{ropsec}: **R OP**erations **SEC**urity

unconf ‘18 project

📦 on GitHub

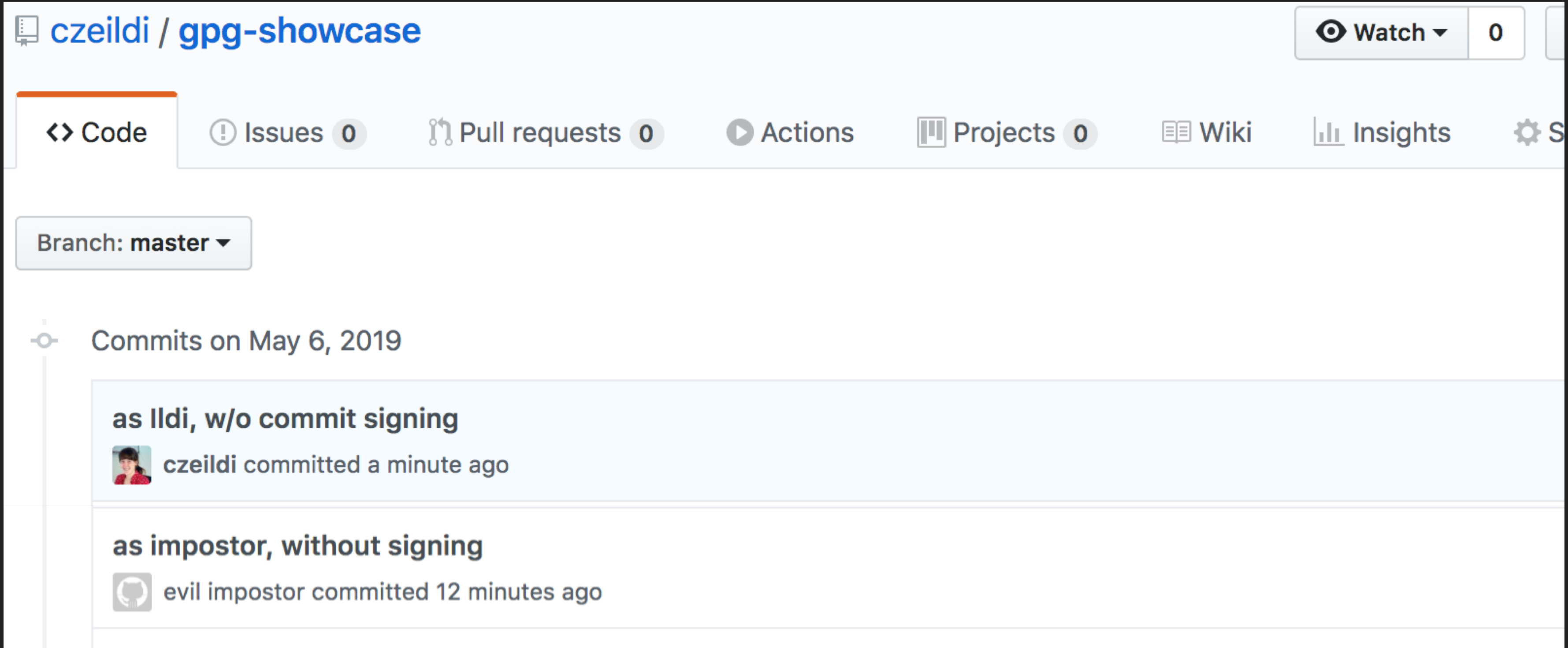
security is important ...

... but unnecessarily hard

verify **authenticity** of commits

Are you who you say you are?

