**; no commands for performing window-related tasks or obtaining user input are included; for example frame buffer configuration is done outside of OpenGL, in conjunction with the windowing system
- OpenGL offers only **low-level primitives** organised through a pipeline in which vertices are assembled into primitives, then to fragments, and finally to pixels in the frame buffer; as such OpenGL is a building-block for higher-level engines (ex: like Godot)
- OpenGL is a **procedural** (function-based, not object-oriented) **state machine** comprising a larger number of variables defined within a given OpenGL state (named *OpenGL context*; comprising vertex coordinates, textures, frame buffer, etc.); said otherwise, relatively to an OpenGL context (which is often implicit), all OpenGL state variables behave like global variables; when a parameter is set, it applies and lasts as long as it is not modified; the effect of an OpenGL command may vary depending on whether certain modes are enabled (i.e. whether some state variables are set)
- so the **currently processed element** (ex: a vertex) **inherits (implicitly) the current settings of the context** (ex: color, normal, texture coordinate, etc.); this is the only reasonable mode of operation, knowing that a host of parameters apply when performing a rendering operation (specifying all these parameters would not be a realistic option); as a result, any specific parameter shall be set first (prior to triggering such an operation), and is to last afterwards (being "implicitly inherited"), until possibly being reassigned in some future

- OpenGL respects a **client/server execution model**: an application (a specific client, running on a CPU) issues commands to a rendering server (on the same host or not - see GLX; generally the server can be seen as running on a local graphic card), that executes them **sequentially and in-order**; as such, most of the calls performed by user programs are **asynchronous**: through OpenGL they are triggered by the program and return almost immediately, whereas they have not been executed yet; they have just be queued; indeed OpenGL implementations are almost always pipelined, so the rendering must be thought as primarily taking place in a background process; additional facilities like *Display Lists* allow to pipeline operations (as opposed to the default *immediate mode*), which are accumulated for processing at a later time

- state variables are mostly server-side, yet some of them are client-side; in both cases, they can be gathered in *attribute groups*, which can be pushed on, and popped from, their respective server or client attribute stacks

- OpenGL manages two types of data, handled by mostly different paths of its rendering pipeline yet that are ultimately integrated in the framebuffer through fragment-yielding rasterization:

  - geometric data (vertices, lines, and polygons)
  - pixel data (pixels, images, and bitmaps)

- vertices and normals are transformed by the **model-view** and **projection** matrices (that can be each set and transformed on a stack of their own), before being used to produce an image in the frame buffer; texture coordinates are transformed by the **texture** matrix

- textures may reside in the main, general-purpose, client, **CPU-side memory** (large and slow to access for the rendering) and/or in any auxiliary, dedicated, server-side **GPU memory** (more constrained, hence prioritized thanks to *texture objects*; and high-performance, rendering-wise)

- OpenGL has to apply any kind of transformation, linear (ex: rotation, scaling) or not (ex: translation, perspective) to geometries, for example in order to perform referential changes or rendering; each of these transformations can be represented as a 4x4 homogeneous matrix, with floating-point (homogeneous) coordinates[6]; a series of transformations can then simply be represented as a single of such matrices, corresponding to the product of the involved transformation matrices

- while this will not change anything regarding the actual OpenGL library and the computations that it performs, the conventions adopted by the OpenGL *documentation* regarding matrices are the following ones:

[6] So a 3D point is specified based on 4 coordinates: $P = \begin{pmatrix} x \\ y \\ z \\ w \end{pmatrix}$, with `w` being usually equal to `1.0` (otherwise the point can be normalised by dividing each of its coordinates by `w`, provided of course `w` is not null).
If `w` is null, then these coordinates do not specify a point but a direction.

- their in-memory representation is column-major order (even if it is unusual, at least in C; this corresponds to Fortran-like conventions), meaning that it enumerates their coordinates first per column rather than per row (and for them a vector is a *row* of coordinates), whereas tools following the row-major counterpart order, like Myriad do the opposite (and vectors are *columns* of coordinates); more clearly, a matrix like $M = \begin{bmatrix} a11 & a12 & ... & a1n \\ a21 & a22 & ... & a2n \\ ... & ... & ... & ... \\ am1 & am2 & ... & amn \end{bmatrix}$
  - will be stored with row-major conventions (ex: Myriad) as: `[ [a11, a12, ... a1n], [a21, a22, ... a2n], ..., [am1, am2, ... amn] ]`
  - whereas, with the conventions discussed, OpenGL will expect it to be stored in-memory in this order: `a11, a21, ..., am1, a21, a22, ..., am2, ..., a1n, a2n, ..., amn`, i.e. as the transpose of the previous matrix
- these OpenGL storage conventions do not tell how matrices are to be multiplied (knowing of course that the matrix product is not commutative); if following the aforementioned OpenGL *documentation* conventions, one should consider that OpenGL relies on the usual multiplication order, that is **post-multiplication**, i.e. *multiplication on the right*; this means that, if applying on a given matrix M a transformation O (ex: rotation, translation, scaling, etc.) represented by a matrix M_O, the resulting matrix will be $M' = M.M_O$ (and not $M' = M_O.M$); a series of operations O_1, then O_2, ..., then O_n will therefore translate to a matrix $M' = M_{O1}.M_{O2}.[...].M_{On}$; applying a vector $\vec{V}$ to a matrix M will result in $\vec{V'} = M.\vec{V}$
- so when an OpenGL program performs calls like first for a rotation (r), then for a scaling (s) and finally for a translation (t):

```
glRotatef(90, 0, 1, 0);
glScalef(1, 10, 1);
glTranslatef(5,10,5);
```

the current matrix M ends up being multiplied (on the right) by $M' = M_r.M_s.M_t$; when applied to a vector $\vec{V}$, still multiplying on the right results in $\vec{V'} = M.\vec{V} = M.M_r.M_s.M_t.\vec{V'}$; so the input vector $\vec{V}$ is first translated, then the result is scaled, then rotated, then transformed by the previous matrix M; as a result: **operations happen in the opposite order of their specification as calls**; said differently: one shall specify the calls corresponding to one's target series of transformations *backwards*

- considering that the OpenGL storage is done in a surprising column-major order was actually a trick so that OpenGL could rely on the (modern, math-originating) vector-as-column convention while being still compliant with its GL ancestor - which relied on the (now unusual) vector-as-row convention and on *pre-multiplication* (where we would have $M' = M_O.M$); indeed, knowing that, when transposing

matrices, $(A.B)^\top = B^\top.A^\top$, one may consider that OpenGL actually always operates on transpose elements, and thus that: (1) matrices are actually specified in row-order and (2) they are multiplied on the left (ex: $M' = M_t.M_s.M_r.M$); note that switching convention does not affect at all the computations, and that the same operations are always performed in reverse call order

- OpenGL can operate on three mutually exclusive **modes**:
  - *rendering*: the default, most common one, discussed here
  - *feedback*: allows to capture the primitives generated by the vertex processing, i.e. to establish the primitives that would be displayed after the transformation and clipping steps; often used in order to resubmit this data multiple times
  - *selection*: determines which primitives would be drawn into some region of a window (like in *feedback* mode), yet based on stacks of only user-specified "names" (so that the actual data of the corresponding primitives is not returned, just their name identifier); a special case of selection is *picking*, allowing to determine what are the primitives rendered at a given point of the viewport (typically the onscreen position of the mouse cursor, to enable corresponding interactions)

Steps for OpenGL Rendering The usual analogy to describe them is the process of **producing a photography**:

1. a set of elements (3D objects) can be placed (in terms of position and orientation) as wanted in order to compose one's scene of interest (*modelling transformations*, with world coordinates)
2. the photographer may similarly place as wanted his camera (*viewing transformations*, with camera coordinates)
3. the settings of the camera can be adjusted, for example regarding its lens / zoom factor (*projection transformations*, with window coordinates)
4. the snapshots that it takes can be further adapted before being printed, for example in terms of scaling (*viewport transformations*, with screen coordinates)

One can see that the first two steps are reciprocal; for example, moving all objects in a direction or moving the camera in the opposite one is basically the same operation. These two operations, being the two sides of the same coin, can thus be managed by a single matrix, the *model-view* one.

Finally, as mentioned, in OpenGL, operations are to be defined in reverse order. If naming M_s the matrix implementing a given step S, the previous process would be implemented by an overall matrix $M = M_4.M_3.M_2.M_1$, so that applying a vector $\vec{V}$ to M results in $\vec{V'} = M.\vec{V} = M_4.M_3.M_2.M_1.\vec{V} = M_4.(M_3.(M_2.(M_1.\vec{V})))$.

Transformations In this context, except notably the projections, most are invertible, and a composition of invertible transformations, in any combination and sequence, is itself invertible.

As mentioned, they can all be expressed as 4x4 homogeneous matrices, and their composition translates into the (orderly) product of their matrices.

Referential transitions are discussed further in this document, in the 3D referentials section.

Translations / Rotations / Scalings / Shearings

- the inverse of a **translation** of a vector $\vec{T}$ is a translation of vector $-\vec{T}$, thus: $(Mt_{\vec{T})^{-1}=Mt_{-\vec{T}}}$
- the inverse of a **rotation** of an angle θ along a vector $\vec{U}$ is a rotation of an angle $-\theta$ along the same vector, thus: $(Mr_{(}\vec{u},\theta))^{-1} = Mr_{(}\vec{u},-\theta)$
- the inverse of a **scaling** of a (non-null) factor f is a scaling of factor $1/f$, thus: $(Ms_f)^{-1} = Ms_{1/f}$; the same applies for each factor when performing a shear mapping

Reflections Symmetries with respect to an axis correspond to a scaling factor of -1 along this axis, and 1 along the other axes.

Affine Transformations An affine transformation designates all geometric transformations that preserve lines and parallelism (but not necessarily distances and angles).

They are compositions of a linear transformation and a translation of their argument.

For them $f(\lambda.x + y) = \lambda.f(x) + f(y)$.

Projections A projection defines 6 clipping planes (at least 6 additional ones can be defined).

A 3D plane is defined by 4 coordinates (ex: `(a, b, c, d)`), and a point $P = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$ will belong to such a plane iff $a.x + b.y + c.z + d = 0$.

Two kinds of projections are considered: orthographic and perspective.

Orthographic Projections

Their viewing volume is a parallelepiped, precisely a rectangular cuboid.

