

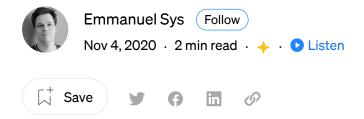






Published in FAUN Publication

You have 2 free member-only stories left this month. Sign up for Medium and get an extra one



# Foolproof Method to Not Push Unencrypted Secrets into Git

Quick fix to prevent committing secrets into your Git repository



Стр. 1 из 6 27.03.2023, 20:27

#### Photo by Stefan Steinbauer on Unsplash

## The problem

It's a frequent problem that every developer faced: committing secrets into your Git repositories.

Once a secret has been pushed to a remote repository, you are doomed to execute a gruesome procedure to clear it. The best way to deal with the problem is to prevent it entirely.

Lots of solutions exist to address the problem: <u>AWS git-secrets</u>, <u>git-secret</u> or even a dedicated <u>SonarQube plugin</u>. Apart from the manifest lack of imagination in finding a meaningful name for these solutions you sometimes only want a simple and quick fix.

### **No Brainer 5 Minutes Solution**

Most of these full-blown solution work by installing themselves as <u>Git client hooks</u>. But it's really simple to write a tailored hook for dealing with exactly what you need.

In my case, I only want to prevent unencrypted secrets from being pushed to the repository. To elaborate, I encode some secrets using <u>sops</u> and I want to check before each commit that all my secrets are properly encrypted.

These secrets all share a naming convention and live in specific folders. Writing the precommit hook is straightforward.

Стр. 2 из 6 27.03.2023, 20:27

```
#!/bin/bash
 2
 3
     # directories containing potential secrets
     DIRS="env/bel1/c1/helm_vars env/bel1/c2/helm_vars env/dev/helm_vars"
 5
 6
     bold=$(tput bold)
 7
     normal=$(tput sgr0)
 8
     # allow to read user input, assigns stdin to keyboard
10
     exec < /dev/tty</pre>
11
12
     for d in $DIRS; do
13
         # find files containing secrets that should be encrypted
         for f in $(find "${d}" -type f -regex ".*secrets.yaml"); do
14
             if ! $(grep -q "^sops:" $f); then
15
                 printf \xF0\x9F\x92\xA5 '
16
                 echo "File $f has non encrypted secrets!"
17
18
                 HAS_NON_ENCRYPTED=1
19
             fi
20
         done
21
     done
22
23
     # still allow to commit with confirmation is non encrypted secrets were found
     if [ ! -z $HAS_NON_ENCRYPTED ]; then
24
         echo
25
26
         printf '\xF0\x9F\xA4\x94 '
         read -p "${bold}Do you still want to commit?${normal} (y|Y to commit) " -n 1 -r REPLY
27
         echo
28
         if [[ ! $REPLY =~ ^[Yy]$ ]]; then
29
             echo "aborted"
30
             exit 1
31
         fi
32
33
     fi
pre-commit.sh hosted with 💙 by GitHub
                                                                                              view raw
```

You put this script in the .git/hooks/pre-commit file. If this script returns 0 the commit is authorized else it is aborted.

Let's test it. First, we check that nothing changed when all secrets are properly encrypted.

Стр. 3 из 6 27.03.2023, 20:27

```
$ echo "key: somesecrets" >> my-secrets.yaml
    $ sops -e -i my-secrets.yaml
     $ cat my-secrets.yaml
 4
     key: ENC[AES256_GCM,data:IermPQamdQoWVQE=,iv:ftvBbgqON/w9e7Q4fvH6QVs0J1fEcJBoo+OJYrgHSk8=,tag:I
 6
     sops:
 7
       kms: []
 8
      gcp_kms: []
       azure_kv: []
10
      hc_vault: []
11
12
13
     $ git add my-secrets.yaml && git commit -m "commit with encrypted secret"
14
15
     [master 00d096b] commit with encrypted secret
     1 file changed, 29 insertions(+)
16
17
     create mode 100644 my-secrets.yaml
test.sh hosted with 💙 by GitHub
                                                                                           view raw
```

No problem here. Now let's decrypt this file and try to commit it:

Стр. 4 из 6 27.03.2023, 20:27

Git Programming Security DevOps Development

Everything is working fine! No more committed secrets. Sometimes 5 minutes is enough to prevent security headache and specific later 🏂

## Sign up for FAUN

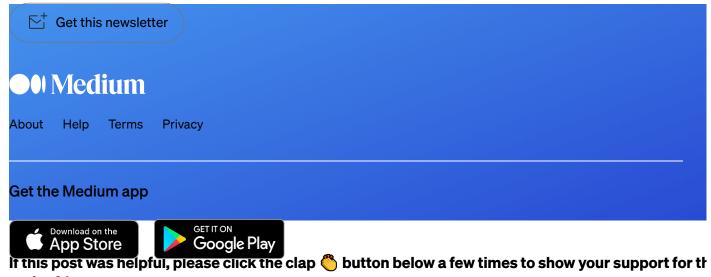
By FAUN Publication
Join FAUN today and receive similar stories each week in your inbox! Get your
Medium's largest and most followed independent DevOps publication. Join thousands of developers and DevOps
Weekly dose of the must-read tech stories, news, and tutorials.

enthusiasts. Jake a look.

Follow us on Twitter 🐔 and Facebook 🕿 and Instagram 🔯 and join our Facebook and

Стр. 5 из 6 27.03.2023, 20:27

**Linkedin** Groups to a Medium account if you don't already have one. Review our <u>Privacy Policy</u> for more information about our privacy practices.



author! |

Стр. 6 из 6 27.03.2023, 20:27