6.857 Homework **Problem Set 1** # 1-1. Security Policy for GitHub

April 6, 2014

# 1 Objective

The purpose of this document is to outline the rules of use and operation of **GitHub** by defining the roles and permissions of its members and the policies that concern usage, protection, and sharing of its assets.

# 2 Definitions

GitHub is a distributed revision control hosting service that makes use of Git revision control software. It facilitates collaborative software development by allowing users (as individuals and/or in teams) to track, share, and discuss source code hosted in public and private repositories. It is available to its users as a website and as a remote endpoint for Git software.

## 2.1 Repositories

A repository can be best understood as a versioned folder for a software project. It contains all the files, documentation, and history pertaining to that project. Repositories can either be private or public. A public repository is open to website visitors, who can be non-registered users. They can view, clone, and pull from it, but must first create a user account before performing any additional actions.

## 2.2 User

A user is an individual GitHub account holder and can create repositories, be invited to join an organization, and collaborate with other users via their repositories. A user can be authorized to perform Git actions on a repository, such as pull, push, commit, clone, branch, and merge.[1] Users can either be free or paid; only paid users are allowed to create private repositories.

[1] A full list of Git actions are available at `http://gitref.org/`.

# 3 User Roles and Access Levels

## 3.1 Primary Roles

### 3.1.1 OWNERS

Users that register an account with GitHub are known as the **OWNER** of the repositories they create. (Only paid users may create private repositories.) They have full control of their account and agree to the following rules of usage:

1. *Protect personal account credentials:* Users must choose a strong account password and must not share it with other users. GitHub provides, and strongly recommends, two-factor authentication so that users can protect their account with more than just a password (§4).
2. *Maintain repositories:* Every **OWNER** is responsible for all content posted under their account. They can create and delete repositories, with read/access privileges (§3.2.3, §3.2.4).
3. *Appoint collaborators:* The **OWNER** of a repository can collaborate on a project by assigning read/write privileges to other users, who are known as **COLLABORATORS** (§3.1.2).

### 3.1.2 COLLABORATORS

When a user is assigned **COLLABORATOR** access by the **OWNER** of a repository, the user has read/write privileges (§3.2.3, §3.2.4) for that repository.

## 3.2 Secondary Roles

A registered GitHub user can create an ***organization*** account and appoint team-based permissions for the repositories created under that account. Other users can also be added to the **OWNERS** or **ADMIN** team of that account. In particular, a user can be a member of an organization at one of four levels in each team, described below. Note that each level includes the permissions of all the levels below it.

### 3.2.1 OWNERS

The users appointed as **OWNERS** of an account have full access to all repositories and teams within it. They control the account profile and settings, billing and payment information, and members. They can delete the account and all of its content.

### 3.2.2 ADMIN Team Members

A user in an **ADMIN** team can:

1. Create repositories within the team. Delete repositories assigned to the team.
2. Change team settings.

3. Transfer repositories to the organization account.
4. Add and remove users from the team. Add collaborators to the repositories assigned to the team.

### 3.2.3 WRITE Access Team Members

A user in a **WRITE** access team can, for the repositories assigned to the team:

1. Push to the repository.
2. Apply labels and milestones. Assign, close, and re-open issues.
3. Edit commits, pull requests, and issue comments.
4. Merge and close pull requests.

### 3.2.4 READ Access Team Members

A user in a **READ** access team can, for the repositories assigned to the team:

1. Pull from the repository.
2. Fork the repository. Send pull requests from forks.
3. Open issues.
4. Edit their own commits, pull requests, and issue comments.

## 4 Authentication

- The service password-protects user accounts and prevents brute-force attacks via rate limiting. The passwords are encrypted and salted.
- GitHub allows users to enable two-factor authentication, which requires the user to enter a password as well as a security code sent to the user's mobile phone or generated via a two-factor application.
- Git actions require either HTTPS authentication via GitHub account username and password or, for convenience, SSH authentication via keys.
- Finally, the service uses SSL for the transmission of all private data.

## 5 Employee Access

- GitHub employees cannot access private repositories unless it is required for user support.
- Employees that do access those repositories must temporarily attach their SSH key to the owner's account.

## 6 Information Gathering and Usage

GitHub collects information via these channels:

1. **User Account Information:** GitHub stores the names and email addresses of all registered users. Additionally, paid users are required to enter billing and payment information, which is securely stored on PCI compliant servers.
2. **Cookies:** GitHub uses browser cookies to record current session information, but does not use permanent cookies. To protect against unauthorized access to user accounts, users are logged out after a certain period of inactivity.
3. **Communication with GitHub:** GitHub stores all communication with the service via website visits, website registrations, surveys, and email.

The information collected by the service is used to improve its quality; it is not shared with or sold to third parties except in special circumstances, such as to comply with subpoenas from law enforcement or to respond to user violations of the Terms of Service (ToS).[2] GitHub users retain all rights to their data, including software projects.

## 7 Amendments to the Security Policy

So far we have defined a security policy for the main GitHub hosting service, but it is open to amendments depending on the needs of its users. To give an example, here are a couple amendments:

- **GitHub Enterprise:** GitHub provides an external service known as GitHub Enterprise that allows users to host their repositories on their own infrastructure.[3]
- **Government Users:** A user that is a U.S. government agency member and account holder of the service on behalf of an agency must agree to a modified ToS.[4] This amendment primarily waives the requirements within the ToS that GitHub be used for private, personal, or non-commercial purposes. GitHub will look solely upon the agency, and not the individual using the service on behalf of the agency, to enforce the modified ToS.

[2] The current GitHub ToS is available at https://help.github.com/articles/github-terms-of-service.

[3] The security for this separate service is discussed at https://enterprise.github.com/security.

[4] https://help.github.com/articles/amendment-to-github-terms-of-service-applicable-to-government-users.

6.857 Network and Computer Security
Spring 2014