With them parallel lines remain parallel; see `gl:ortho/6` and `glu:ortho2D/4`.

Perspective Projections

Their viewing volume is a truncated pyramid.

They are defined based on a field of view and an aspect ratio; see `gl:frustum/6` and `glu:perspective/4`.

Viewport Transformations As for the viewport, it is generally defined with `gl:viewport/4` so that its size corresponds to the widget in which rendering will take place.

To avoid distortion, its aspect ratio must be the same as the one of the projection transformation.

Camera The default model-view matrix is an identity; the camera is situated at the origin, points down the negative Z-axis, and has an up-vector of `(0, 1, 0)`.

With Z-up conventions (like in MyriadGUI ones), this corresponds to a camera pointing downward.

Calling `glu:lookAt/9` allows to set arbitrarily one's camera (or eye) position and orientation.

In order to switch from (OpenGL) Y-up conventions to Z-up ones, another option is to rotate the initial (identity) model-view matrix along the X axis of an angle of $-\pi/2$, or to (post-)multiply the model-view matrix with:

$$M_{camera} = P_{zup \to yup} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

For example, if we want that this camera sees, in (Z-up) MyriadGUI referential, a point `P` at coordinates $P_{zup} = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$ (thus a point in its Y axis), its coordinates in the base OpenGL (Y-up) referential must be $P_{yup} = P_{zup \to yup}.P_{zup} = \begin{bmatrix} 0 \\ 0 \\ -1 \end{bmatrix}$; refer to the Computing Transition Matrices section for more information.

Mini OpenGL Glossary Terms that are more or less specific to OpenGL:

- `Accumulation buffer`: a buffer that may be used for scene antialiasing; the scene is rendered several times, each time jittered less than one pixel, and the images are accumulated and then averaged
- `Alpha Test`: to reject fragments based on their alpha coordinate; useful to reduce the number of fragments rendered through transparent surfaces
- `Context`: a rendering context corresponds to the OpenGL state and the connection between OpenGL and the system; in order to perform rendering, a suitable context must be current (i.e. bound, active for the OpenGL commands); it is possible to have multiple rendering contexts share buffer data and textures, which is specially useful when the application use multiple threads for updating data into the memory of the graphics card
- `Display list`: a series of OpenGL commands, identified by an integer, to be stored (server-side) for subsequent execution; it is defined so that it can be sent and processed more efficiently, and probably multiple times, by the graphic card (compared to doing the same in immediate mode)
- (pixel) `fragment`: two-dimensional description of elements (point, line segment, or polygon) produced by the rasterization step, before being stored as pixels in the frame buffer; also defined as: "a point and its associated information"; a fragment translates to a pixel after a process involving in turn: texture mapping, fog effect, antialiasing, tests (scissor, alpha, stencil, depth), blending, dithering, and logical operations on fragments (and, or, xor, not, etc.)

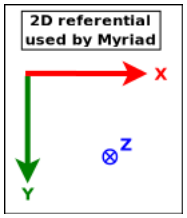
- `Evaluator`: the part of the pipeline to perform polynomial mapping (basis functions) and transform higher-level primitives (such as NURBS) into actual ones (vertices, normals, texture coordinates and colors)
- `Frame buffer`: the "server-side" pixel buffer, filled, after rasterization took place, by combinations (notably blending) of the selected fragments; it is actually made of a set of logical buffers of bitplanes: the color (itself comprising multiple buffers), depth (for hidden-surface removal), accumulation, and stencil buffers
- `GL`: *Graphics Library* (also a shorthand for *OpenGL*)
- `GLU`: *OpenGL Utility Library*, a standard part of every OpenGL implementation, providing auxiliary features (ex:image scaling, automatic mipmapping, setting up matrices for specific viewing orientations and projections, performing polygon tessellation, rendering surfaces, supporting quadrics routines that create spheres, cylinders, cones, etc.); see this page for more information
- `GLUT`, *OpenGL Utility Toolkit*, a window system-independent toolkit hiding the complexities of differing window system APIs and more complicated three-dimensional objects such as a sphere, a torus, and a teapot; its main interest was when learning OpenGL, nowadays is less used
- `GLX`: the X extension of the OpenGL interface, i.e. a solution to integrate OpenGL to X servers; see this page for more information
- `Pixel`: *Picture Element*
- `Primitive`: points, lines, polygons, images, and bitmaps
- (geometric) `Primitives`: they are (exactly) points, lines, and polygons
- `Rasterization`: the process by which a primitive is converted to a two-dimensional image
- `Scissor Test`: an arbitrary screen-aligned rectangle outside of which fragments will be discarded; useful to clear or update only a part of the viewport
- `Stencil Test`: conditionally discards a fragment based on the outcome of a selected comparison between the value in the stencil buffer and a reference value; useful to perform non-rectangular clipping
- `Texel`: *Texture Element* ; it corresponds to a `(s,t)` pair of coordinates in `[0,1]` designating a point in a texture
- `Vertex Array`: these in-memory client-side arrays may aggregate 6 types of data (vertex coordinates, RGBA colors, color indices, surface normals, texture coordinates, polygon edge flags), possibly interleaved; such arrays allow to reduce the number of calls to OpenGL functions, and also to share elements (ex: vertices pertaining to multiple faces should preferably be defined only once); in a non-networked setting, the GPU just dereferences the corresponding pointers

Refer to the description of the pipeline for further details.

Referentials

Referentials In 2D A popular convention, for example detailed in this section of the Red book, is to consider that the ordinates increase when going from the *bottom of the viewport to its top*; then for example the on-screen lower-left corner of the OpenGL canvas is `(0,0)`, and its upper-right corner is `(Width,Height)`.

As for us, we prefer the MyriadGUI 2D conventions, in which ordinates increase when going from the *top of the viewport to its bottom*, as depicted in the following figure:



Such a setting can be obtained thanks to:

```
gl:matrixMode( ?GL_PROJECTION ),
gl:loadIdentity(),

% Like glu:ortho2D/4:
gl:ortho( _Left=0.0, _Right=float( CanvasWidth ),
  _Bottom=float( CanvasHeight ), _Top=0.0, _Near=-1.0, _Far=1.0 )
```

In this case, the viewport can be addressed like a **usual (2D) framebuffer** (like provided by any classical 2D backend such as SDL) obeying the coordinate system just described: if the width of the OpenGL canvas is 800 pixels and its height is 600 pixels, then its top-left on-screen corner is `(0,0)` and its bottom-right one is `(799,599)`, and any pixel-level operation can be directly performed there "as usual". One may refer to `gui_opengl_2D_test.erl` for a full example thereof, in which line-based letters are drawn to demonstrate these conventions.

Each time the OpenGL canvas is resized, this projection matrix will have to be updated, with the same procedure yet based on the new dimensions.

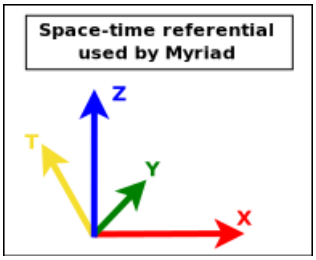
Another option - still with axes respecting the MyriadGUI 2D conventions - is to operate this time based on **normalised, definition-independent coordinates**, ranging in `[0.0, 1.0]`, like in:

```
gl:matrixMode( ?GL_PROJECTION ),
gl:loadIdentity(),

gl:ortho( _Left=0.0, _Right=1.0, _Bottom=1.0, _Top=0.0, _Near=-1.0,
  _Far=1.0 )
```

Using "stable", device-independent floats instead of integers directly accounting for pixels may be more convenient. For example a resizing of the viewport will then not require an update of the projection matrix. One may refer to `gui_opengl_minimal_test.erl` for a full example thereof.

Referentials In 3D We will rely here as well on the MyriadGUI conventions, this time for 3D (not taking specifically time into account here):



These are thus Z-up conventions (the Z axis being vertical and designating altitudes), like modelling software such as Blender.

A Tree of Referentials In the general case, either in 2D or (more often of interest here) in 3D, a given scene (a model) is made of a set of elements (ex: the model of a street may comprise a car, two bikes, a few people) that will have to be rendered from a given viewpoint (ex: a window on the second floor of a given building) onto the (flat) user screen (with suitable clipping, perspective division and projection on the viewport). Let's start from the intended result and unwind the process.

The rendering objective requires to have ultimately one's scene transformed as a whole in eyes coordinates (to obtain coordinates along the aforementioned 2D screen referential, along the X and Y axes - the Z one serving to sort out depth, as per our conventions).

For that, a prerequisite is to have the target scene correctly composed, with all its elements defined in the same (scene-global) space, in their respective position and orientation (then only the viewpoint, i.e. the virtual camera, can take into account the scene as a whole, to transform it to eye coordinates).

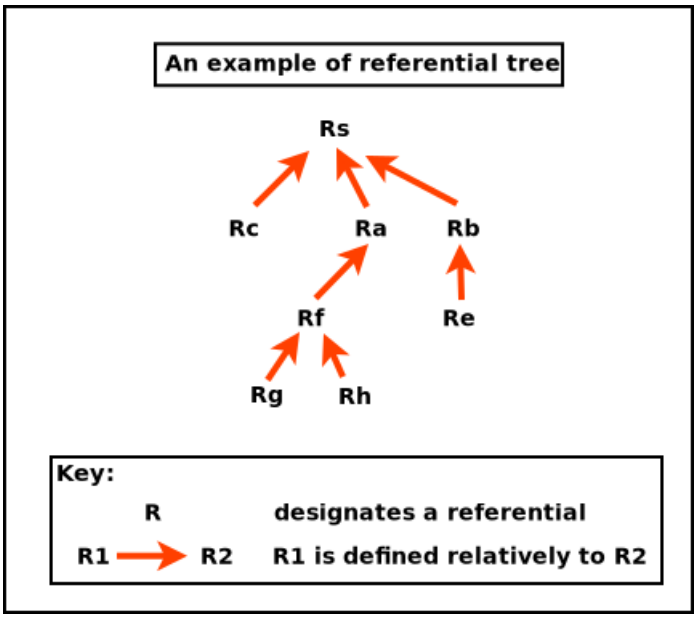
As each individual type of model (ex: a bike model) is natively defined in an abstract, local referential (an orthonormal basis) of its own, each actual model instance (ex: the first bike, the second bike) has to be specifically placed in the referential of the overall scene. This placement is either directly defined in that target space (ex: bike A is at this absolute position and orientation in the scene global referential) or relatively to a *series* of parent referentials (ex: this character rides bike B - and thus is defined relatively to it, knowing that the bike is placed relatively to the car, and that the car itself is placed relatively to the scene).

