

OpenSSL

Cryptography and SSL/TLS Toolkit

- Glossary

[!TIP]

Italic words means that they have their definition written in the Glossary

Word	Definition
<i>pushed</i>	push is a git action to add new files or changes to the current state of the project
<i>rsa</i>	is a cryptosystem algorithm widely used for secure data transmission
<i>repository</i>	a Git repository is a folder that tracks all changes made to files in your project, building history over time.
<i>issue</i>	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 intellectual 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 :

```
+ epsi openssl genrsa -out example.key
Generating RSA private key, 2048 bit long modulus (2 primes)
.....+++++
.....+++++
e is 65537 (0x010001)
```

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-----
MIIEpAIBAAKCAQEAqg4wuoJr6lneLCC08dEXqmaRht184b1y2zf1NXZi+EjhWpIY0RcAVmu
g8DNTp2qpftMMg8cVTXWM0aM4MEoHk1mNCqXgGmZPM6fpQWtSz8d3fxNJ1r9dU6sOdfS3pD
LcNUdbTtax6Wkd8zFfz9cM1AxUr1IgwEAVq2C8ssK00MPDauNMA6mdTAXTP3HIDnv+hFzCc
GGxoBPz03TWZ4L3PG0y3krmG+LVxbF3tehrWelJVaSxfSrnPGKts63c1BiX1yL3DZtG1q9B
4W4bZ60Bf1DrCMq5VlwyAuFCLGxSiA4BccqLtyr3YF7G8jubYTatJ3auwiyZ5d6JIiNNJzw
IDAQABAAoIBAQCXaWsZpWZQkxOuVrDFX1aj8g9A9ZRrqlJ3UrH1CoKSF78IvGIgkFQLiqfB
OMCr1PhfnLLq908dBFp3A4Sk9mU5rXKXc25tJcwFmp7JkLkXHb3UfL+P4yyVlAS9Bk8dd6N
rzp1VhbaatEhktBVz2sMP2FjmWWfjxToC06YdtZnTK9mukPofaAP5mVkt9dc8mP+q9l9ckU
iAG8nYDms1c0jhorZ5gpJbJhHC5G5dFYxuBb0rjjCaU8bayXZWCtQo2C0kZioa04xJt055/
