

... but don't forget your keys.

(Digital Privacy & Security for Researchers)

QUT DMRC Summer School 2017

Brenda Moon & Felix Victor Münch

Why are we here?

Metadata retention

The Assignment

You, a data analyst for the Australian police, are on the train heading home when your phone starts buzzing. You got a text from your boss, who is asking you to take a look at your work emails. You reluctantly open your mailbox only to find the following email:

From: Finn Coburn <finn.coburn@thepolice.com> To:
data-analysts@thepolice.com Date: 2016-12-10 10:58 Subject:
Fixing a leak at Minecorp

Good morning analysts,

[...]

It seems there is a whistleblower at Minecorp leaking to a
journalist at MineWatch.

[...]

May I remind you that the mines in Australia are all
critical infrastructure, [...]. Therefore, we need
to identify the person of interest to put him/her under
arrest.

So I need you to dig this guy up for me. [...]

All logs you will need for the investigation should be available on Kibana. You will need to solve the preceding tasks before moving on to the next.

Do not forget to have a look on the Kibana cheat sheet that Sharon put together last week for us.

Keep me updated and let me know if you get stuck. I need the info to be submitted here by no later than 2:30 pm.

FINN COBURN CHIEF DATA OFFICER COMPUTER CRIME SQUAD Tel:
16131 www.thepolice.com

<https://snitchhunt.org/challenge>



How pre-teens using metadata found a whistleblower in two hours

POSTED MON 12 DEC 2016, 6:58PM Updated Mon 12 Dec 2016, 10:34pm

 Like 3.1k



By James Purtil

SHARE



Team Sherlock began the scenario with one clue: the leaked documents about fracking chemicals had been sent to anna@minewatch.org.au.

(<http://www.abc.net.au/triplej/programs/hack/how-team-of-pre-teens-found-whistleblower-using-metadata/8113668>)

worst case
scenarios

weak password reuse

your Twitter account is hacked by angry gamergaters – and
suddenly your devices are wiped

Activity

Visit <https://haveibeenpwned.com/> and look up your most used email address, to see whether your data has been published after a successful cyber attack or data breach.

revealing IP address

researching in extremist bulletin boards/social networks
getting harassed in your neighbourhood afterwards

unencrypted communication

communication with protesters in an authoritarian surveillance state via iMessage but message gets sent via SMS service

unencrypted devices

interview with journalist in country oppressing the press with
'off-the-record' content on unencrypted Android phone gets
confiscated at the airport before leaving the country

Why are you here?

What do you want to get out of this session? What privacy or security issues might effect your research? Discuss in groups!
(5 minutes)

Passwords

one ring to rule you all might not be a good idea

Main risks

Especially when you've been pwned:

- common password (qwerty, 12345, monkey, love, ...)
- easy to guess (qwerty12345, your name, your birthday, your partners birthday, your postcode,)
- reuse of passwords
- storing password in an unsafe place (i.e. unencrypted and accessible from outside)
- forgetting your password

Solution #1:

Use a password manager

What is a password manager?

- allows you to access all your passwords with a master password and/or keyfile ("secret file", e.g. on a USB stick)
- stores passwords in an encrypted file (i.e. not readable without a key)
- can often generate secure passwords for you

Therefore your passwords will be strong, will not be reused, and you don't have to worry about memorising them anymore.

We recommend

- KeePass, KeePassX, KeeWeb
 - Open source +
 - interoperable +
 - high reputation +
 - free +
 - not so convenient -
- 1Password
 - high reputation +
 - very convenient +
 - costs money -
 - closed source -


Solution #2:


Use 2-factor authentication



What is 2-factor authentication?

- similar to one time passwords for online banking
- something you know (your password) and something you have (your device)
- having device is verified by either
 - sending second code to you by SMS or
 - generating it in an App on your device
- this second element changes each time

SMS is not a secure channel!



Telstra 
@Telstra


Due to today's incident, it's possible some SMS messages were incorrectly delivered. All messages will be held while we resolve the issue.