So in the general case, referentials are nested (recursively defined relatively to their parent) and form a tree[7] whose root corresponds to the referential of the overall scene, like in:

A series of model transformations has thus to be operated in order to express all models in the scene referential:

[7]This is actually named a *scene graph* rather than a *scene tree*, as if we consider the leaves of that "tree" to contain actual geometries (ex: of an abstract bike), as soon as a given geometry is instantiated more than once (ex: if having 2 of such bikes in the scene), this geometry will have multiple parents and thus the corresponding scene will be a graph.

As for us, we consider *referential trees* (no geometry involved) - a given 3D object being possibly associated to (1) a referential and (2) a geometry (independently).



`(local referential of model Rf) -> (parent referential Rd) -> (...) -> (Ra) -> (scene`

For example the hand of a character may be defined in R_h, itself defined relatively to its associated forearm in R_f up to the overall referential R_a of that character, defined relatively to the referential of the whole scene, R_s. This referential may have no explicit parent defined, meaning implicitly that it is defined in the canonical, global referential.

Once the **model** is expressed as a whole in the scene-global referential, the next transformations have to be conducted : **view** and projection. The view transformation involves at least an extra referential, the one of the camera in charge of the rendering, which is R_c, possibly defined relatively to R_s.

So a geometry (ex: a part of the hand, defined in R_f) has been transformed upward in the referential tree in order to be expressed in the common, "global" scene referential R_s, before being transformed last in the camera one, R_c.

In practice, all these operations can be done thanks to the multiplication of homogeneous 4x4 matrices, each able to express any combination of rotations, scalings/reflections/shearings, translations, which thus include the transformation of one referential into another. Their product can be computed once, and then applying a vector (ex: corresponding to a vertex) to the resulting matrix allows to perform in one go the full composition thereof, encoding all model-view transformations and even the projection as well.

Noting $P_{a\to b}$ the transition matrix transforming a vector $\vec{V_a}$ expressed in R_a into its representation $\vec{V_b}$ in R_b, we have:

$$\vec{V_b} = P_{a\to b}.\vec{V_a}$$

Thus, to express the geometry of said hand (natively defined in R_h) in camera space (hence in R_c), the following composition of referential changes[8] shall be applied:

$$P_{h\to c} = P_{s\to c}.P_{a\to s}.P_{f\to a}.P_{h\to f}.$$

So a whole series of transformations can be done by applying a single matrix - whose coordinates are now to be determined.

Computing Transition Matrices For that, let's consider an homogeneous 4x4 matrix is in the form of:

$$M = \begin{bmatrix} r_{11} & r_{12} & r_{13} & t_1 \\ r_{21} & r_{22} & r_{23} & t_2 \\ r_{31} & r_{32} & r_{33} & t_3 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

It can be interpreted as a matrix comprising two blocks of interest, R and $\vec{T}$:

$$P_{1\to 2} = \begin{bmatrix} R & \vec{T} \\ 0 & 1 \end{bmatrix}$$

with:

- R, which accounts for a 3D rotation submatrix:

$$R = \begin{bmatrix} r_{11} & r_{12} & r_{13} \\ r_{21} & r_{22} & r_{23} \\ r_{31} & r_{32} & r_{33} \end{bmatrix}$$

- $\vec{T}$, which accounts for a 3D translation vector:

$$\vec{T} = \begin{bmatrix} t1 \\ t2 \\ t3 \end{bmatrix}$$

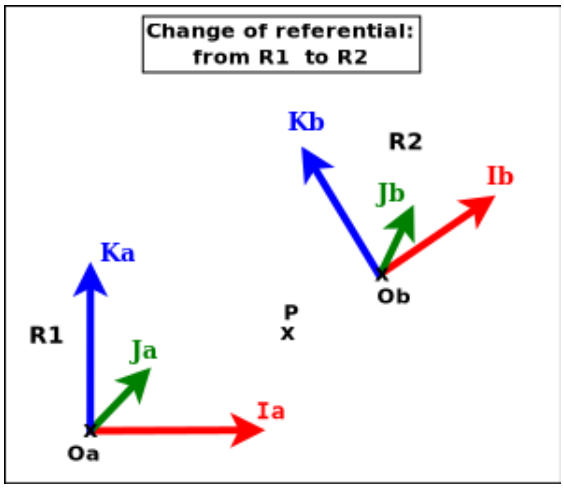
Applying a (4x4 homogeneous) point $P = \begin{Bmatrix} x \\ y \\ z \\ 1 \end{Bmatrix}$ to M yields $P' = M.P$ where P' corresponds to P once it has been (1) rotated by R and then (2) translated by $\vec{T}$ (order matters).

Let's consider now:

- two referentials (defined as orthonormal bases), R_1 and R_2; R_2 may for example be defined relatively to R_1; for a given point or vector U, U_1 will designate its coordinates in R_1 (and U_2 its coordinates in R_2)
- $P_{2\to 1}$ the (homogeneous 4x4) transition matrix from R_2 to R_1, specified first by blocks then by coordinates as:

$$P_{2\to 1} = \begin{bmatrix} R & \vec{T} \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} r_{11} & r_{12} & r_{13} & t_1 \\ r_{21} & r_{22} & r_{23} & t_2 \\ r_{31} & r_{32} & r_{33} & t_3 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

[8] Thus transformation matrices, knowing that the product of such matrices is in turn a transformation matrix.



- any (4D) point P, whose coordinates are P_1 in R_1, and P_2 in R_2

The objective is to determine $P_{2\to1}$, i.e. R and $\vec{T}$.

By definition of a transition matrix, for any point P, we have: $P_1 = P_{2\to1}.P_2$ (1)

Let's study $P_{2\to1}$ by first choosing a point P equal to the origin of R_2 (shown as `Ob` in the figure).

By design, in homogeneous coordinates, $P_2 = Ob_2 = \begin{Bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{Bmatrix}$ and applying it on (1) gives us: $P_1 = Ob_1 = \begin{Bmatrix} t1 \\ t2 \\ t3 \\ 1 \end{Bmatrix}$.

So if $Ob_1 = \begin{Bmatrix} XOb_1 \\ YOb_1 \\ ZOb_1 \\ 1 \end{Bmatrix}$, we have: $\vec{T} = \vec{T_{2\to1}} = \begin{bmatrix} XOb_1 \\ YOb_1 \\ ZOb_1 \end{bmatrix}$.

Let's now determine the r_{xy} coordinates.

Let $R_{2\to1}$ be the (3x3) rotation matrix transforming any vector expressed in R_2 in its representation in R_1: for any (3D) vector $\vec{V}$, we have $\vec{V_1} = R_{2\to1}.\vec{V_2}$ (2)

(we are dealing with vectors, not points, hence the origins are not involved here).

By choosing $\vec{V}$ equal to the $\vec{Ib}$ (abscissa) axis of R_2 (shown as `Ib` in the figure), we have $\vec{Ib_1} = R_{2\to1}.\vec{Ib_2}$

Knowing that by design $\vec{Ib_2} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$, (2) gives us:

$$\vec{Ib_1} = \begin{bmatrix} r_{11} \\ r_{21} \\ r_{31} \end{bmatrix} = \begin{bmatrix} XIb_1 \\ YIb_1 \\ ZIb_1 \end{bmatrix}$$

So the first column of the R matrix is $I\vec{b}_1$, i.e. the first axis of R_2 as expressed in R_1.

Using in the same way the two other axes of R_2 (shown as `Jb` and `Kb` in the figure), we see that:

$$R = R_{2\to1} = \begin{bmatrix} XIb_1 & XJb_1 & XKb_1 \\ YIb_1 & YJb_1 & YKb_1 \\ ZIb_1 & ZJb_1 & ZKb_1 \end{bmatrix}$$

Note

So finally the transition matrix from R_2 to R_1 is:

$$P_{2\to1} = \begin{bmatrix} R_{2\to1} & \vec{T_{2\to1}} \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} XIb_1 & XJb_1 & XKb_1 & XOb_1 \\ YIb_1 & YJb_1 & YKb_1 & YOb_1 \\ ZIb_1 & ZJb_1 & ZKb_1 & ZOb_1 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

where:

- $R_{2\to1}$ is the 3x3 rotation matrix converting vectors of R_2 in R_1, i.e. whose columns are the axes of R_2 expressed in R_1
- $\vec{T_{1\to2}} = Ob_1$ is the 3D vector of the coordinates of the origin of R_2 as expressed in R_1

This also corresponds to a matrix obtained by describing the R_2 referential in R_1, by listing first the three (4D) vector axes of R_2 then its (4D) origin, i.e. $P_{2\to1} = \left[I\vec{b}_1 \quad J\vec{b}_1 \quad K\vec{b}_1 \quad Ob_1\right]$.

As a result, from the definition of a tree of referentials, we are able to compute the transition matrix transforming the representation of a vector expressed in any of them to its representation in any of the other referentials.

For that, like in the case of the scene-to-camera transformation, transition matrices may have to be inversed, knowing that $(P_{2\to1})^{-1} = P_{1\to2}$ (since by definition $P_{2\to1}.P_{1\to2} = Id$).

A special case of interest is, for the sake of rendering, to transform, through that tree, a local referential in which a geometry is defined into the one of the camera, defining where it is positioned and aimed[9]; in OpenGL parlance, this corresponds to the *model-view* matrix (for "modelling and viewing transformations") that we designate here as M_{mv} and which corresponds to $P_{local\to camera}$.

Taking into account the last rendering step, the *projection* (comprising clipping, projection division and viewport transformation), which can be implemented as well thanks to a 4x4 matrix designated here as M_p, we see that a

[9] `gluLookAt` can define such a viewing transformation matrix, when given (1) the position of the camera, (2) a point at which it shall look, and (3) a vector specifying its up direction (i.e. where is the upward direction for the camera - as otherwise all directions orthogonal to its line of sight defined by (1) and (2) could be chosen).

single combined overall matrix $M_o = M_p.M_{mv}$ is sufficient[10] to convey in one go all transformations that shall be applied to a given geometry for its rendering.

More Advanced Topics

Shadows Determining the shadow of an arbitrary object on an arbitrary plane (representing typically the ground - or other objects) from an arbitrary light source (possibly at infinity) corresponds to performing a specific **projection**. For that, a relevant 4x4 (based on homogeneous coordinates) matrix (singular, i.e. non-invertible matrix) can be defined.