without signing



czeildi / gpg-showcase

Commits on May 6, 2019

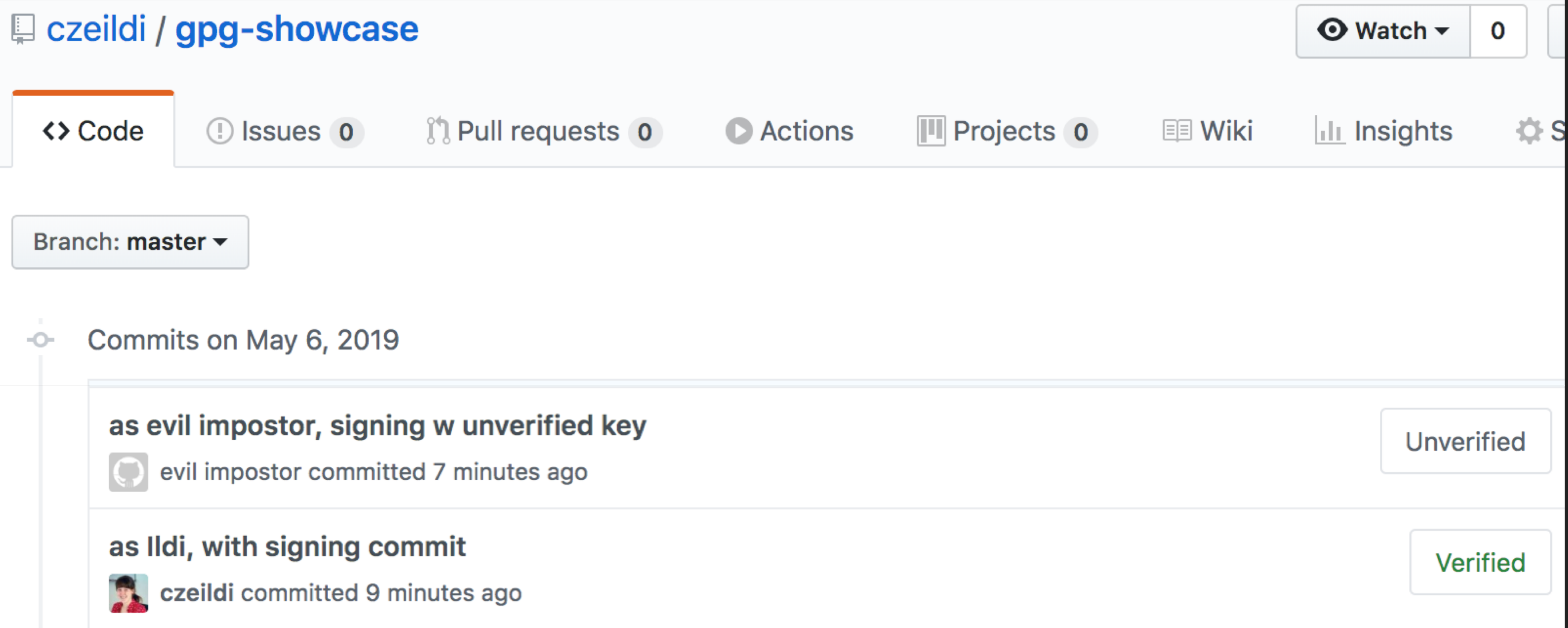
as Ildi, w/o commit signing

czeildi committed a minute ago

as impostor, without signing

evil impostor committed 12 minutes ago

with signing



Commits on May 6, 2019

as evil impostor, signing w unverified key

evil impostor committed 7 minutes ago

Unverified

as Ildi, with signing commit

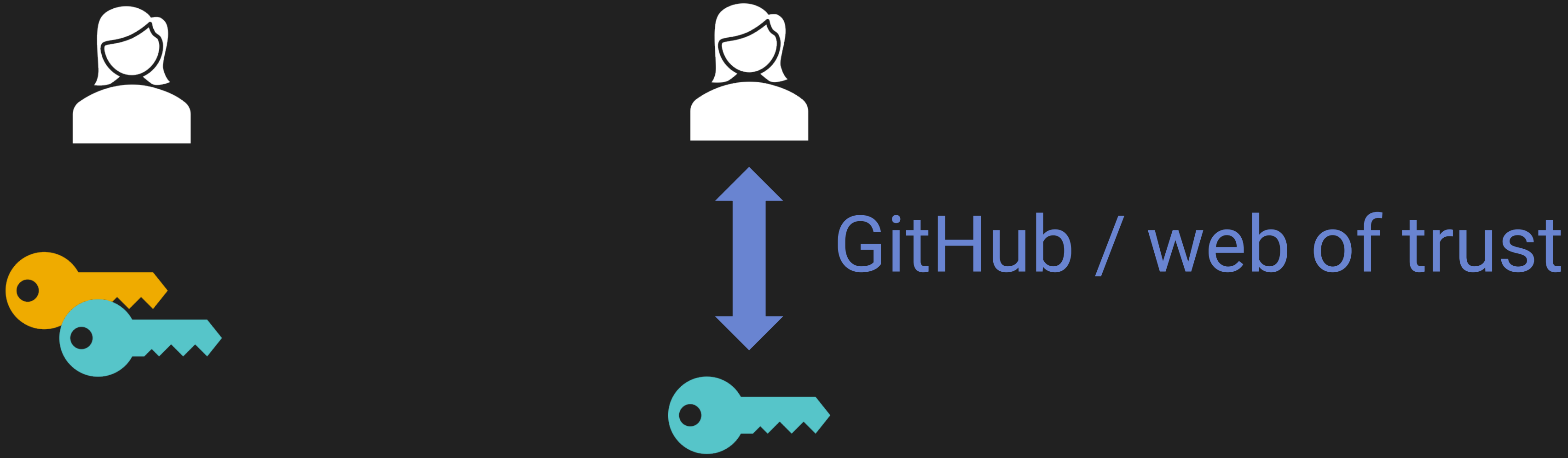
czeildi committed 9 minutes ago

Verified

@czeildi

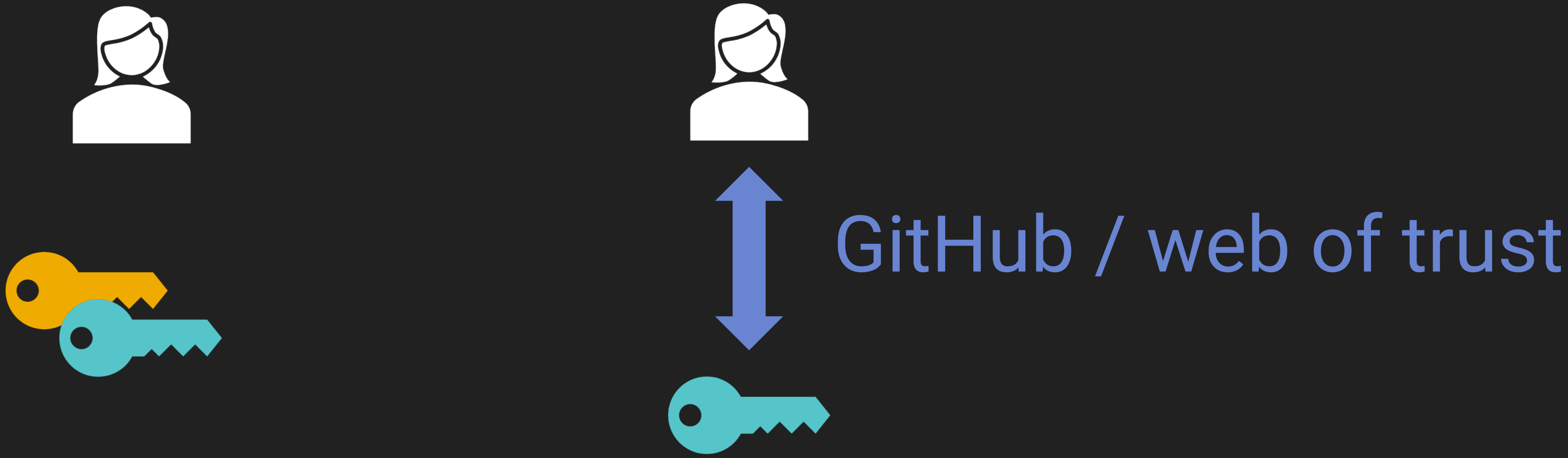
Data Scientist @Emarsys

- Person 1 as person 1: good commit
- Person 2 as person 2: good commit
- Person 3 as person 1: evil commit



GitHub / web of trust

👤 sign with 🔑, GitHub verifies with 🔑



GitHub / web of trust

👤 sign with 🔑, GitHub verifies with 🔑

specific technology

- OpenPGP: standard
- gpg 📦: low-level
- **ropsec** 📦: end2end

reduce risk of mistake

`ropsec::sign_commits_with_key()`

```
Do you want to sign future commits with `9958986BA31B2E1E`?

⚠ This will set your user.email
  from example@gmail.com to test@test.com.

1: Yes
2: No
```

communicate status

```
ropsec::store_public_key()
```

```
✓ Public GPG key is uploaded to GitHub.

✗ Unauthorized request. Check your token.

⚠ Uploaded key is unverified, emails do not match. Delete
the key (https://github.com/settings/keys) and try again.
```

testing global changes

- `askYesNo, getPass::getPass`
- `git2r::config`
- `gpg::gpg_keygen`

testing global changes

```
#throws error if password prompt cancelled:

stub(generate_key, "getPass::getPass", NULL)

expect_error(
  generate_key("John Doe", "jd@example.com"),
  "GPG key generation cancelled by user"
)
```

audit your computer in detail

```
ropsec::full_on_audit()$suggestions
```

- Use SSH key of size at least 2048
- Install a PAM module for password strength testing like pam_cracklib

{ropsec}: 📦 available on GitHub

- sign your commits
- audit your computer