RETWEETS


35


LIKES


20



2:54 PM - 2 Feb 2017

 14

 35

 20

SMS problems

- misdelivery
- unauthorised phone number porting
- not available during phone outages
- not encrypted - can be intercepted with scanner

We recommend

Use an app for 2 factor authentication:

- FreeOTP
- Google Authenticator (Android/iPhone/BlackBerry)
- Amazon AWS MFA (Android)
- Authenticator (Windows Phone 7)
- Authy

Group activity!

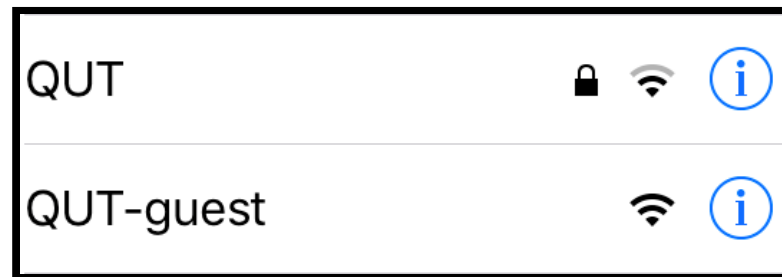
Find out whether one of your most used services provides 2-factor-authentication!

Communication

Main risks

While transmitting sensitive information: the men in the middle

- your email/messaging provider or anybody who has hacked them or pretends to be them
- authorities who subpoena any of your communication providers
- others in open/untrusted WiFi



Solution #1:

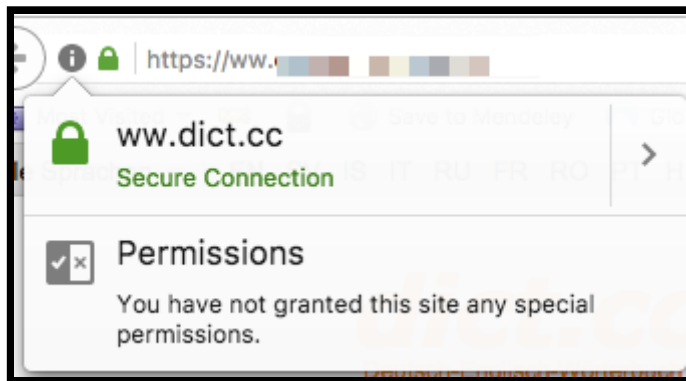
<https>

What is https?

- browser checks whether website has a valid certificate ('ID card')
- encrypts traffic between browser and website

We recommend

- check the address bar in your browser



- <https://www.eff.org/https-everywhere>

Examples for bad certificates: <https://badssl.com/>

Solution #2:

PGP encryption

"Pretty Good Privacy"

What is PGP encryption?

- Encryption protects your information so that no one except the intended recipient can read it.
- PGP adds two extra features by using a Public Key:
 - it allows you to encrypt information for a recipient without contacting them first - using their Public Key
 - you can verify that information signed by them is from them

