A Secure Distributed Version Control System based on Git

Project Members:

1. Vishal Singh Kushwaha (2019H1120047P)
2. Ashirwad Pradhan (2019H1120043P)

About the Idea:

A version control system is a very useful tool to keep track of modifications done to the code. Git provides us a gateway to handle the above problem with ease. But there are few things which are still missing from the security perspective.

We aim to build a secure cloud VCS application on top of Git with added security features such as:

1. Encryption of git repository on the cloud
2. Access control system to manage access to the developers with correct authorization.
3. Securing the **git transport protocol** with TLS to allow git operations restricted to authorized users
4. An integrated solution to the Key Management Problem where the developers need to worry minimal about the key storage complications.

Why is this interesting?

Today solutions like Github and Bitbucket mainly focus on open source project development and most of the code/data is stored unencrypted. This restricts many potential users such as those working in **defence/ confidential drug development** from using the system. Though the idea of private repository is often provided as a solution but it is often flawed as the third party is still in control of the data which is stored in their servers.

Solution Description:

Our idea described above provides a solution to people from areas of defence or any other field which requires secure code development with VCS. The users can set up their own in-house git repository and can host in their own network or their preferred cloud provider. The data which is stored is always in their own control and no third party can read or write to it unless the keys are compromised or unless access rules specify the action. The communication between the VCS server and the developers are also based on the secure communication method based on TLS.

The git transport protocol as of now in current state is un-authenticated but provides a very good compression factor hence saving on bandwidth and data. We also aim to make this protocol authenticated so that we can get the best of both worlds.

Plan of Action Overview:

We have identified a few macro milestones to build the system.

1. Realize an **efficient** encryption scheme to encrypt the repository data.
2. Create a workflow for the multi key encryption/decryption which enables a team to work securing on the same repository simultaneously.
3. Access control layer for authorization of users attached to a repository.
4. Decide on the interaction flow between the keys mentioned above.
5. Securing the **git transport protocol** messages with TLS.
6. Realize a system to efficiently manage the keys.
7. Command line client tool which will enable developers to perform operations(create, clone, push, pull) to the secure repository.

List of Deliverables:

We expect to provide the following deliverables.

1. A cloud based SaaS for a secure and efficient distributed VCS.
2. A command line client tool to interact with the system.
3. Deployment on AWS EC2.
4. User manual on how to install and use the system.