8XzhN67yNIq0GAKvDiuLg2lEwmNzu0/69/MkFvXXwRTiTule+OURoRQWNE6AilV2BAoGBAN
Y0CClHjlMkErrtmzcvEgXueWMEabEU6rZs0iuKPPY0pNBwmDIOPiPAqI6Ui21FnC/9vBk42
9UybeqoJyTnpt9HIIdCEQ21XMThiW14P5n52+ahAm0g51JG8ouluzTX2UHKRsL5XjZA3hcxH
SrUWXD91ee1TYgdpPrvCchIbxWHzAoGBAMs83l4bRoRhmd8RaRQELtc48FBNRCKLQVfgr1k
tXcUzbZe1CMhC3wxERcbAjlw/P3eud45SL4b08s/uSAqZlU8T4NPjzbm5fHd3RGWrrj6xQy2h
n+XFRp0xq+Vt0pD3uytU00aKtbbHBSwT vzT4z430b6ukXBS1eYZBC9JnfAAB01AoGAerQXs
L3i09GoQRh3f6chJfCz7HrMqLoYsi0oSXTJ4XWKRDSzmoj6I7TrWbHSJOhpTjyFkdU2a0yY
doGY2tUwJfRNdguWLH50HZ6KRFnLacpxvWY1DazDDjEHCb2FJFJTRY4aFw9Ecsa7iIeWTiH
f6G/9RmwrjZ9GZnw+qAzshu0CgYEAx20oJVtNC4NVmmtSU7jm22+ZFK85MUq9iKF+ZlCdr/
yMgFGz1AVHHpm8ewlfUXv1lLsKEypI/DUDvqm4v9aZIJ0CG1t39ACNJJmH/j4s21wobWgG3
SoVWh9yyPcHoavqAvcn6TWAZZJK0a4bVYqx7kn9hYHlkmKJKYLowoMzkCECgYA01ES7bHWz
e0pzMxTADi7mBRj/77Uo0Uesw1T+2NvAuaUxDWpi08YLw9qbjkH6Uj349U1U3u3XDrV095K
VsCW089iLi1e3kti4Yu0fnyZv7Wsfq76rQ56S34vs1DEcYLB9D4TTD1m294t4x1spGih5g1
cMUqJNNJUK8bEL2wfnuQ==
-----END RSA PRIVATE KEY-----
```

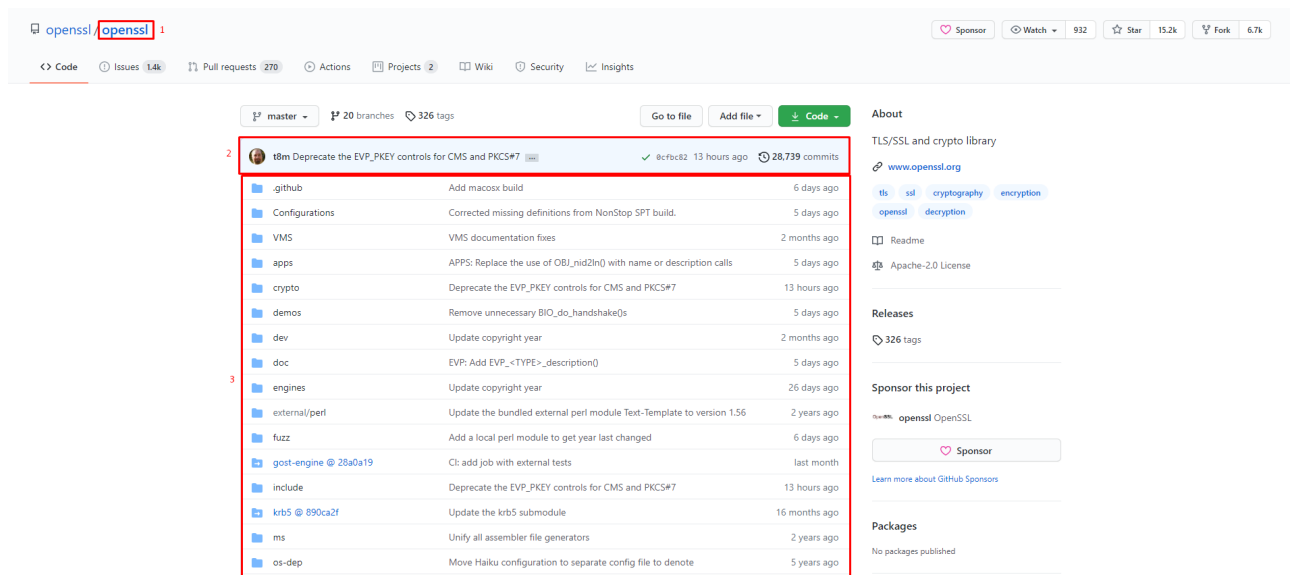
To summarize OpenSSL is a crucial tool used for most of the transport layer security structures.

Open question

: wouldn't it be strange for an security program to have its source code publicly available ?

- Open development

- Github website



Here is the home page of the source code of [OpenSSL](https://github.com/openssl/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

- **Definition and Example**

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 :

