Module 2.1
Zymbit PKCS#11

CompuThings *Technology;

Module Target

- Use Zymkey as Source of Key Pair

Possible Risk

- Private key in .ssh/id_rsa is taken when the SD card is stolen
- The idea of keeping credentials in the Hardware Security Module (HSM) is a common practice in the industry.
- How its different?
- Because HSM have their own private keys that user can use it but can’t modify it.
- Zymkey provide 3 slots with ready to use private keys.

Possible Risk

- Private key in .ssh/id_rsa is taken when the SD card is stolen
- The idea of keeping credentials in the Hardware Security Module (HSM) is a common practice in the industry.
- How its different?
- Because HSM have their own private keys that user can use it but can’t modify it.
- Zymkey provide 3 slots with ready to use private keys.

Getting ECDSA public key

#python

>>>import zymkey

>>>zymkey.client.get_ecdsa_public_key()

>>>zymkey.client.create_ecdsa_public_key_file("/tmp/mypublic.pub")

Configuring PKCS#11

- PKCS#11 API is used to handle and store cryptographic keys.
- Zymkey supports PKCS#11 through a package called zkpkcs11.
- It is use to initialized the authentication token that use Zymkey's private and public keys.

  #sudo usermod -a -G zk_pkcs11 pi

  #sudo zk_pkcs11-util --init-token --slot 0 --label Zymkey

  (you will ask for SO PIN and User PIN. Don't forget them. You will also get the slot number)

Configuring PKCS#11

- PKCS#11 API is used to handle and store cryptographic keys.
- Zymkey supports PKCS#11 through a package called zkpkcs11.
- It is use to initialized the authentication token that use Zymkey's private and public keys.

  #sudo usermod -a -G zk_pkcs11 pi

  #sudo zk_pkcs11-util --init-token --slot 0 --label Zymkey

  (you will ask for SO PIN and User PIN. Don't forget them. You will also get the slot number)

Configuring PKCS#11...2

- zk_pkcs11-util --use-zkslot 0 --slot 1597039069 --label sshkey --id 0001
- sudo apt-get install opensc
- sudo pkcs11-tool --module /usr/lib/libzk_pkcs11.so -l -p 1234 --token Zymkey –list-object
- You will see the public and private key information

Token Detail

Public Key Object; EC EC_POINT 256 bits

EC_POINT:
04410439fe87083c9b9e0e315ff07a5489e5a86ca6a38a6585d886398a88c84a8f8aa7329e30bceb83c8d813eda50e
2c1c948a26d3c77c770cb3822a59b5defe08d638

EC_PARAMS: 06082a8648ce3d030107

label: sshkey

ID: 0001

Usage: verify

Private Key Object; EC

label: sshkey

ID: 0001

Usage: sign

Conclusion

- Zk pkcs package tie software only solution into HSM linked cryptographic services.
- The key generated can be extent to be used in ssh and other public key security services.