Two Factor SSH with Google Authenticator

POSTED ON FEBRUARY 18, 2011 / IN SECURITY / 36 COMMENTS

SOURCE : HTTPS://WWW.MNXSOLUTIONS.COM/SECURITY/TWO-FACTOR-SSH-WITH-GOOGLE-AUTHENTICATOR.HTML

Last week, Google enabled two factor authentication for everyone. This article explains how to install and configure Google Authenticator in conjunction with SSH for two factor authentication. Two-factor authentication relies on something you know (a password) and something you have (your phone).

Update: I have posted another article describing this same implementation with a Yubikey.

You can use this existing implementation and Google Authenticator application with SSH via an included PAM in the Google Authenticator open source application.

Download the Google Authenticator application

First, download and install Google Authenticator on your Iphone/Android/Blackberry.

Compile, install, configure Google authenticator PAM

You may need a few dependencies. On RHEL 5 I was missing 'pam-devel'.

```
$ hg clone https://google-authenticator.googlecode.com/hg/ google-authenticator/
$ cd google-authenticator/libpam/
$ make
$ sudo make install
$ sudo vi /etc/pam.d/sshd
```

Add the following line to the beginning of /etc/pam.d/sshd:

```
auth required pam_google_authenticator.so
```

You also need to update /etc/ssh/sshd_config and add/update:

```
ChallengeResponseAuthentication yes
```

Setup your user to require two-factor authentication

As a user, you can now run ‘google-authenticator’. This will generate a secret key, and add a file to your home directory that the newly installed PAM uses.

```
$ google-authenticator
https://www.google.com/chart?chs=200x200&chld=M|0&cht=qr&chl=otpauth://totp/user@host.com%3Fsecret%3DAAAAAAAAAAAAAAAA
Your new secret key is: AAAAAAAAAAAAAAAA
Your verification code is 123123
Your emergency scratch codes are:
81283812
18283182
18128381
38383838
18283120

Do you want me to update your "~/.google_authenticator" file (y/n) y
Do you want to disallow multiple uses of the same authentication
token? This restricts you to one login about every 30s, but it increases
your chances to notice or even prevent man-in-the-middle attacks (y/n) y
```

Note: The emergency scratch codes are one-time use verification codes in the event your phone is unavailable.

Configure this new secret key in Google Authenticator

 In your Google Authenticator application on your phone, add this new secret key that was generated in the previous step. Note, a URL is also displayed, that can be scanned from your Google Authenticator application.

Wrapping up the setup

You will now need to restart SSH for the pam/ssh changes to activate.

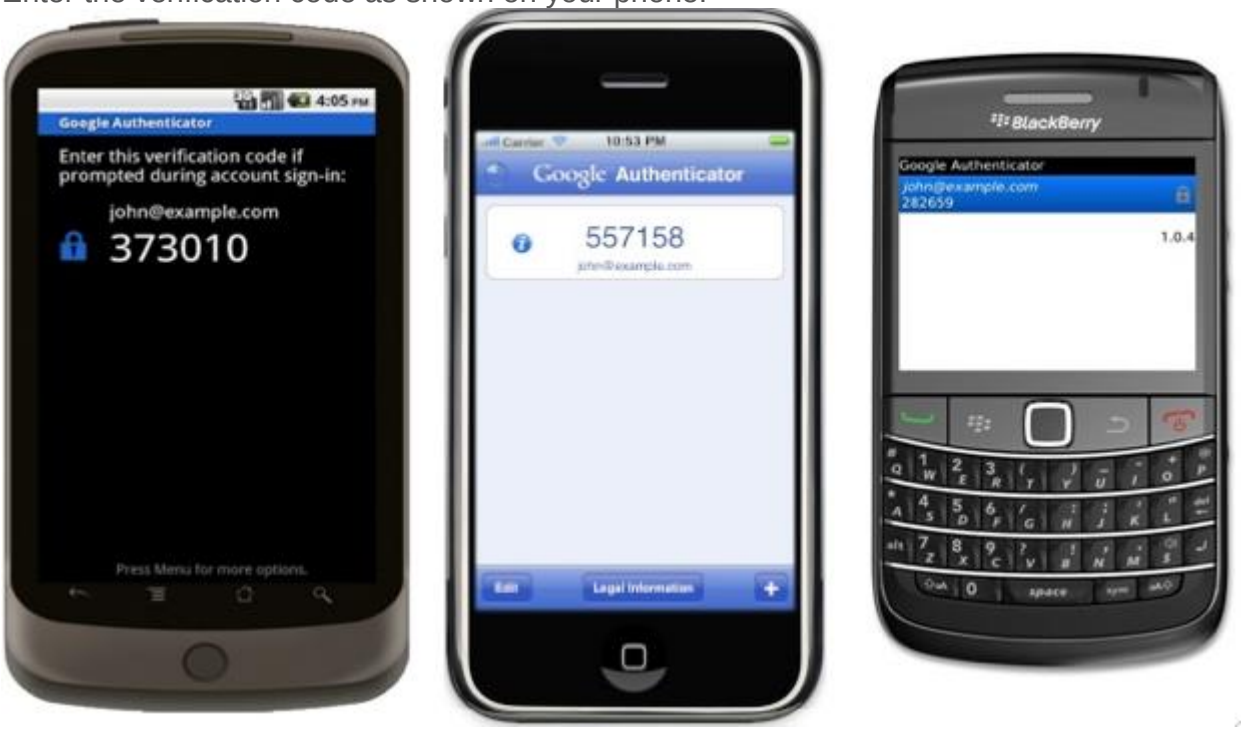
At this point, you will want to stay logged into the server while you test in another shell.

Testing

Test that two-factor authentication is working.

```
$ ssh example.com
Verification code:
Password:
[user@host ~]$
```

Enter the verification code as shown on your phone.



Your SSH sessions are now protected with two factor authentication