

Advanced 5

Git Hooks

EECS 201 Winter 2021

Submission Instructions

This assignment will be submitted as a repository on the [UMich GitLab server](#). Create a Project on it with the name/path `eeecs201-adv5` and add `brng` as a Reporter. The repository should have the following directory structure, starting from the repository's root:

```
/
|-- commit-msg
|-- pre-commit
|-- report.txt
```

In order to submit, you'll have to copy your hook scripts over to a repo and submit that repo.

Git Hooks

One feature of most version control systems is **hooks**. A hook is an automated script or tool that runs at various points in time. For example, you can automatically run test cases every time anyone commits code.

A slightly easier one to wire up, however, is a hook that will automatically check the spelling of your commit messages for you, letting you know if you made any mistakes. While spelling rarely counts for a class projects, it adds a nice bit of professionalism to any future work you'll share with others.

I recommend creating a temporary Git repository to play with while you test things and try to get things working.

Git stores all of its information and configuration in a folder named `.git` in the root of each project. Navigate to `.git/hooks` and rename `commit-msg.sample` to `commit-msg`. This activates the commit message hook, which runs after you write and save your commit message. Now go back to your repository, make a change, and commit it. Hmm, doesn't look like anything changed. Make another change, but this time make this your commit message (**exactly this, capitalization matters**):

```
This is a test.
```

```
Signed-off-by: Me!
Signed-off-by: Me!
```

After trying to commit, type `git status`. What happened? Go back and look at the commit hook. Do you understand what it does? Try running `git commit --no-verify` with the same commit message. Go edit the commit hook and delete the line `exit 1`. Try making a new commit with the same commit message, what happens now? What is `$1` in this script? (not sure? try adding lines like `echo $1` or `echo $(file $1)` or `echo $(cat $1)` to the hook and making commits, what happens?)

1 Automating Professionalism (5)

`aspell` is a simple command-line utility that checks spelling. Install it and play with it a little.

Write a commit message hook that checks the spelling of a commit message. Your hook **should not** prevent the commit from going through (that'd be annoying...). Your hook should print out "Spelling errors detected!" and then print out a `sorted` list of offending words, with one word per line.

Example output:

```
Spelling errors detected!  
alkdj  
dakfjll  
dklak  
ldkafjlk  
notarealword
```

Some tips

- Remember to look only at the **commit message** itself. Commit message files have "commented out" stuff with lines beginning with `#` to communicate with the user what's going on in a commit, but they aren't in the commit message itself.
- This can be a little intimidating to get started. *Try some things.* Make a bunch of garbage commits, modify the hook a little, see what happens.
- Remember that a shell script is exactly like working in a terminal. The only magic is that you've typed all the commands in advance instead of one at a time. So try some things in your terminal! Mess around until you get some commands that do what you want, then copy them to your script.
- There is **zero** need to be efficient. This hook is called rarely and operates on hundreds of bytes of text. Read the file 6 times. Write 7 temporary files. *Who cares.* The goal is not to be pretty, the goal is to work.
- Speaking of temporary files, the `/tmp` directory can be a great place to throw those. There's even a command called `mktemp` to create temporary files or directories here.

Further exploration and some gotchas:

- Take a look at some of the other hooks, are any of them useful?
- For a list of all available hooks, type `man githooks`.
- Hooks have to be marked as executable to run (`chmod +x`). The sample hooks already had the executable bit set, which is why renaming the existing sample worked above.
- Hooks can call other scripts. Because invocation of hooks is controlled by the name of the script, if you want multiple scripts to run for a single hook, you'll need to have one script named correctly that calls your other hooks.
- Git hooks need not necessarily be shell scripts; they can be any sort of executable. You could possibly implement your hooks as, for example, Python scripts (not in this assignment though).

2 Automating security (5)

When you are developing a web application, sometimes you need to access the services of some API to access things like weather information from one source or a user's Google calendar from another.

Such services tend to require the use of an *API key* that is used to authenticate the client requesting services and can be used to do things like rate limiting and tracking API use.

If someone else (say, another competing application) gets a hold of your application's API key, they could mooch off of whatever quotas that API key has.

Another security issue is when people unwittingly put private SSH keys into a repository. Recall that when you generated an SSH key it created a private and public key pair (e.g. public: `id_rsa.pub`, private: `id_rsa`.) The public key, being "public" is provided to various servers to authenticate your computer with. Your private key is what verifies that you are you: if it gets out of your hands, others can access things that have saved your public key for authorization. (This is simplifying it greatly: just know that your private key is private!).

Such things shouldn't necessarily be put onto a public Git repository being hosted somewhere (unless you actually intended for the entire internet to be able to use your key).

In this exercise you'll be writing a Git **pre-commit hook** that **stops** the commit from happening when an API key is directly in the staged code files or if a private SSH key file is staged. If your hook fails the commit, it should print out "Keys detected!" and a **sorted** list of what files are the culprits, one file on each line. **Every** offending file should have its name printed out; do **not** exit early once a key is detected.

Example output:

```
Keys detected!
example_key_assigns
example_rsa_private_key
```

Here are some things to identify each component with (these are simplified for this exercise).

API keys:

- They are a string literal enclosed by double quotes (`"`) or single quotes (`'`)
- They are a string composed of alphanumeric characters of both cases (A-Z, a-z, 0-9)
- They are being assigned via `=` to some variable whose name ends in `"key"` or `"Key"`. There can be an arbitrary amount of whitespace around the `=`

SSH private keys:

- The file's first line is `-----BEGIN OPENSSH PRIVATE KEY-----`
- The file's last line is `-----END OPENSSH PRIVATE KEY-----`

Helpful hints:

- The <https://eecs.umich.edu/courses/eecs201/files/assignments/adv5.tar.gz> archive has an example private key and API key assignments.
- You can get a list of staged files via `git diff --name-only --cached`.
- `head` and `tail` can get the first and last lines of a file.

3 Conclusion

1. Copy your hook scripts to your submission repo and commit them.
2. Create a file called `report.txt`.
3. On the first line provide an integer time in minutes of how long it took for you to complete this assignment.
4. On the second line and beyond, write down what you learned while doing this assignment. If you already knew how to do all of this, put down "N/A".
5. Add and commit this `report.txt` file. Push your repo.