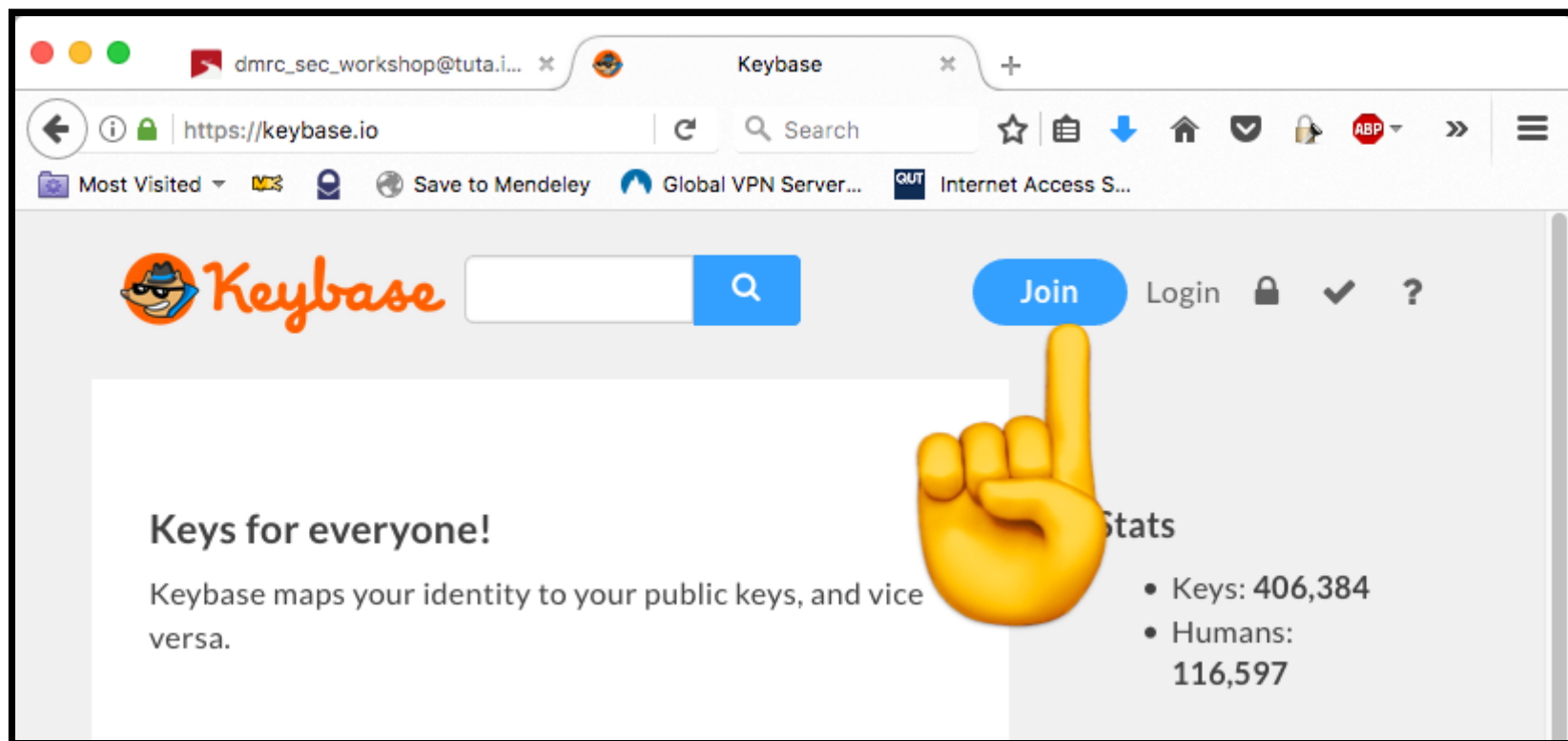
We recommend

- [keybase](#)
- [GPGTools](#)
- [Enigmail for Thunderbird](#)
- email clients with GPG support

Group activity!

Get an account on keybase.io and encrypt a message to somebody else in this workshop. Send it to their email address!

Decrypt a message that someone sends you!



Quick! Join Keybase



Email address

dmrc_sec_workshop@tuta.io

Claim my username

keybase.io/

dmrc_sec_tes

e.g. your Twitter handle

Passphrase (min. 12 characters)

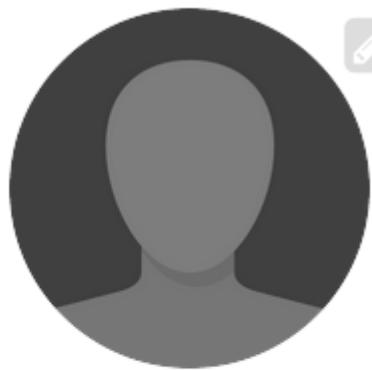
Has to be secure!
And don't forget it.

Repeat

Hint: use password
manager



Activate!



keybase.io/**dmrc_sec_test**

⚠ Action ▾

❓ [add a PGP key](#)



Your Full Name ✎

Your brief bio goes here. ✎

Wherever, Earth ✎

dmrc_sec_test, add a public key



Adventure!

Let's get your public key established

I need a public key

I have one already

Generating...

Math time, dmrc_sec_test.

You are about to discover a *4096-bit* key pair. Your computer will hunt for big prime numbers. It could take anywhere from a few seconds to many minutes.

On the bright side, this will warm up your home or office.



Ok, got it

Generating...



