Hardening PGP using GnuPG and Yubikey

hybrid multifactor authentication and cryptography

John Roman

Linux System Administrator
RAND Corporation

SCALE 2017
• public/private keyrings
- public/private keyrings
- public keys go to the world, generated on machine
• public/private keyrings
• public keys go to the world, generated on machine
• key types: signing, authentication, cryptography
pitfalls

- private keyring... but how private?
- private keyring... but how private?
- portability
pitfalls

- private keyring... but how private?
- portability
- standards compliance
conventional example, the CAC/PIV

- Common Access Card, in service since 2005
conventional example, the CAC/PIV

- Common Access Card, in service since 2005
- FIPS201 PIV Federal Information Processing Standard (FIPS) 201, Personal Identity Verification
OpenPGP: we we’re JUST thinking that!

- OpenPGP Card: in service since 2004
OpenPGP: we we’re JUST thinking that!

- OpenPGP Card: in service since 2004
- 9 different vendors, multiple form factors
OpenPGP: we we’re JUST thinking that!

- OpenPGP Card: in service since 2004
- 9 different vendors, multiple form factors
- relatively unknown outside of FSF Europe.
Our focus: Yubikey

- supports hybrid mode
Our focus: Yubikey

- supports hybrid mode
- hermetic, crushproof, scaleable pricing
Our focus: Yubikey

- supports hybrid mode
- hermetic, crushproof, scaleable pricing
- NFC option.
general concepts

- card has a CPU, firmware.
general concepts

- card has a CPU, firmware.
- keys are loaded into slots, or generated by the card
general concepts

- card has a CPU, firmware.
- keys are loaded into slots, or generated by the card
- encryption, decryption, signature are all commands
general concepts

- card has a CPU, firmware.
- keys are loaded into slots, or generated by the card
- encryption, decryption, signature are all commands
- once loaded, private keys are sacrosanct.
general concepts

- card has a CPU, firmware.
- keys are loaded into slots, or generated by the card
- encryption, decryption, signature are all commands
- once loaded, private keys are sacrosanct.
- Yubikey only accepts commands, only returns data. NEVER KEYS.
HSM Specific concepts

- pin number similar to european credit cards
HSM Specific concepts

- Pin number similar to European credit cards
- 3 strikes, your pin is locked
HSM Specific concepts

- pin number similar to european credit cards
- 3 strikes, your pin is locked
- pin can be unlocked with a security officer pin.
HSM Specific concepts

- pin number similar to European credit cards
- 3 strikes, your pin is locked
- pin can be unlocked with a security officer pin.
- 3 strikes against the SO pin? Card is bricked. Keys lost. Game over.
HSM Specific concepts

- pin number similar to european credit cards
- 3 strikes, your pin is locked
- pin can be unlocked with a security officer pin.
- 3 strikes against the SO pin? card is bricked. keys lost. game over.
- pin length 6-8 characters, some implementations more than 128 char.
placing the card into 'hybrid' mode

ykpersonalize -d -m82
Firmware version 4.3.1 Touch level 527 Program sequence 3

The USB mode will be set to: 0x82

Commit? (y/n) [n]: n
keys were loaded from an airgapped system using the keytocard command.

- cicero@cypher ~ $ gpg --card-status
  Application ID: D2760001240102001006049011200000
  Version: 2 1
  Manufacturer: Yubico
  Serial number: 04001120
  Name of cardholder: John Roman
  Language prefs: [not set]
  Sex: male
  URL of public key: https://device.com/johnroman.gpg
  Login data: nimbus
  Signature PIN: not forced
  Key attributes: 4096R 4096R 4096R
  Max. PIN lengths: 127 127 127
  PIN retry counter: 3 0 3
  Signature counter: 51
  Signature created: 2016-12-27 04:27:41
  Encryption key: 8402 B920 F553 B6A6 F9C3 55FB 4F6F 7F56 D7F7 774D
  created: 2016-12-27 04:27:41
  Encryption key: EA74 1A65 152D 4C23 6A22 3FEC 63A1 BF2C AF9C 8338
  created: 2016-12-27 04:20:40
  Authentication key: B6CC 078S C1AE D58E 22C2 C697 116A F523 D67B 445B
  created: 2016-12-27 04:33:13
  General key info: sub 4096R/D7F7774D 2016-12-27 John Roman (just another lonely soul on the internet) <john@device.com>
  sec 4096R/D7F7774D created: 2016-12-27 expires: 2017-12-27
  ssh> 4096R/D7F7774D created: 2016-12-27 expires: 2017-12-27
  card-no: 0006 04901120
  ssh> 4096R/D7F7774D created: 2016-12-27 expires: 2017-06-25
  card-no: 0006 04901120
  ssh> 4096R/D673445B created: 2016-12-27 expires: 2017-06-25
  card-no: 0006 04901120
  cicero@cypher ~ $ scdaemon[24952]: updating slot 0 status. 0x0000->0x0007 (0->1)
  scdaemon[24952]: scdaemon (GnuPG) 2.0.30 stopped
OpenPGP card programming

```
gpg –card-edit mode, admin commands enabled

fetch  fetch the key specified in the card URL
passwd menu to change or unblock the PIN
verify verify the PIN and list all data
unblock unblock the PIN using a Reset Code

gpg/card> admin
Admin commands are allowed

```

Roman, John PGP
applications

- anything GPG enabled
- anything GPG enabled
- anything PAM enabled
- anything GPG enabled
- anything PAM enabled
- defense in depth: OTP/Cert/PW? sure
- anything GPG enabled
- anything PAM enabled
- defense in depth: OTP/Cert/PW? sure
- multiple cards per key, each has a unique subkey (code signing!)
THERE IS A POINT WHERE WE NEEDED TO STOP
AND WE HAVE CLEARLY PASSED IT

BUT LET'S KEEP GOING
AND SEE WHAT HAPPENS
NFC option: here be dragons

- easy integration with Openkeychain in Android/IPhone
NFC option: here be dragons

- easy integration with Openkeychain in Android/IPhone
- keys need to be generated by the user
NFC option: here be dragons

- easy integration with Openkeychain in Android/IPhone
- keys need to be generated by the user
- only supports a 2048 bit key
deploying 450 (thousand?) of these things.
Entropy.

GPG relies on kernel, not userland entropy.
- Flying Stone FST01 from the FSF store!
- RTL digital TV dongle and a tractor paper copy of phrack
OpenPGP not included...

Red Hat Enterprise Linux 7 does not include opensc GnuPG
NFC user fatigue.
not all NFC devices are “great” at picking up NFC
lack of a yubikey might cause lack of communication.
“destroyed” cards...

– try not to trigger a SO/Reset pin lock!!
– to reissue or reset?

Roman, John PGP
cardware considerations

processing rate is a function of USB IO and CPU. generating keys on the card = Entropy + CPU.
Questions?