OPENSSL REVIEW

Figure 1: logo.

- ## Glossary

  [!TIP] *Italic* words means that they have their definition written in the Glossary

Word	Definition
pushed	push is a git action to add new files or changes to the current state of the project
rsa	is a cryptosystem algorithm widely used for secure data transmission
repository	a Git repository is a folder that tracks all changes made to files in your project, building history over time.
issue	a Git issue has the same meaning as in english: there is a problem in the code of project, if someone identifies an error in the project they can notify the project team of its content.

- ## Introduction to OpenSSL

  –

  ### Open-source and Open development

  Open-source is a type of software in which source code is openly published on Internet.

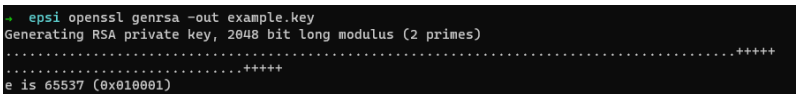
Anybody has access to it and can look at its details.
It is a relatively new kind of intelectual property. Regarding its usage, Open source branches out into :

* Free and open-source : in which its usage, modification and distribution is non-restricted.
* Under Open Source Licence : access to its source code remains public but its usage has to reference the owner and the licence. — Open development is a type of Open Source software going a step further by reviewing anybody's **request** on a part of their source code. And if it asserted as a valuable addition : it is *pushed* and added the code. Everyone can participate in development of all code bases. From reporting bugs and improvement requests to providing the solution in form of pull requests.

–

What is OpenSSL

OpenSSL is a command line tool commonly used to generate private keys and other security certificates. Private key are the most essential part of any encryption and is used for authentication during a SSL/TLS session. As an example the following commands generated this key :



this would generate a **private** *rsa* key like this one: > [!REMINDER] > In use or used private keys shouldn't ever be publicly shared!

```
-----BEGIN RSA PRIVATE KEY-----MIIEpAIBAAKCAQEAqg4wuoJr6lneLCC08dEXqmaRht184b1y2z
-----END RSA PRIVATE KEY-----
```

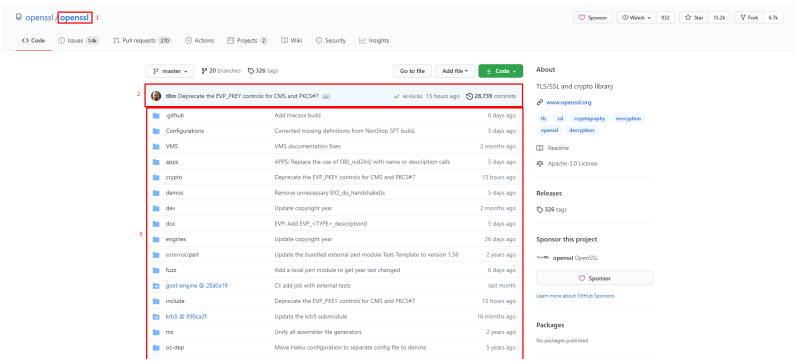
To summarize OpenSSL is a crucial tool used for most of the transport layer security structures.
As an open question : wouldn't it be strange for an security program to have its source code publicly available ?

•

Open developement

–

Github website



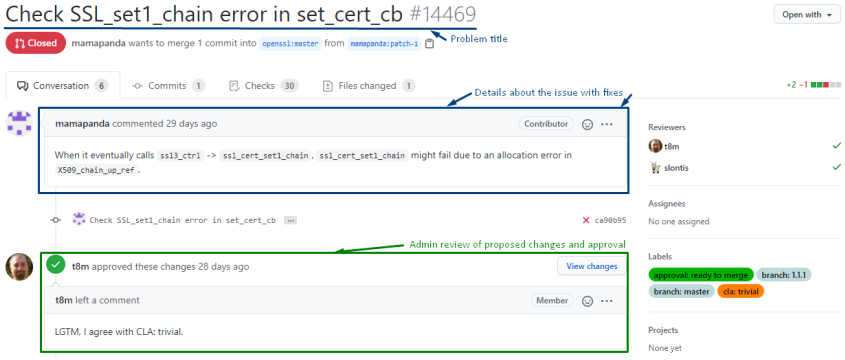
Here is the home page of the source code of OpenSSL.
On the top left [1] is the **title** of the *repository*, the project hosted on github. The core content is composed of the **latest *commit*** [2] followed by the **source code** [3] of the project.
Github offers other functionalities as shown in the multiple tabs under the *repository* name (Code, Issues, Pull Request, ...).

–

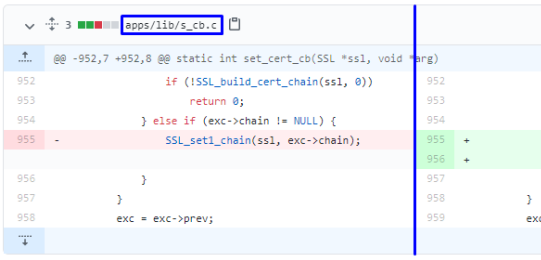
Example of pull request

A Pull Request is a an initiative from a contributor that isn't from the project team, proposing changes to the source code in order to solve an *Issue*. Pull Requests are the Open source way of submitting theses changes to the project.

Let's examine one from **mamapanda** which integrated the core of OpenSSL:



Here someone found a problem **but also** found a way to correct it.
The changes from **mamapanda** was review by someone from the OpenSSL team and approved to be added to the source code.



Let's have a look at what change **mamapanda** proposed : On the top we can see in which file the change occured apps/lib/**s_cb.c** / On the left is the old code and on the right the snippet **mamapanda** wrote to correct the *issue*. ### Technical Explanation The return of the function SSL_set1_chain() was not listened to, if an error occured in the function: the function calling SSL_set1_chain() would have no idea that there were an error. `c SSL_set1_chain(ssl, exc->chain);` So by **testing** the return and propagating it, would be a better function behavior : `c if (!SSL_set1_chain(ssl, exc->chain)) return 0;`

Take out This is a small example of a bug but even small ones could make the program crash or define a non intended behavior that malevolant individuals could **use** to jeopardize or attack the system.

There are nevertheless a great community of developpers happy to help and contribute to Open Source projects like this.

–

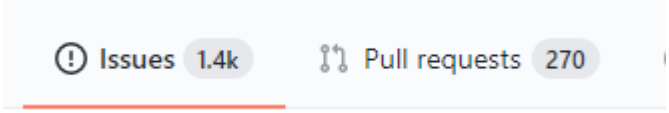
Top Contributors

OpenSSL counts more than 550 contributors in 22 years of Open Development. Some of them even wrote half a milion lines of the source code

–

Unresolved / In progress requests

There is still numerous problems and improvement suggestions of OpenSSL being reviewed and worked on to this day.



—

•

Conclusion

–

Benefits of Open developement

Companies that give Open Source access to their product can rely on a thriving community of programmers bound by a common drive to

support and improve the solution. The company can thus improve the reliability of its product, having external experts testing and looking for errors, it can also cost less in development budget because it is backed by volunteer contributors helping.

–

Take out about security and white/black hat behavior

It does comes with a few disadvantages such as being vulnerable to malicious users. Indeed having all source code freely displayed, it isn't restricted to local servers protected by firewall and encryption methods. Thus if any user finds a major issue capable of crashing or inducing unintended behavior, then it can be used to attack the unpatched versions of the software.
That being said having an entire community identifying issues and proposing changes to fix them makes it so the software is gradually becoming more secure.