Full name

Don't put anything in here

Email #1

you don't want to be public!

Email #2

optional

Email #3

optional

The above info is public. Include any email address(es) you plan to use for sending/receiving encrypted mail.

Please confirm your keybase.io passphrase.

Can you remember it?

Let the math begin

Generating...

Public key

-----BEGIN PGP PUBLIC KEY BLOCK-----

Version: Keybase OpenPGP v2.0.62

Comment: <https://keybase.io/crypto>

xsFNBFiZJHYBEACu4mce0202p+A0GFRCI5ut9jQ5cJS1KirmY0IjVDIKVeQWxCGC

☒ Host encrypted private key, too (recommended)

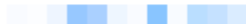
↑ **Not the safest thing to do, but convenient. Will do for this workshop.**



♥ Done, post to Keybase



Search for recipient

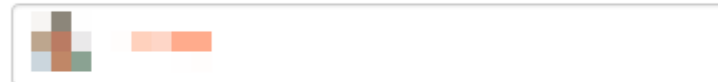


PGP Encrypt





Recipient



Message to encrypt

**Super secret
message**

Do you want this?

☐ sign the message (proof it's from you,
dmrc_sec_test)

Encrypt

GO!



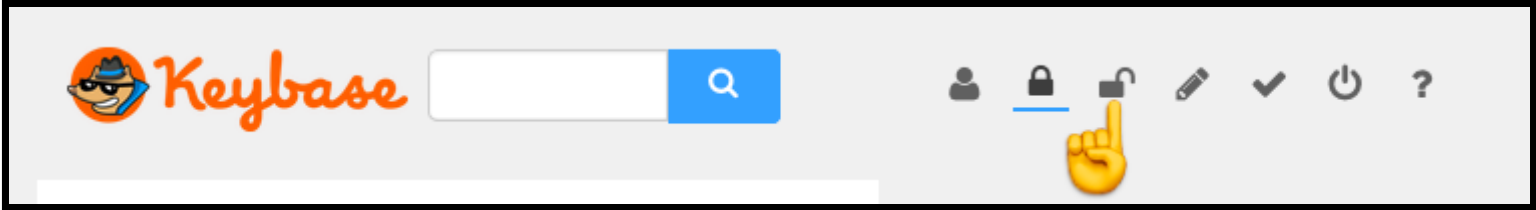
Success! You can paste the below message into an email, IM, whatever.

The secret message

-----BEGIN PGP MESSAGE-----
Version: Keybase OpenPGP v2.0.62
Comment: <https://keybase.io/cryptol>
Send this!
wcBMA5TkF1liDBD6AQf+OzLDMMUEUWI+TeMK9ZDlq
MGSdxRc5hxQ/glM32KIWEY5
vESa1XxbmdNSIXmFCx0G6FddL5c+qfPQBKkgALv19
u3UYq7y7dWf6ZEFwGoWcv9J
VhULN4g5I8gJA8FdTZ4sgqbHFWNlxj6omBjLK0zWg
cP91/mXYqKql02bdAi99Z9P
F17USr7yIL66qui8mBJrnSsfZgwPPrZW
/tx0X2+reDC1lmH7qIySJdnYofL9sATH
fVlY3eMQa0B5RRV14euQnWlWIU35NetCrcoDsCXFM
VySEWZWYIv92KXZAHJFjrfr
Vh9jZ95v4M0oypXucn0WVFf8YZ4GPUgpyVx71tvYE
+70AD1Mf+P+1CMG+4u48V...

Edit

Done - nuke the plaintext





Message to decrypt

```
LjATL5RQcoLmTEAti6
/G05cARq2UxbW7JCuZq0CKuI2h75qt8Ku
e89iqCqMfP5Ie
Ma1l+ExELiP7MXCbPSF3mUKZ1zrWGKk3Y
aEfnYtfxMWmTFbS33gIXBdANgR28Vwj
mscawljoix3De8tBVbLIUHiLhhv/kje5q
/r+0h9b/FTB09D+n4kZxcPT/wdbapNH
1BPje85zbgrwRj7Ns0Aog/LUFxIeGW0EW
/aHt0Jo8XF+hzl83aJcYS8UIcPZ0rXk
ndFlvjmqfEM
=75Gl
-----END PGP MESSAGE-----
```

Received PGP message

Your passphrase, dmrc_sec_test

Do you still know it?