```
@@ -952,7 +952,8 @@ static int set_cert_cb(SSL *ssl, void *arg)
952         if (!SSL_build_cert_chain(ssl, 0))
953             return 0;
954     } else if (exc->chain != NULL) {
955 -        SSL_set1_chain(ssl, exc->chain);
956 +        if (!SSL_set1_chain(ssl, exc->chain))
957 +            return 0;
958     }
959     exc = exc->prev;
```

On the top we can see in which file the change occurred `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 occurred in the function: the function calling `SSL_set1_chain()` would have no idea that there were an error.

```
SSL_set1_chain(ssl, exc->chain);
```

So by **testing** the return and propagating it, would be a better function behavior :

```
if (!SSL_set1_chain(ssl, exc->chain))
    return 0;
```

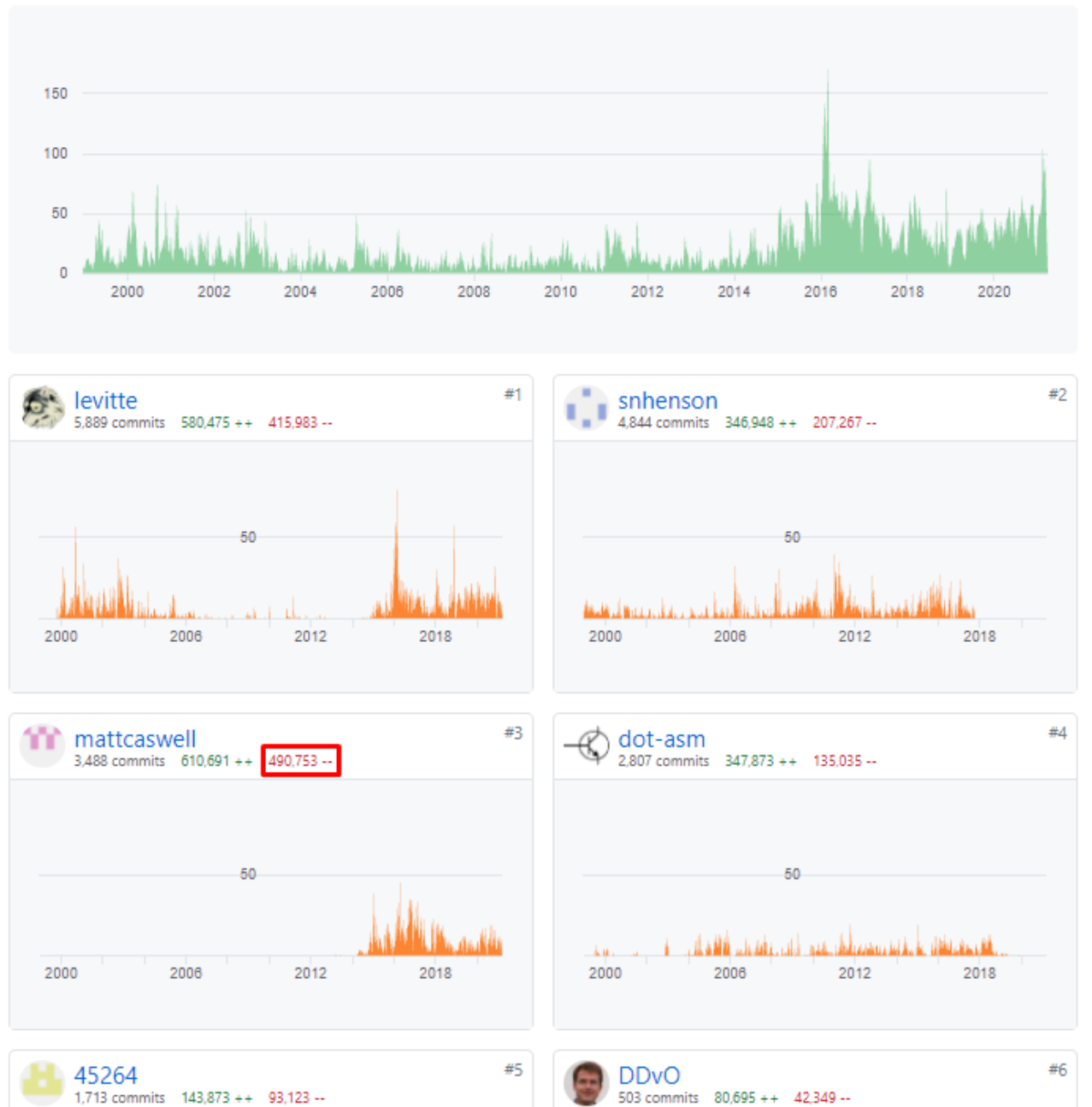
■ Take out

This is a small example of a bug but even small ones could make the program crash or define a non intended behavior that malevolent 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 million 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.