Share Credentials The Safe Way

Use your Wiki/ Share, GPG and a keyring to share credentials

Onkobu Tanaake

2019-01-20T20:00:00

Companies sometimes need shared credentials. You need to access a customer's testing system, log in to a sample cloud instance or exchange work in progress from developer accounts. These systems are password protected and normally you have a shared document, a Wiki or a mailing list. It has never been a good idea to share passwords this way. Once you saved the credentials access is unlimited.

GPG or PGP offer an easy to handle alternative. I assume that you already have key pairs and some sort of public key infrastructure. If not, ask for the next article regarding LDAP/ Active Directory and hierarchical web of trust. You also have a large group of co workers and a smaller group you want to share the credentials with. So you'll need:

- A command line interface
- GPG or PGP-installation, I prefer GPG because it's open source
- Text editor, Notepad, Notepad++, any IDE
- public key infrastructure
- A shared data store like a network filesystem, a Wiki, version control system

Start with a text editor of your choice to simply write down the text file containing the credentials. I often use a sort of formatting, to also explain the target system, provide URLs and contact information:

```
Access to Testing System Ulysses

Username   : joycejames
Password   : trampcosinelegacyfrog
Valid until: Dec. 2019
Admin: testing-infrastructure@it-company.com
```

With this file saved as *credentials_ulysses.txt* you switch to your favorite command line. You may also use any of the software at your company providing GPG/ PGP-encryption. I prefer the command line to stay focused on the task instead of bothering about install process, side effects or limitations of nearly-free software:

```
# Display all the keys in your keyring to check the user ids
```

```
#
$> gpg --list-keys

# Encrypt (-e) the file for multiple recipients (-r) and
# output ASCII-safe (-a)
#
$> gpg -ea -r Alice -r Bob -r Homer -r Minnie credentials_ulysses
```

Luckily your keyring knows all the recepients by their user ids. If your key infrastructure is good this is a simple task, using the names you know. And after a blink of an eye your command line contains something like this:

```
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.0.7 (MingW32)

chunkOfASCIIcharacters
-----END PGP MESSAGE-----
```

This works very efficiently, because the message is not encrypted once for each recepient. Instead an intermediate key is created, that all from the list can re-generate and therefore decrypt the message. It is safe to paste this into your wiki or shared storage. I even have some pro-tips:

- If stored as a file, use the *shred*-command to wipe out the file before deletion, otherwise data can be restored easily
- Don't even use the file, instead use clipboard and gpg's interactive mode
- Ask a developer at hand to write a handy little tool for this every day task with a fancy Share- or Upload-button

For the interactive mode, only write down the information you want to share encrypted in the text editor. Copy the text to the clipboard. Invoke gpg command line without a file name. It opens in interactive mode and waits for user input. Paste your clipboard content into the command line. Finish by pressing Ctrl+D. Copy the output as mentioned above.