Decrypt



YAY!



✓ Signed by dmrc_sec_test

The secret message

What's up?

It's really us!

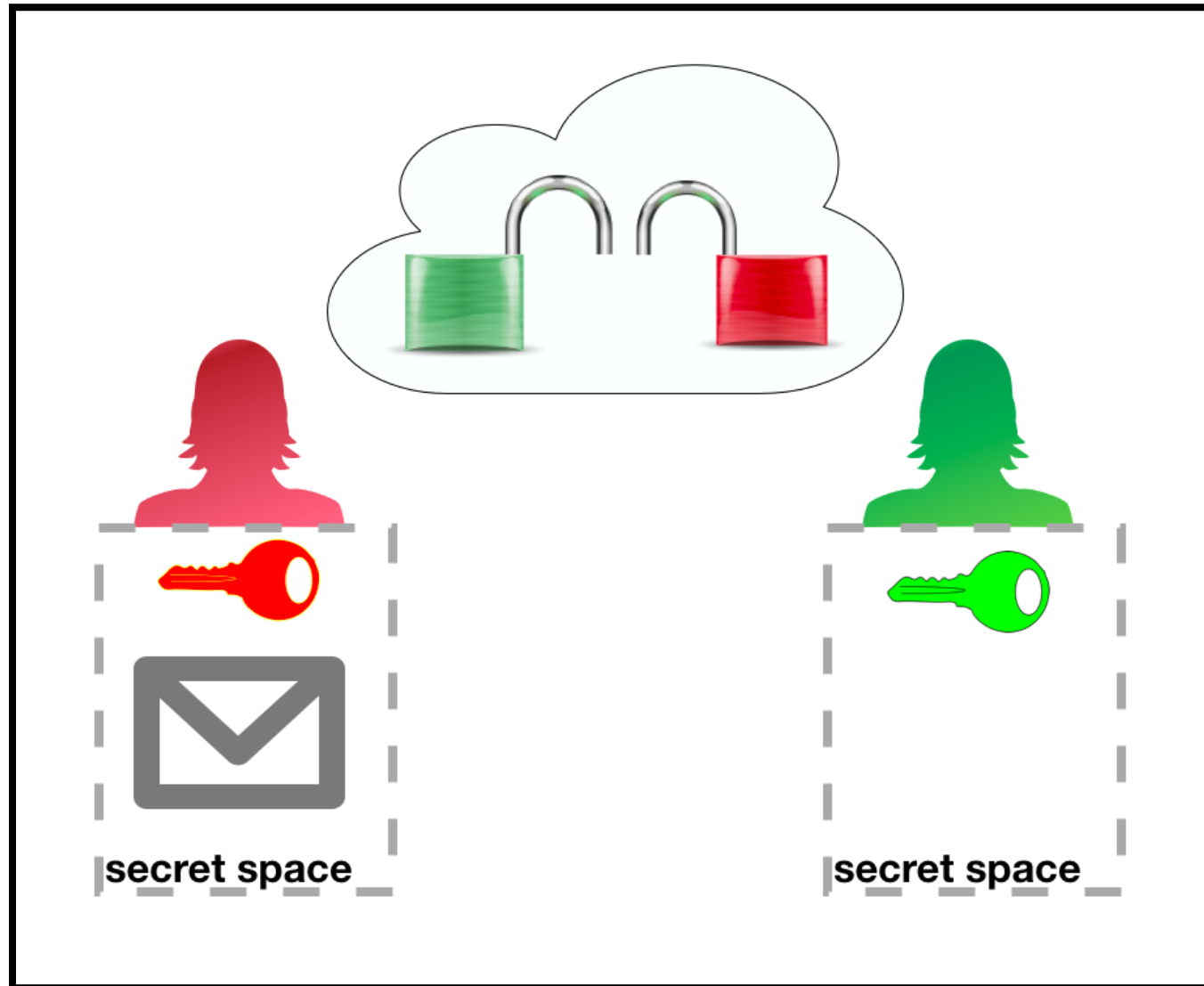
Ok, fair enough, that's
a bit anticlimactic

