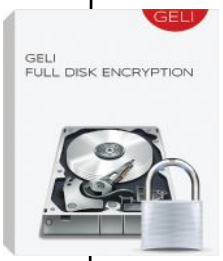
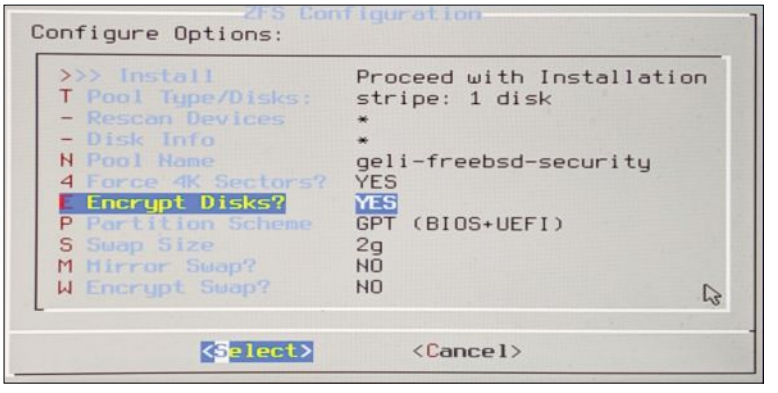
CONFIGURING Full-disk Encryption on FreeBSD

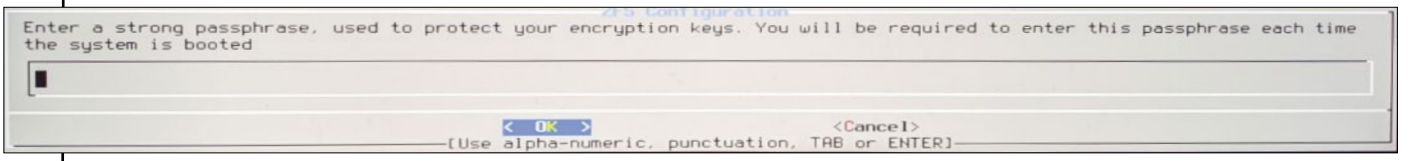
by Roller Angel

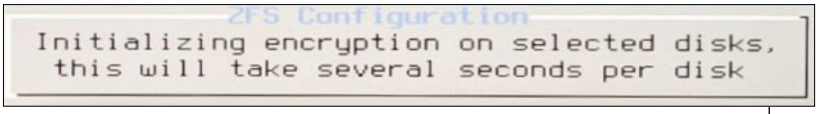
While there are multiple ways to configure full-disk encryption on FreeBSD, this article will focus on one method and provide an easy route to follow and get started using GELI. If you already have FreeBSD installed on your machine and are looking for instructions on how to enable GELI full-disk encryption on a separate disk that you attach to your existing install, you'll find the details in the book *FreeBSD Storage Essentials* by Michael W Lucas.



On the machine used in this article, we're installing FreeBSD as a fresh install and using the normal installer to enable full-disk encryption with GELI on ZFS. Go through the installer as you normally would but when you get to the Partitioning screen, select Auto (ZFS). Next select the Pool Type/Disks option and choose the disk you want to fully encrypt and on which you want to install FreeBSD. Choose stripe as the Virtual Device type. Select the disk using the Space Bar then press Enter. This will bring you back to the ZFS Configuration menu and you can go down to Encrypt Disks? and press Enter to change the NO to YES. Go up to Proceed with Installation to let the utility do the work of enabling full-disk encryption on your fresh FreeBSD install. The next screen will ask you to enter in the passphrase that will be used to decrypt the disk each time you boot the machine. We're using a







38-character static passphrase on a YubiKey along with a passphrase that is memorized and manually entered prior to the passphrase stored on the YubiKey. First, we enter in the memorized passphrase and then press the button on the YubiKey to type out the 38-character passphrase and press Enter for us. This memorized bit of the passphrase prevents a thief from being able to use your stored passphrase from your YubiKey to decrypt your machine, assuming they got their hands on both your machine and your YubiKey. They would also have to know the first part you have memorized, so make sure to keep that a secret.