This matrix can be multiplied with the top of the model-view matrix stack, before drawing the object of interest in the shadow color (a shade of black generally).

Refer to this page for more information.

Sources of Information

The reference pages for the various versions of OpenGL are available on the Khronos official website.

Two very well-written books, strongly recommended, that are still perfectly relevant despite their old age (circa 1996):

- *The Official Guide to Learning OpenGL*: the OpenGL Red book
- *The OpenGL Reference Manual*: the OpenGL Blue book

Other elements of interest:

- FAQ for OpenGL and GLUT
- the (archived) OpenGL FAQ and Troubleshooting Guide, containing much valuable information, including regarding transformations
- About OpenGL Performance
- in French: Introduction à OpenGL et GLUT, by Nicolas Roussel
- any textbook on linear algebra

Operating System Support for 3D

Benefiting from a proper 2D/3D hardware acceleration on GNU/Linux is unfortunately not always straightforward, and sometimes brittle.

[10] In practice, for more flexibility, in OpenGL the management of the viewport, of the projection and of the model-view transformations is done separately (for example, respectively, with: `glViewport`, `glMatrixMode(GL_MODEL-VIEW)` and `glMatrixMode(GL_PROJECTION)`; so there is a matrix stack corresponding to `GL_MODEL-VIEW` and another one to `GL_PROJECTION`).

Testing

First, one may check whether such acceleration is already available by running, from the command-line, the `glxinfo` executable (to be obtained on Arch Linux thanks to the `mesa-utils` package), and hope to see, among the many displayed lines, `direct rendering: Yes`.

One may also run our display-opengl-information.sh script to report relevant information.

A final validation might be to run the `glxgears` executable (still obtained through the `mesa-utils` package), and to ensure that a window appears, showing three gears properly rotating.

Troubleshooting

If it is not the case (no direct rendering, or a GLX error being returned - typically involving any `X Error of failed request: BadValue` for a `X_GLXCreateNewContext`), one should investigate one's configuration (with `lspci | grep VGA`, `lsmod`, etc.), update one's video driver on par with the current kernel, reboot, sacrifice a chicken, etc.

If using a NVidia graphic card, consider reading this Arch Linux wiki page first.

In our case, installation could be done with `pacman -Sy nvidia nvidia-utils` but requested a reboot.

Despite package dependencies and a not-so-successful attempt of using DKMS in order to link kernel updates with graphic controller updates, too often a proper 3D support was lost, either from the boot or afterwards. Refer to our software update section for hints in order to secure the durable use of proper drivers.

3D-Related Mini-Glossary

- **HDRP**: *High Definition Render Pipeline*, a high-fidelity scriptable render pipeline, made by Unity to target **modern** (Compute Shader compatible) platforms (so HDRP is the high-end counterpart of URP)
- **IK**: *Inverse Kinematics*, the **computation of intermediary joint parameters** so that the end of the kinematic chain is at a given position and orientation; typically, if one wants the hand of a character to grasp the top of a chair, IK is used in order to determine the parameters of the character's wrist, arm, elbow, etc. that may be retained so that the hand is ultimately correctly placed on the chair (more information)
- **Material**: controls the optical properties of an object, i.e. how a 3D object appears on the screen, that is: the color of each point of the object (generally thanks to multiple texture maps, like diffusion, normal, specular, glow, etc.) and how reflective or dull its surface appears; designates, with OpenGL, a set of coefficients that define **how the lighting model interacts with the surface**; in particular, ambient, diffuse, and specular coefficients for each color component (R,G,B) are defined and applied to a surface and effectively multiplied by the amount of light of each

kind/color that strikes the surface; a final emmissivity coefficient is then added to each color component so that objects can also be light emitters

- **NURBS**: *Non-Uniform Rational B-Spline*, a mathematical model using basis splines (B-splines) that is commonly used in computer graphics for representing **curves and surfaces**, whose shape is determined by control points (more information)
- **PBR**: *Physically-Based Rendering* designates approaches to render images in a way that **models the flow of light in the real world**, for example thanks to photogrammetry; many PBR pipelines aim to achieve photorealism; in practice they often rely on the **micro-facet theory**, with specific materials (generally based on texture maps) and shaders (is also called PBS, for *Physically-Based Shading*); PBR is slowly becoming the standard for all materials
- **PSD**: *Photoshop Document*, a proprietary format for graphics with layers, masks, etc. used by Adobe Photoshop (a commercial counterpart to Gimp, Krita, etc.) often used to store textures that may still be edited as templates by the user - provided they are using Photoshop as well; however, at least to some extent, Gimp is able to edit PSD files and Krita too
- **Rigging** (or *Skeletal Animation*) consists in **controlling the deformation of a mesh** (a.k.a. a *skin*, the surface of a body) of an articulated object (typically a character) **based on a virtual inner armature** (a hierarchical set of interconnected parts, called *bones*, and collectively forming the skeleton or *rig*) in order to animate that mesh (more information)
- **Textures**: bitmaps (images) used to **skin 3D objects**, by defining the color of each point on the surface of the object in terms of texture coordinates; besides such 2D textures, 1D, 3D and 4D ones exist
- **Texture Atlas**: a texture (an image) containing a **set of separate, elementary graphic elements**, meant to be extracted thanks to texture coordinates, akin to a sprite sheet; doing so is useful to reduce the overhead that would be induced by the management of many smaller textures (more information)
- **URP**: *Universal Render Pipeline*, a prebuilt scriptable render pipeline, made by Unity that implements workflows across a range of platforms, from mobile to high-end consoles and PC (in practice URP is the low-end counterpart of HDRP)

See also the Wikipedia's glossary of computer graphics.

Network Management

Organisation: Copyright (C) 2021-2022 Olivier Boudeville

Contact: about (dash) howtos (at) esperide (dot) com

Creation date: Saturday, November 20, 2021

Lastly updated: Wednesday, January 12, 2022

Investigating Network Issues

Tools like `ping`, `traceroute`, `drill`, `arp`, etc. are invaluable.

Use ip-scan.sh to scans all IPs with any specified prefix, and ip-examine.sh to collect information about a given IP.

Use monitor-network.sh to investigate unstable connections.

Firewall Management

On GNU/Linux, some level of knowledge about `iptables` is useful, notably if exposing a computer to the Internet; note though that it is to be superseded by nftables.

One should read first the very clear Arch wiki section about iptables basic concepts.

A general rule that we retain, especially for an Internet gateway, is to drop all packets by default, and then only to accept the expected ones explicitly and carefully.

Configuration of a Gateway to the Internet Our iptables.rules-Gateway.sh script sets up an iptables configuration with various services that can be enabled (ex: for masquerading, IPTV, different kinds of servers) as an example that we hope is secure enough[11].

This script expects a settings file to be available as `/etc/iptables.settings-Gateway.sh` (this file is meant to be sourced, not executed).

An example thereof:

```
# Local firewall settings.
#
# Meant to be sourced by the iptables.rules-Gateway.sh script.

# Where firewall-related outputs will be written:
log_file=/root/.last-gateway-firewall-activation

# Local (LAN) interface, the one we trust:
#lan_if=eth1
lan_if=enp2s0

# Internet (WAN) interface, the one we distrust:

# For PPP ADSL connections:
#net_if=ppp0
```

[11] Please email us if you found otherwise! Refer to the top of this document for that.

```
# For direct connection to a set-top (telecom) box from your provider:
#net_if=eth0
net_if=enp4s0

ban_file="/etc/ban-rules.iptables"

# As the IPs banned through the ban file above are quite minimal:
use_ban_rules="true"
#use_ban_rules="false"

# IP of a test client (to avoid too many logs, selecting only related events):
#test_client_ip="xxx"

# Enabled input TCP port range for traffic from LAN to gateway:
enable_unfiltered_tcp_range="true"

# TCP unfiltered window (ex: for passive FTP and BEAM port ranges):
tcp_unfiltered_low_port=50000
tcp_unfiltered_high_port=55000

# Tells whether IPTV (TV on the Internet thanks to a box) should be allowed:
enable_iptv=false

# Tells whether a SMTP server can be used:
enable_smtp=false

# Typically a set-top box from one's ISP (defined as a possibly log match
# criteria):

# Classical example:
telecom_box="192.168.0.254"

# DHT subsection, for P2P exchanges:
# More infos: https://github.com/rakshasa/rtorrent/wiki/Using-DHT

dht_udp_port=7881

#use_dht="true"
use_dht="false"

# One may use a non-standard port:
#ssh_port=22
ssh_port=22320

smtp_port=25

# SMTPS is obsolete:
smtp_secure_port=465
```

```
# STARTTLS over SMTP is the proper way of securing SMTP:
msa_port=587

pop3_port=110

# POP3S:
pop3_secure_port=995

imap_port=143
imap_secure_port=993
```

A script to configure iptables is best integrated to systemd, see the iptables.rules-Gateway.service file for that (typically to be placed in `/etc/systemd/system`). Then one may test with:

```
$ systemctl start iptables.rules-Gateway.service
```

and enable it for good with:

```
$ systemctl enable iptables.rules-Gateway.service
```

Note that often these scripts are setup remotely, while being connected thanks to SSH from another host. Care must be taken in order not to lock oneself out of the target server, notably when updating rules (this happens quite easily). We advise to prefer the `restart` option of our iptables script in order to reduce the risk of "bricking" one's server.

Firewall-related Troubleshooting Use iptables-inspect.sh to list the currently-used firewall rules for the chains of the main tables. Like `iptables -nL --line-numbers`, it displays the number of each rule of a given chain, which allows to add/remove rules more easily, like in:

```
# Deletes the first rule of the FORWARD chain (of the 'filter' table):
# (note that all the next rules will bear a decremented number afterwards!)
$ iptables -D FORWARD 1
```

Setting environment variables (either through files such as `/etc/iptables.settings-Gateway.sh` or directly in the shell) is less error-prone; ex:

```
[...]
$ lan_if=enp2s0
$ net_if=enp4s0
$ iptables -I FORWARD -i ${lan_if} -o ${net_if} -d ${telecom_box} -j LOG
$ journalctl -kf --grep="IN=.*OUT=.*" | grep -v "SRC=${telecom_box}"
```

To further match packets, one may specify log prefixes, like in:

```
$ iptables -A INPUT -i lan.foobar -j LOG --log-prefix "[VLAN INP FOO]"
```

Note that the `LOG` target does not intercept a packet, which thus continues to flow in the next rule(s). so log targets are better defined as first rules (and thus could be inserted lastly).

