

{ropsec}: R OPerations SECurity



unconf '18 project



on GitHub

security is important ...

... but unnecessarily hard

verify authenticity of commits

Are you who you say you are?

@czeildi

Data Scientist @Emarsys

without signing

The screenshot shows the GitHub interface for the repository 'czeildi / gpg-showcase'. At the top right, there is a 'Watch' button with a dropdown arrow and a '0' indicator. Below this is a navigation bar with tabs for 'Code', 'Issues 0', 'Pull requests 0', 'Actions', 'Projects 0', 'Wiki', 'Insights', and a settings gear icon. A 'Branch: master' dropdown is visible below the navigation bar. The main content area is titled 'Commits on May 6, 2019' and lists two commits:

- as lldi, w/o commit signing**
czeildi committed a minute ago
- as impostor, without signing**
evil impostor committed 12 minutes ago

@czeildi

Data Scientist @Emarsys

with signing

The screenshot shows the GitHub interface for the repository 'czeildi / gpg-showcase'. At the top right, there is a 'Watch' button with a dropdown arrow and the number '0'. Below this is a navigation bar with buttons for 'Code', 'Issues 0', 'Pull requests 0', 'Actions', 'Projects 0', 'Wiki', 'Insights', and a settings gear icon. A 'Branch: master' dropdown is visible on the left. The main content area is titled 'Commits on May 6, 2019' and lists two commits:

- as evil impostor, signing w unverified key** (Unverified)
evil impostor committed 7 minutes ago
- as lldi, with signing commit** (Verified)
czeildi committed 9 minutes ago

@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 

@czeildi

Data Scientist @Emarsys



GitHub / web of trust



sign with , GitHub verifies with 

@czeildi

Data Scientist @Emarsys

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

@czeildi

Data Scientist @Emarsys

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