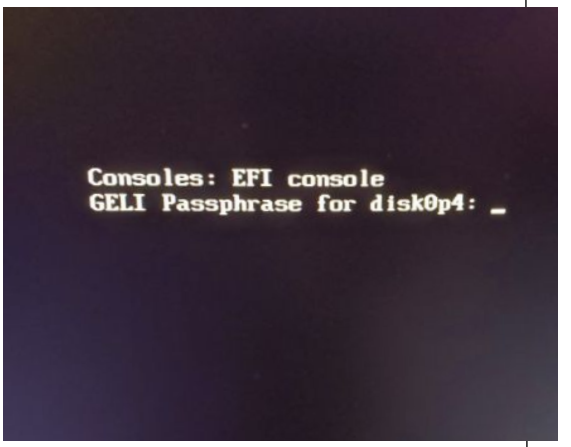
You can follow the "Guide to Getting Started with FreeBSD on Virtual and Real Hardware" available in the January/February 2019 edition of the *FreeBSD Journal* to get a desktop up and running where you'll be able to interact with the YubiKey Personalization utility and program your YubiKey to store a passphrase with a maximum of 38 characters. Once you have programmed your YubiKey, you can reinstall FreeBSD to get the benefits of full-disk encryption. Essentially, the benefits are that if one were to steal your computer or temporarily obtain access to it while it was off, they wouldn't be able to access the files on it because the disk is encrypted at rest and the data stored on it isn't accessible until GELI is used to decrypt the disk using your passphrase. To program your YubiKey, you'll first need to install the software provided by Yubico by typing the following command:

```
sudo pkg install -y yubikey-personalization-gui
```

You can then either use the menu in Lumina to select the newly installed software to open it or run the following command to get it to open up:

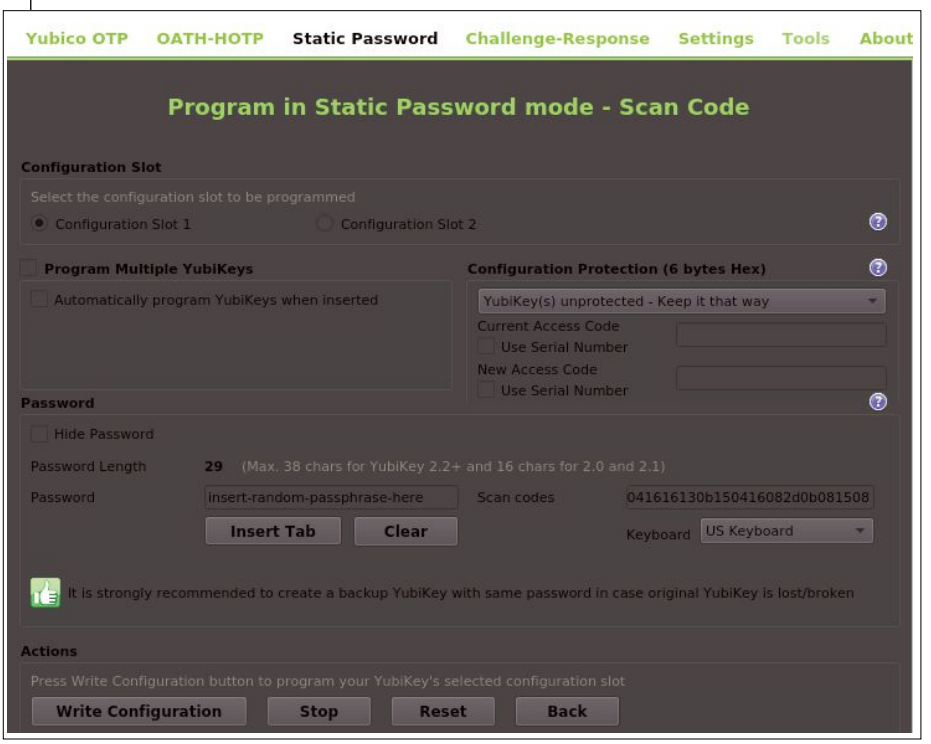
```
yubikey-personalization-gui
```

Visit the Static Password tab. Next click on the Scan Code button. The first step is to choose the Configuration Slot to use. See the notes provided using the ? icon next to the Configuration Slot selection bubbles for details about the configuration slots and instructions on how to use them. Next, in the Password section, look for the Keyboard label with the Choose-a-Layout—drop-down menu next to it—and select the keyboard layout you'll be using. Now you can insert your random passphrase into the box next to the Password field. Finally, with your YubiKey inserted, select Write Configuration to save that passphrase to the chosen configuration slot of your YubiKey. Now, when you press and hold the button on your YubiKey, you'll see the



passphrase automatically type out as if you were to enter it in manually on the keyboard. Keep in mind that the amount of time you hold the button varies depending on which Configuration Slot you programmed.

Reboot the machine on which you just installed FreeBSD and the first thing you'll see is a screen asking you to enter in your passphrase. Once you have entered in your passphrase correctly, the system will boot like normal. ●



Roller Angel is an avid BSD user who enjoys all the amazing things that can be done with BSD technology. He has taught programming workshops based on FreeBSD and is working on building an online training platform for teaching BSD and related technologies. See BSD.pw for more information.