As a reminder, for a given table (`filter` by default), rules may be:

- appended *at the end* of the selected chain with `-A`
- inserted either at the *beginning* of the selected chain with `-I`, or at its position N with `-I N`

See also the iptables section in the Arch wiki.

Network Troubleshooting

A few pieces of advice/information:

- be familiar with `ip link`, `ip addr` and `ip route` (generally used in that order), and `tcpdump` for the worst cases
- nowadays, many devices change their MAC address regularly, like smartphones do
- one may rely on `netctl`, and create as many profiles as found useful
- regularly inspect network-related messages (ex: with `journalctl -kf`) to detect anomalies such as `IPv4: martian source 192.168.0.49`
- interfaces may be associated to any number of IP addresses, this may create surprises
- when a network does not work properly, always consider that this device may be faulty, that cables may malfunction, and that power supplies may be culprits
- having smart switches may help a lot, to better control one's network (ex: disabling ports, checking statuses, isolating sections, etc.)
- beware to DHCP server(s) being left unnoticed; various devices may use them to get a random address and become difficult to spot
- netmasks shall not be neglected, for example in routes:

```
$ ip route add 192.168.0.0/16 dev enp4s0 scope link
$ ip route
default via 192.168.0.254 dev enp4s0 proto dhcp src 192.168.0.1 metric 1002
10.0.0.0/8 dev enp2s0 proto kernel scope link src 10.0.0.1
192.168.0.0/16 dev enp4s0 scope link
```

Here for example, in `192.168.0.0/16`, `16` corresponds to the length of *the network prefix*; the next 16 bits are left to designate hosts, whose addresses therefore range in `192.168.[0..254].[1..254]`. So `192.168.0.0/16` includes the `192.168.27.0/24` network, whereas `192.168.0.0/24` would not.

- go for VLAN only when having reached a first level of correct operation; note that some devices (ex: non-manageable switches) are not able to handle VLAN-tagged packets and may reject or overwrite this information

- in some cases, hard reboots / returns to factory settings will fix inexplicable situations; updating to latest firmware may help too (network appliances *do* have bugs as well!)
- secure spare parts (if possible all cables, fibers, devices, power supply, etc. shall exist at least in two copies, tested just after purchased): when the one in operation will fail, the outage will be quickly solved by switching element; the troubleshooting will be easier as well: replace the whole set of equipment, check that everything works again, and try to progress by dichotomy (change half of the elements, and check whether everything remains functional)
- purchase only equipment of quality, and treat it gently (ex: use an Uninterruptible Power Supply providing good-quality current)
- take notes about the operations that are performed, the detected issues and the current configuration, and put the whole in VCS
- check temperature, ventilation and prevent dust accumulation
- consider monitoring temperatures, fans, availability, performances

See Also

- Ceylan-Hull's section about scripts for network management and for firewall configuration
- A bit of Cybersecurity

A Bit of Cybersecurity

Contact: about (dash) howtos (at) esperide (dot) com

Creation date: Saturday, November 20, 2021

Lastly updated: Saturday, December 18, 2021

Pointers to various Security Topics

A goal here is to favor cryptographic privacy and authentication for data communication.

More precisely:

- for **data storage** (be it a USB key or a SSD disk), it may translate to partition encryption, typically with LUKS2 and cryptsetup
- **individual files** may be encrypted/decrypted with the help of appropriate scripts; see also Ceylan-Myriad's support for additional basic, old-school ciphering
- for the **management of credentials** such as passwords, some Ceylan-Hull scripts may be of help, including for the generation of proper passwords or for the locking of screens
- regarding **network**, each host may be protected by a relevant firewall configuration, opened ports may be checked, etc.; see also our section for firewall management
- for **webservers**, it relates to use the HTTPS protocol with proper X.509 security certificates for TLS-secured exchanges, possibly thanks to Ceylan-LEEC
- for **emails**, see the next section about OpenPGP

Securing thanks to OpenPGP

Purpose Albeit such a securing scheme may apply to at least most of the digital exchanges, in practice it is mainly used in the context of email security.

In the general case, sending an email will end up having its content stored at least on:

- your disk
- a disk of one of the servers of your Internet provider
- a disk of a server of the provider of the recipient
- the recipient's host

Possibly with intermediate organisations between the endpoint ones, possibly stored on several locations per organisation - possibly times the number of specified recipients.

Moreover many countries require by law that emails are stored by Internet providers durably (often at least for one year) - not to mention the large-scale

data harvesting that many countries perform, officially or not, with their own measures, on their own territory or on the one of others.

That's a rather large number of copies for one's private correspondence - to the point that emails sent in clear text could be mostly considered as public. Not to mention that they could also be altered in the process, at some point(s) in the chain.

Encrypting and signing are solutions to restore some privacy and safety - yours, but also the ones of the persons with whom you happen to correspond.

Technical Solution It is currently best done thanks to the OpenPGP open standard for encrypting, signing and decrypting data and communications.

GnuPG (*GNU Privacy Guard*) is a complete and free implementation of it (we suppose here that at least its 2.2.* version is used).

The corresponding command-line executable, `gpg`, can be installed on Arch Linux with: `pacman -Sy gnupg`.

Obtaining One's Keys The first step is to generate locally one's key pair, knowing that each public key is bound to a username or an e-mail address (which is our preference; having one's domain name allows to create any number of them).

A nice feature of this cryptographic scheme is that one may issue any number of keys in full autonomy and with neither consequences nor cost. So as many key pairs as notions of "unrelated identities" may be freely created.

Several settings can be chosen when generating a key, and logically the strongest keys are preferred. Yet uncommon/too recent generation algorithms and/or higher key lengths may not be supported by the various tools[12], so applying the default settings retained by gpg, or similar ones yet a bit stronger (ex: at the time of this writing, November 2021, RSA 4096 bits rather than 3072 bits) is probably the way to go (it can already be deemed safe, and will be widely supported); so the generation may be best triggered simply thanks to:

```
# For current defaults:
$ gpg --gen-key

# Or, for more control:
$ gpg --full-gen-key
```

If preferring rather paranoid settings, presumably for an extra security/durability, one can select ECC (for Elliptic-curve cryptography), with the `Sign`, `Certify` and `Authenticate` capabilities enabled (even if authentification is not used by many common protocols), and opt for the `Brainpool P-512` curve through:

```
$ gpg --full-gen-key --expert
```

[12] With "cutting-edge" settings, some tools (like Thunderbird) on your side and/or the email clients of your recipients may be unable to make use of the resulting keys, and may fail to report clearly that they actually do not support this algorithm or its parametrisation. So one may consider sticking to the reasonable gpg defaults.

In all cases, one may enter `1y` to set the initial validity duration of the generated key to one year, and already plan in one's agenda, a dozen days before the end of its validity, its renewal.

Then one may enter one's selected identity (ex: for `Real name`, one may enter `James Bond`), one's email address of interest (ex: `james.bond@mi6.org`) and possibly:

- either no specific comment (they are not normalised anyway)
- or one pointing to an authoritative source against which the public key may be verified (such as: "This public key can be verified against its reference in https://mi6.org/james-bond.pub" - provided of course such a file is to exist)

The requested passphrase only consists on a last-resort protection of the generated private key (that you should *never* transmit to *anyone*), in order to avoid that anyone accessing this file on your computer becomes directly able to fully impersonate this identity.

The operation generates a public/private key pair, and also an associated emergency revocation certificate, so that you can invalidate it at any time and for any reason:

```
gpg: key 9A60ADA4E151B8B5 marked as ultimately trusted
gpg: directory '/home/james/.gnupg/openpgp-revocs.d' created
gpg: revocation certificate stored as '/home/james/.gnupg/openpgp-revocs.d/C3987680AD9
public and secret key created and signed.

pub   brainpoolP512r1 2021-11-26 [SCA] [expires: 2022-11-26]
      C3987680AD9B79FDC6B7D25C9D60ADA5E115A8B5
uid   James Bond <james.bond@mi6.org>
```

Here `C3987680AD9B79FDC6B7D25C9D60ADA5E115A8B5` is the full fingerprint of the public key; it could be shortened to its 8, if not 4, last characters (long/short ID), yet it would expose to the forging of intentionally-colliding keys, so one should only designate a key based on its full fingerprint, and forget unsafe abbreviations.

The public key can be freely shared, whereas the private one and the revocation certificate must be equally well protected (preferably in different places).

The only well-known threats to these keys are either a flaw (intentional loophole or accidental weakness) in the cryptographic algorithms on which they rely, or the advent of major research progresses such as quantum computing. Yet it still remains possible for one to "upgrade" one's key with newer algorithms (a new key superseding an older one that is to be revoked afterwards), so as always it will be a never-ending struggle between the spear and the shield, i.e. attack and defense.

As signing and encrypting correspond to different use cases, having different keys for each may make sense. But instead of generating two unrelated keys, one shall create:

- first an infrequently-used, very-well protected (hence less accessible), signing-only "master" (primary) key of longer validity (one's actual identity)

- then at least two subkeys (deriving from the previous one, yet autonomous) may be of use:
  - one for everyday encrypting; a proper subkey has already been automatically created and used by gnupg
  - an extra one for everyday signing: such a subkey may be created with a sufficient lifespan so that past signatures can be durably verified

These "derived" subkeys are meant to change more frequently, to be able to be revoked independently, and thus are safer to expose in less secure systems.

Use `gpg --edit-key` and `addkey` in order to add a subkey to a key, and refer to this section to export the subkey.

See also these very relevant Debian guidelines for further information about subkey management.

Where are the keys, and how to backup them? The full gpg state is stored by default in its `~/.gnupg/` tree.

One may notably notice in it:

- the private keys, whose extension is `.key` and whose security is of course of paramount importance
- the revocation certificates, whose extension is `.rev`, in order to revoke one's corresponding key pair (as important as the related private key)
- certificate revocation lists, to consider that the corresponding certificates are valid yet shall *not* be trusted
- the sets of keys ("rings") containing the public keys that have been transmitted to you, gathered according to the level of trust that you dedicated to them

The public keys are usually given a `.pub` extension[13].

