with
COMMUNICATIONS

Vault

January 3, 2016

Passwords, keys, and tokens: each of these are technological methods of protecting sensitive data, and, ironically, each are also pieces of sensitive data themselves. Managing secrets and deployments like passwords can be tricky because these bits of information can lead to huge security breaches if they aren't properly protected.

At this year's "All Things Open" conference, Mitchell Hashimoto, the creator of Vagrant, and his company HashiCorp discussed a new piece of open source software called Vault which they have designed in an attempt to respond to this problem of keeping secrets secret.

Vault is aimed at mitigating the risks involved when secrets like passwords, keys, and tokens are left 'lying around,' for lack of better wording. Putting secrets and deployments into files or file systems can prove as risky as keeping them outside a source code repository. Unmanaged files can become out of sync, lost, or exposed, but these secrets must still be stored, verified, and validated somewhere.

This software has considered the issues inherent in password protection methods. It allows users to customize who can access these secrets and when they can use that access. Deeper customizations make it possible to spread a key amongst several people, requiring so many to be in one spot to unlock a vault.

For example, a quorum could be created where 5 people are given keys to a vault, but said vault can only be opened when 3 of these people put their keys together. Any 3 people in the 5-person group can come together to unlock the vault, but it won't open for any less than that number of participants.

Vault is also capable of creating dynamic secrets. New database passwords can be generated each time an application starts, with the passwords being deleted instantly so that the user accesses the application without ever actually seeing a password.

This process is set in motion when the application in question asks Vault for a database password. The software is able to provide one on the backend by creating a user with a brand-new password on the fly. This authentication data is then sent to the application to unlock it without the password being stored anywhere in the software. This means that if there is an attempted breach, an unauthorized user would be unable to find the current password because it never actually existed within the database.

Another handy feature is Vault's customization. If a lower level of security is desired, one person can set up the software so that they are the only one managing all the keys and security. However, if higher levels of security are required, Vault can be set up and run by a team with a quorum.

Lastly, Vault’s base software is free, with some optional enterprise plug-ins for users who require them. However, the functionality that comes with the free version will likely satisfy the needs of 80 to 90 percent of those seeking to utilize Vault.