Even if a backup of one's key pair could be made by creating and encrypting an archive of this gpg filesystem tree, a far better solution is to use its integrated procedure, as the structure of its internal state may change from a version/platform of gpg to another. So the best course of action is to use the following command in order to generate a backup of a key pair in a standard, durable form:

```
$ gpg -o $(date '+%Y%m%d')-full-key-backup-for-james.bond-at-mi6.org.gpg --export-secr
```

This will produce a half-kilobyte file containing the full key pair, whose type is:

```
20211126-full-key-backup-for-james.bond-at-mi6.org.gpg: OpenPGP Secret Key Version 4,
```

[13] Other common extensions are `.gpg` (for encrypted content and also standard signatures), `.asc` (for clear-text signatures and other ASCII content), and `.sig` (for detached signatures).

Of course, so that it may be used in the future, this backup of (notably) the private key should *not* be encrypted with that same key.

Specifying in filenames the email address may be avoided, in the sense that rather than having multiple keys (ex: as many as email accounts), it is often more convenient to have a single key supporting multiple names/addresses (see the section about subkey below); so:

```
# If using fingerprints and potentially having multiple registered email
# accounts,just focusing on their common identity:
#
$ gpg -o $(date '+%Y%m%d')-full-key-backup-for-james.bond.gpg --export-secret-keys C3
```

A backup of the revocation certificate shall be done as well (knowing that by design it is not password-protected, and thus having access to this certificate is sufficient to be able to kill your key), preferably in a different location as the role of this certificate is to serve as an urgent safety measure should the private key be lost (non-emergency revocations should be performed thanks to the more adapted and informative `--generate-revocation` option instead).

For long-term auxiliary storage, such a backup can be printed (on paper), possibly thanks to Paperkey (installed on Arch with `pacman -Sy paperkey`). For example:

```
# To print directly:
gpg --export-secret-key my_key_fingerprint | paperkey | lpr

# To store first (less secure):
gpg --export-secret-key my_key_fingerprint | paperkey --output my_key_fingerprint.asc
```

Such exports are ASCII texts, but they can also take the perhaps more convenient (and maybe less secured if having to trust one's smartphone) form of a QR code:

```
$ gpg --export-secret-key my_key_fingerprint | paperkey --output-type raw | qrencode
```

Besides key pairs, following backups shall be done:

- the known public keys, thanks to: `gpg -o $(date '+%Y%m%d')-known-public-keys.gpg --export`
- the associated level of trust (level per public key): `gpg --export-ownertrust > $(date '+%Y%m%d')-openpgp-trust.txt`

How Can Public Keys be Shared? As mentioned, public keys can be freely shared without involving any specific risk, as in practice a private key cannot be derived from its public counterpart.

So basically any means of sharing them is legit, including the least secured ones. However the point is that their recipients must be sure that they obtained the right public certificate, and not one that has been tampered with.

Indeed, any man-in-the-middle M between peers A and B able to intercept the communication of A's public key could replace it by his. B would then have

no means of detecting that it is actually relying on M's keys rather than on A's ones.

So, on top of the generation of key pairs, a safe mechanism to share public ones shall be carefully considered, to establish the authenticity of the binding between a public key and its owner. Such mechanisms exist in two forms, peer-to-peer ones, or centralised ones.

Decentralised Sharing

The Web of trust is a decentralized trust model, which - like Internet federates a large number of computer networks - is to federate trust networks.

A user may have multiple key pairs, and each of the corresponding public keys may be known of various trust networks.

The trust conceded by identity A to identity B means that A endorses the association of the public key of B with the person or entity listed in its certificate.

The goal is to enable the emergence of some level of global trust from the trust that each given identity concedes to the various identities that it knows directly.

Trust is indeed to be spread, by extending it from peer to peer (or friend to friend) in an increasingly large network of trust, typically with trust levels that decrease with the number of peers that have to be traversed in the network before reaching a given identity: you may trust friends of your friends, albeit probably a bit less than your direct friends; networks of trust may reflect that increasing risk, typically based on mean shortest distance between endpoints.

In practice, if A expresses some level of trust to B, A will digitally sign (thus with its own private key) the public certificate of B, to assess its association with the identity it embeds. This is commonly done at key signing parties (a nice way of meeting likely-minded folks as well).

Various schemes for vetting (validating in practice the identity carried by B; ex: should we request B to show their identity card, to prove they control a given domain, or any other identity/ownership proof?) and voting (to decide on the overall trust to be derived from a potentially conflicting set of peer-to-peer endorsements A1, A2, etc. about B) exist; one remains of course free to decide for oneself on which grounds one concedes trust, it is the beauty of a decentralised mode of operation.

In practice, the sharing of public certificates used to be done through SKS key servers; it is as simple as requesting gpg to send the pblic key that corresponds to the specified fingerprint (here its last 8 characters):

```
$ gpg --send-keys E115A8B5
gpg: sending key 9D60ADA5E115A8B5 to hkps://keyserver.ubuntu.com
```

Note that this sharing discloses the corresponding email address, and thus exposes it to spam.

As various issues threaten SKS-based solutions, public keys may also be sent to the Hagrid-based OpenGPG server, `keys.openpgp.org` (which is not replicated to peer servers, yet performs more verification of the issuer of registered certificates).

To do so, register first this server in your configuration:

```
$ echo "keyserver hkps://keys.openpgp.org" >> ~/.gnupg/dirmngr.conf
```

```
# Reload gpg daemon:
$ gpgconf --reload dirmngr

# Extract the public key of interest in a .pub file:
$ gpg -o $(date '+%Y%m%d')-james.bond-at-mi6.org.pub --export james.bond@mi6.org
```

This file shall be uploaded via this web page that will guide you through the verification process, i.e. sending an email to the electronic address embedded in the transmitted public key in order to check that it is legit (by waiting for you to visit the URL that it generated and specified in said email).

More generally, various keyservers are looked up by gpg and thus can be considered (with different configurations regarding federation, verification, ability to forget keys, etc.).

Afterwards anyone will be able to search for such key:

```
$ gpg --search-keys james.bond@mi6.org
gpg: data source: https://keys.openpgp.org:443
(1)     James Bond <james.bond@mi6.org>
          512 bit ECDSA key 9A60ADA4E151B8B5, created: 2021-11-26
```

Of course checking that only one matches is returned is important to detect spoofing attempts.

Specifying your OpenPGP fingerprint in your email footers offers little interest, as your recipients cannot be sure that such incoming emails have not been tampered with.

So ultimately one will have either to trust such a decentralised scheme, or to trust a central authority like discussed next.

Centralised Sharing

A centralized trust model is based on a Public Key Infrastructure (PKI, usually based on the X.509 standard), which relies exclusively on a Certificate Authority (CA), or more often a hierarchy of such: a CA's certificate may itself be signed by a different CA, all the way up to a self-signed root certificate.

So a certificate chain has to be validated, knowing that tools like browsers, and operating systems alike, come with their own keystore already comprising root certificates, and regularly updating them.

These certificates are well protected, yet any compromising thereof may jeopardise their whole "subtree".

Sharing Largely

So a public certificate can be spread as widely as wanted, through key servers / PKIs, but also it should be shared through any reliable, authoritative reference of a given identity, like one's own webserver, emails, social accounts, etc.

This can be directly your public certificate (here is mine)[14] or a (shorter) fingerprint thereof (ex: the full fingerprint of my key is `DCA8E181DC3CEAF0EAE4033F9987EE77188E9BF4`).

Such public keys can be listed and then obtained respectively thanks to:

[14] Note the HTTPS protection and that it currently refers to `online.fr` rather than to `esperide.com`.

```
$ gpg --list-keys james.bond@mi6.org
pub   brainpoolP512r1 2021-11-26 [SCA] [expires: 2022-11-26]
      C3987680AD9B79FDC6B7D25C9D60ADA5E115A8B5
uid           [ultimate] James Bond <james.bond@mi6.org>

# For a binary version of the public key:
$ gpg -o james-bond.pub ---export C3987680AD9B79FDC6B7D25C9D60ADA5E115A8B5

# For an ASCII-based version (ex: suitable to register in GitHub):
$ gpg -o james-bond.pub.asc --armor --export C3987680AD9B79FDC6B7D25C9D60ADA5E115A8B5
```

What can be done with these keys? One may:

- **encrypt** a file: `gpg -r james.bond@mi6.org -e my_file_to_encrypt`; this generates a `my_file_to_encrypt.gpg` file
- **sign** a file, with three possibilities:
  - `--sign` / `-s` to generate a file containing both the input file (wrapped in an OpenPGP packet) and the signature
  - `--clear-sign` to generate a file containing both the input file (verbatim, expected to be a text file) and the signature
  - `--detach-sign` / `-b` to only generate a file containing said signature; so the input file will be needed in this mode to verify that signature; this possibility is useful when distributing content (ex: binaries), so that the intended public can check the signature if wanted
- **decrypt** and possibly in the same movement **check the signature** of a file: `gpg -d my_file_to_decrypt.gpg` (everything will be output to the standard stream)
- **verify** a signature: see the `--verify` option for the 3 types of signatures
- **verify** signed emails:
  - import the public key of the sender: `gpg --search-keys dr.no@foobar.org`
  - determine whether it is valid and, more importantly, deserving trust (is it the right public key?); if yes; sign it with `gpg --edit-key dr.no@foobar.org`
- **import** keys (yours or not) in your email client; if using a (recent) Thunderbird, no plugin is needed, but the local gpg rings will *not* be used by Thunderbird; refer to this documentation
- **encrypt** and/or **sign** emails

A Link With Decentralized Identifiers

The use of key pairs in the absence of a certificate authority directly relates to Decentralized Identifiers (DIDs), a class of universal solutions (not depending on any context/organisation, and able to be recognized by any) with which anyone can create one's (globally unique) identifiers that remain in one's full control: one freely issues them, they remain valid as long as their issuer wishes (as none but their creator itself can revoke them), and (for example unlike mere UUIDs) they can be cryptographically verified by anyone.

No external central authority applies to such identifiers, which cannot reveal personal information unless decided by their issuer and thus sole controller.

In practice, although other solutions could maybe be considered, it involves, like discussed in the previous sections, generating on one's own at least a public/private key pair, to store safely the private one and to share as widely as needed the public one. Then one can sign and/or encrypt one's messages with a pretty good hope that they will remain secure for a while; such a system enables partial disclosure (as one chooses what one encrypts or signs) in full control (as all operations are driven by the private key that the issuer is the only one to control).

These decentralised identifiers, together with the principle of addressing a digital content by its fingerprint (ex: SHA1), offer a solution bringing many interesting properties and opening new possibilities to distributed systems (ex: for blockchains, a user account is often identified by the fingerprint of its associated public certificate).

Hints

- whenever useful, add the `--armor` option to use ASCII output armor, suitable for copying and pasting content in text format
- if you have multiple email accounts, thanks to `--edit-key` you can add each one of themin the same key as an identity (name), using the `adduid` command; you can then set your favourite one as primary
- to always show full fingerprints of keys, add `with-fingerprint` to your configuration file (typically `~/.gnupg/dirmngr.conf`)
- these Debian guidelines describe a robust, well-defined process for key management that may apply to most developers

See Also

- a complete, well-written tutorial, in French: Bien démarrer avec GnuPG
- other interesting usage hints, still in French
- GnuPG on Arch, for much additional information
- Network Management information

About Build Tools

Organisation: Copyright (C) 2021-2021 Olivier Boudeville

Contact: about (dash) howtos (at) esperide (dot) com

Creation date: Saturday, November 20, 2021

Lastly updated: Friday, December 17, 2021

Purpose of Build Tools

A build tool allows to automate all kinds of tasks, by **applying rules and tracking dependencies**: not only compiling, linking, etc. applications, but also checking them, generating their documentation, running and debugging them, etc.

Choice

Often build tools are tied to some programming languages (ex: Maven for Java, Rebar3 for Erlang, etc.).

Some tools are more generic by nature, like late GNU autotools, or Cmake, GNU make, etc.

For most uses, our personal preference goes to the latter. Notably all our Erlang-based developments, starting from Ceylan-Myriad, are based on GNU make.

GNU make

We recommend the reading of this essential source for reference purpose, notably the section about The Two Flavors of Variables.

Taking our Erlang developments as an example, their base, first layer, Ceylan-Myriad, relies on build facilities that are designed to be also reused and further adapted / specialised / parametrised in turn by all layers above in the stack (ex: Ceylan-WOOPER).

For that, Myriad defines three top-level makefiles:

- base build-related *variables* (settings) in GNUmakevars.inc, providing defaults that can be overridden by upper layers
- *automatic rules*, in GNUmakerules-automatic.inc, able to operate generically on patterns, typically based on file extensions
- *explicit rules*, in GNUmakerules-explicit.inc, for all specific named make targets (ex: `all`, `clean`)

Each layer references its specialisation of these three elements (and the ones of all layers below) in its own GNUmakesettings.inc file, which is the only element that each per-directory `GNUmakefile` file will have to include.

Such a system allows defining (build-time and runtime) settings and rules once for all, while remaining flexible and enabling individual makefiles to be minimalistic: beside said include, they just have to list which of their subdirectories the build should traverse (thanks to the `MODULES_DIRS` variable, see example).

See Also

asdf, an extendable version manager for various languages (Ruby, Node.js, Elixir, Erlang, etc.).

One may refer to the development section of Ceylan-Hull, or go back to the Ceylan-HOWTOs main page.

Version Control Systems: in Practice, now, Git

Organisation: Copyright (C) 2021-2022 Olivier Boudeville

Contact: about (dash) howtos (at) esperide (dot) com

Creation date: Saturday, November 20, 2021

Lastly updated: Wednesday, February 2, 2022

Overview

No real software development shall happen without the use of a VCS - standing for *Version Control System* - of some sorts, notably in order to track the versions of the source files involved and to ease the collaborative work on them.

Many solutions have been defined for this purpose (CVS, Clearcase, SVN, Mercurial, etc.), but now a single tool is the de facto standard: Git, which is a distributed version control system available as free software; refer to its website for more details.

Git Usage

Beyond the documentation relative to its general use, projects have to adopt their own set of conventions - regarding the management of branches, commits, tags, etc - based on their preferences and context.

Recommended General Conventions The ones to which we try to stick are:

- the path (including names) of files and directories should not include spaces; as separator, prefer dashes (`-`) to underscores (`_`)
- the character case shall be uniform (ex: directory names starting always or never with a capital letter)
- the language used shall be uniform (ex: only English)
- a commit message shall describe synthetically the modifications operated on the corresponding new filesystem snapshot; such a message, preferably in English, should always start with a capital letter and end with a dot; ex: "*Fixed the computation of angles.*"
- the file formats shall be, as much as possible, homogeneous, notably for text files with regard to the line terminators; either only UNIX conventions (only `LF`; preferred), or only Windows ones (`CRLF`); use `dos2unix` whenever necessary, possibly automated through a Git hook
- abbreviations are convenient (ex: `br` for branch, `co` for `checkout`, etc.); they can be defined in one's `~/.gitconfig`

Basic Operations

- **managing branches**:
  - to create a branch deriving from the current one (the current `HEAD`) and switching to it (performing its checkout, while inheriting any local changes): `git co -b my_new_branch`
  - to delete a local branch: `git branch -d my_branch`
- **managing tags**:
  - to list (local) tags: `git tag`
  - to have information about an already-existing tag: `git show my_tag`
  - to set a new annotated tag: `git tag -a foobar-version-2.4.0 -m "Release of the version 2.4.0 of Foobar."`; prefer naming tags differently from branches (ex: `foobar-version-2.4.0` rather than `foobar-2.4.0`) to spare ambiguities to Git
  - a set tag must be specifically pushed on a remote, for example: `git push origin my_tag`; all tags can be pushed with `git push --tags` (the remote can be implied)
  - to delete a tag that was not pushed: `git tag --delete my_tag`
- **determining whether a file is in VCS**, knowing that due to `.gitignore` rules, `update-index --skip-worktree`, etc. it is not always obvious:

```
# Target file is tracked iff is listed by:
$ git ls-files | grep my_file

# Or, in order to trigger an error if this target file is not tracked:
git ls-files --error-unmatch my_file
```

Managing Branches Creating branches allows to separate threads of work (while preserving their lineage) and progress concurrently. Yet often their content will have to converge ultimately; depending on the intent, two use cases can be considered, resulting in different Git uses.

Merge versus Rebase Here one may want:

- either to **integrate back a development branch** (ex: `my-feature`) **in a shared, parent one** (ex: `master`): then one shall prefer using `merge`, in order to keep separate histories and not affect the past one of the shared branch
- or to **resynchronise a development branch** (ex: `my-feature`) **on the last version of a shared branch and continue these developments**: then one shall prefer `rebase`, so that the history of the development branch contains only its own changes (less noise, linear history)

In practice, in order to transfer the changes of a branch A in a branch B:

```
$ git checkout B

# Either first case (integrate development A in master B):
$ git merge A # or: git pull A

# Or second one (resynchronise development B on master A):
$ git rebase A # or: git pull -rebase A
```

How such a last `rebase` of branch A in branch B is done? The bifurcation point of B compared to A is moved from its initial position to the current head of A, on which all changes recorded in B are applied; the resulting history of B looks like if these changes had been directly performed from the version of A designated in this rebase, and thus B can be then directly fast-forwarded to its tip, which comprises both the changes synchronised from A and, then, the ones specifically introduced in B.

More information: [1] or, in French: [2], [3], [4].

Direct Merge Sometimes, one may want to directly transfer the changes of a derivate branch B in a parent branch A. When one knows for sure that the versions in B shall be preferred in all cases to their counterparts in A (note that a classical merge is already fully able to manage fast-forwards), one may use:

```
$ git checkout A
$ git merge -X theirs B
```

No conflict should arise (source).

Common Procedures

Overcoming auto-signed SSL certificate issues To avoid, typically in a company internal setting, errors like:

```
Cloning into 'XXX'...
fatal: unable to access 'https://foo.bar.org/XX/XXX/': SSL certificate problem: self s
```

the `http.sslVerify=false` option may be used, even if it weakens the overall security.

This is typically useful initially:

```
$ git -c http.sslVerify=false clone https://foo.bar.org/XX/XXX
```

In order that the next operations (ex: future pushes) overcome too this problem for the current repository, use from within the current clone:

```
$ git config http.sslVerify false
```

Setting the right metadata for the next commits Doing so prevent from having to amend commits a posteriori.

If these information apply for all projects:

```
$ git config --global user.name "John Doe"
$ git config --global user.email john.doe@foobar.org
```

Otherwise shall be done at least on a per-project basis with:

```
$ git config user.name "John Doe"
$ git config user.email john.doe@foobar.org
```

Also `git config --global --edit` may be of use (beware to trigger a `vi` by accident...).

Performing operation on remotes with no systematic authentication Using a SSH key pair, hence with its public key declared on said remote, is a relevant approach, safer than from example using a `~/.netrc` file.

Creating an empty branch Rather than creating it from a pre-existing branch and removing all inherited content, prefer:

```
$ git checkout --orphan my_new_branch
```

(typically useful for GitHub Pages branches)

Listing differences with prior versions of a file In order to list the differences of a given file with the previous commits (precisely: of a set of pathspecs), one may use our `dif-prev.sh` script, which by default reports the differences with the last committed version. With the `--all` option, it lists all differences, until the first addition of this file.

Preventing the commit of a file in VCS that is often locally modified One should use this method:

```
$ git update-index --skip-worktree <file-list>
```

The opposite operation is:

```
$ git update-index --no-skip-worktree <file-list>
```

Listing the files managed in VCS from the current directory Use `git ls-files` to determine the files that are already managed in VCS, recursively from the current directory.

To list the untracked files (i.e. the files *not* in VCS), use `git ls-files --others`.

Reducing the size of a repository One may use our list-largest-vcs-blobs.sh script to detect any larger files that should not be in VCS (ex: should a colleague have committed by mistake a third-party archive, or unexpected data such as CSV files).

Then install BFG Repo-Cleaner:

```
$ mkdir -p ~/Software/bfg-repo-cleaner/
$ cd $_
$ mv ~/bfg-1.14.0.jar .
$ ln -s bfg-1.14.0.jar bfg.jar
# For example in ~/.bashrc:
$ alias bfg="java -jar ~/Software/bfg-repo-cleaner/bfg.jar"
```

All developers should be asked to commit their sources (git add + push), to archive their clone (ex: in a timestamped `.xz` file like `20220412-archive-clone-foobar.tar.xz`), and to wait until notified that they can create a new clone.

The repository may be then cleaned up (ex: from large, unnecessary CSV files) in isolation, with:

```
$ git clone --mirror XXX/foobar.git
$ bfg --delete-files '*.csv' foobar.git
$ cd foobar
$ git reflog expire --expire=now --all && git gc --prune=now --aggressive
$ git push
```

Then all developers shall be requested to perform a new clone and to check the fetched content (ex: with regard to the content of the last branch in which they committed).

Tools

On Most Platforms At least on UNIX, the command-line Git client (`git`) is certainly the best tool. In difficult situations, graphical tools such as `gitk` may be of help.

See also our Ceylan-Hull section about VCS-related scripts.

On Windows Tools like TortoiseGit may foster a view on the usage of Git that is a bit particular, conflating concepts or introducing extra ones (ex: a `sync` command). Apparently also at least some pulls did not reintroduce files just removed from the working directory.

More generally, cloning on a Windows host an UNIX-originating repository comprising symbolic links may induce oddities (ex: a symlink named `S` pointing to `Foobar` resulting, on a Windows clone, in a file named `S` whose content is, literally, the text `"Foobar"`, instead of the expected content of the `Foobar` file).

Another option is to use Visual Studio Code (`vscode`), which supports natively Git (provided that the command-line version is already installed). One may select `View -> SCM` (or `Ctrl-Shift-G`) for that. Clicking on the "VCS" icon (three rings links by two curves; the third from the top) displays a contextual view offering various associated operations (here based on Git).

We finally preferred using MSYS2 + Git rather than Git Bash, named "Git for Windows"; hints to speed up these tools may apply.

Inner Workings

Git stores internally every version of every file separately (not as a diff with a parent version) as a blob (an opaque binary content) identified by its (SHA1) hash.

A commit is the identifier of a tree representing the filesystem of interest at a given moment (snapshot). This tree references the files through their SHA1, similarly to a Merkle tree.

A branch is thus nothing but a pointer on a given commit, and `HEAD` designates the current branch. Git stores natively only blobs, trees and commits.

The reported differences in the content of a file or a tree are thus only recreated (established dynamically) by Git commands, they are not natively tracked.

Translations

From English to French:

- `repository` -> `dépôt`
- `to checkout` -> `extraire`
- `to commit` -> `valider`
- `a commit` -> `validation`
- `in VCS` -> `en GCL` (Gestion de Configuration Logicielle)
- `snapshot` -> `instantané` (de l'état du sous-système de fichiers géré en GCL)
- `merge` -> `fusion`
- `head` -> `tête`
- `fast-forward` -> `avancement direct`
- `fast-forwarded` -> `directement avancée`

Documentation

Many pointers exist, doing a great job in unveiling how Git is to be used.

In English, Pro GIT is surely a reference.

In French:

- introduction en français
- cours sur OpenClassrooms
- référence incontournable et conseillée : Pro GIT, notamment pour l'explication de ses rudiments puis de son fonctionnement interne, à commencer par ses objets

Documentation Generation

Organisation: Copyright (C) 2022-2022 Olivier Boudeville

Contact: about (dash) howtos (at) esperide (dot) com

Creation date: Wednesday, January 12, 2022

Lastly updated: Wednesday, January 19, 2022

Objective

We want to be able to generate, **from a single source**, at least two **documentation formats**:

- a set of **interlinked static web pages** (the most popular, flexible format)
- a single, **standalone PDF file** (convenient for offline reading, printing, etc.)

The document source shall be expressed in a simple, non-limiting, high-level syntax; in practice a rather standard, lightweight markup language.

All standard documentation elements shall be available (ex: title, tables, images, links, references, tables of content, etc.) and be customisable.

The resulting documents shall be quickly and easily generated, with proper error report, and be beautiful and user-friendly (ex: with well-configured LaTeX, with appropriate CSS, icons and features like banners, with proper rendering of equations).

Per-format overriding shall be possible (ex: to define different image sizes depending on web output or PDF one).

The whole documentation process shall be powered only by free software solutions, easily automated (ex: with Make) and suitable for version control (ex: with Git).

Our Recommended Approach

We chose to rely on the reStructuredText syntax and tools, also known as RST, a part of the Docutils project. We did not specifically rely on elements related to Python or the Sphinx toolchain.

We augmented reStructuredText with:

- a set of **make-based defines and rules** (automatic or explicit) that were aggregated in Ceylan-Myriad (see notably GNUmakerules-docutils.inc and the generate-docutils.sh generation script); this mechanism is layer-friendly, in the sense that all layers defined (directly or not) on top of Myriad are able by default to re-use these elements and to customise them if needed
- a **template** on which we rely for most documents, featuring notably a standard table (to specify usual metadata such as organisation, contact information, abstract, versions, etc.), a table of contents, conventions in terms of title hierarchy and, for the HTML output, a banner (a fixed, non-scrolling panel offering shortcuts, in the top-right corner of the page)

- a simple **tag-based system** to have the actual document markup (`*.rst`) directly generated from a higher-level source one (`*.rst.template`); in practice, if defined, only the latter element is edited by the user, and tags (such as `*_VERSION_TAG`, `*_DATE_TAG`, etc.) are automatically filled-in appropriately

Of course this website, and many others that we created, rely on this approach; as an example, one may look at the sources of the current document.

Technical Details

Rendering Mathematical Elements With the RST toolchain, the PDF output, thanks to LaTeX, offers built-in high-quality rendering of mathematical elements such as equations, matrices, etc.

By default, the HTML output does not benefit from LaTeX, and remains significantly less pleasing to the eye, and less readable.

So we complement it by MathJax, a neat open-source "*JavaScript display engine for mathematics that works in all browsers*".

It shall thus be installed once for all first. For example, on Arch Linux, as `root`, it is sufficient to execute:

```
$ pacman -Sy mathjax
```

Then, to enable the use of MathJax for a given website based on Ceylan-Myriad, run from its root (often a `doc` directory):

```
make create-mathjax-symlink
```

(this target is defined in GNUmakerules-docutils.inc; it boils down to symlinking `/usr/share/mathjax`; see also the HOWTOs corresponding makefile to properly manage this dependency afterwards, notably when deploying web content)

The list of TeX/LaTeX commands supported by MathJax may be of use.

A few examples of resulting math-related outputs can be seen for example in this section.

Title Hierarchy It must be consistent: a given type of subtitle must always be placed at the same level in the title hierarchy.

We rely on the markup conventions exposed in this demonstration file (created by David Goodger), whose source is here.

From the top-level title to the most nested ones:

- =", on top and below the title (document title)
- -, on top and below the title (document subtitle)
- =, below the title (H1)
- -, below the title (H2)
- . , below the title (H3)
- _, below the title (H4)

- `*`, below the title (H5)
- `:`, below the title (H6)
- `+`, below the title (H7)

Multi-File Documents

Targeting a Standalone Document Although they tend to be less convenient to edit, longer documents may be split in a **set of RST source files** (the Myriad documentation is an example of it; the WOOPER documentation is an example of the opposite approach, based on a single source file).

Targeting Interlinked Modular Documents In some cases, at least for the HTML output, the need is not to produce a single, large, monolithic document, but a set of interlinked ones (the present HOWTO is an example thereof) that can be browsed as separate pages.

Then a convenient approach is to define different entry points for different output formats, like, for these HOWTOs, this one for the HTML output and this one for the PDF output.

Inner Links Defining any title (ex: the `"Rendering Mathematical Elements"` one above) automatically introduces in turn a corresponding anchor, which, for the HTML output, can then be referenced from any page, for example as raw HTML (like MyPage.html#rendering-mathematical-elements, or directly from the current page as #rendering-mathematical-elements) or directly through RST in the document (ex: specified as `‘Rendering Mathematical Elements‘_`, resulting in: Rendering Mathematical Elements).

Note the light transformation (spaces becoming dashes) of the specified name once a it is translated into a legit HTML anchor.

Extra local anchors (ex: that could be named `"how to render equations"`) can also be specified anywhere in the document (ex: just before the previously mentioned title, so that it can be designated with other words), thanks to:

```
.. _‘how to render equations‘:
```

It can then be referenced from the same page as #how-to-render-equations or from another one as MyPage.html#how-to-render-equations.

Validating / Checking In addition to the verification of the messages reported when the document is built, some tools allow to perform some checks on a generated document.

Notably an online HTML page, or set of pages, can be verified by third-party tools like this one, to detect dead links.

Miscellaneous

Conversion between Markup Formats Pandoc is the tool of choice for such operations, as it often yields good results.

For example, in order to convert a page written in Mediawiki syntax, whose source content has been pasted in a `old-content-in-mediawiki.txt` file, into one that be specified in a GitLab wiki (hence in GFM markup, for *GitLab Flavored Markdown*) from a converted content, to be written in a `converted-content.gfm` file, one may use:

```
$ pandoc old-content-in-mediawiki.txt --from=mediawiki --to=gfm --standalone -o conver

# Or, for older versions of pandoc not supporting a gfm writer:
$ pandoc old-content-in-mediawiki.txt --from=mediawiki --to=markdown_github --standalo
```

Then the content in `converted-content.gfm` file can be pasted in the target GitLab wiki page.

The lists of the input and output formats supported by Pandoc and of their corresponding command-line options is specified here.

These options are also returned by: `pandoc --list-input-formats` and `pandoc --list-output-formats` (or, for older versions of pandoc, thanks to `pandoc --help`).

An input file may not be encoded in UTF-8, which can result in:

```
pandoc: Cannot decode byte '\xe9': Data.Text.Internal.Encoding.Fusion.streamUtf8: Inva
```

In this case, the actual encoding shall be determined, for example with:

```
$ file input.html
input.html: HTML document, ISO-8859 text
```

Then the encoding may be changed before calling pandoc, for example like:

```
$ iconv -f ISO-8859-1 -t utf-8 input.html | pandoc --from=html --to=markdown_github --
```

Transformation of PDF files For that, one may use the `pdftk` tool:

- to concatenate PDFs: `pdftk 1.pdf 2.pdf 3.pdf cat output 123.pdf`
- to split all pages of a PDF in as many individual files (named `pg_0001.pdf`, `pg_0002.pdf`, etc.): `pdftk document.pdf burst`

Please React!

If you have information more detailed or more recent than those presented in this document, if you noticed errors, neglects or points insufficiently discussed, drop us a line! (for that, use the contact address at the top of this document).

Ending Word

Hoping that these Ceylan-HOWTOs may be of help!