Clear & Hide

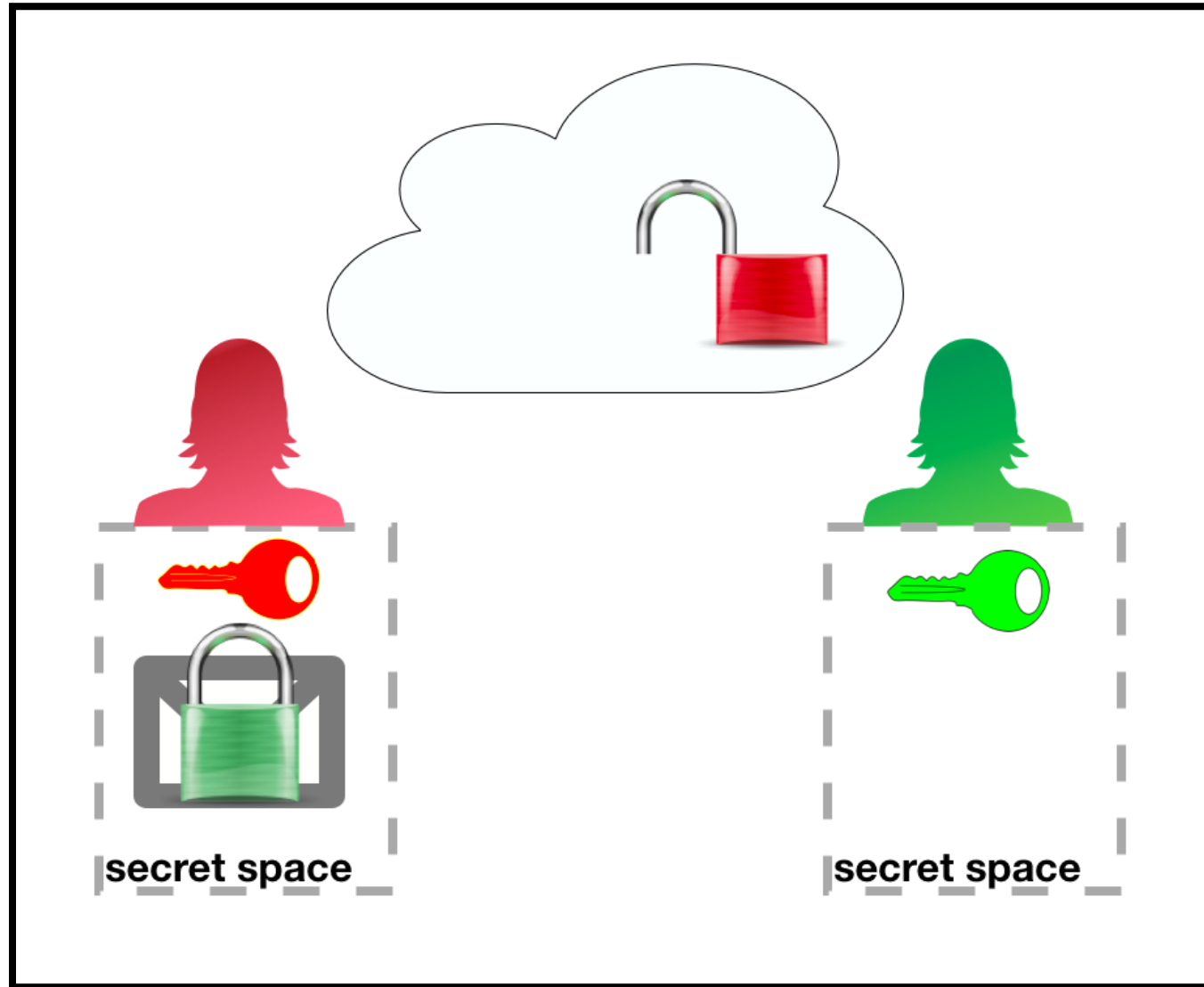
Whoot! So how did that work?

Let's call the public key a 'padlock'.

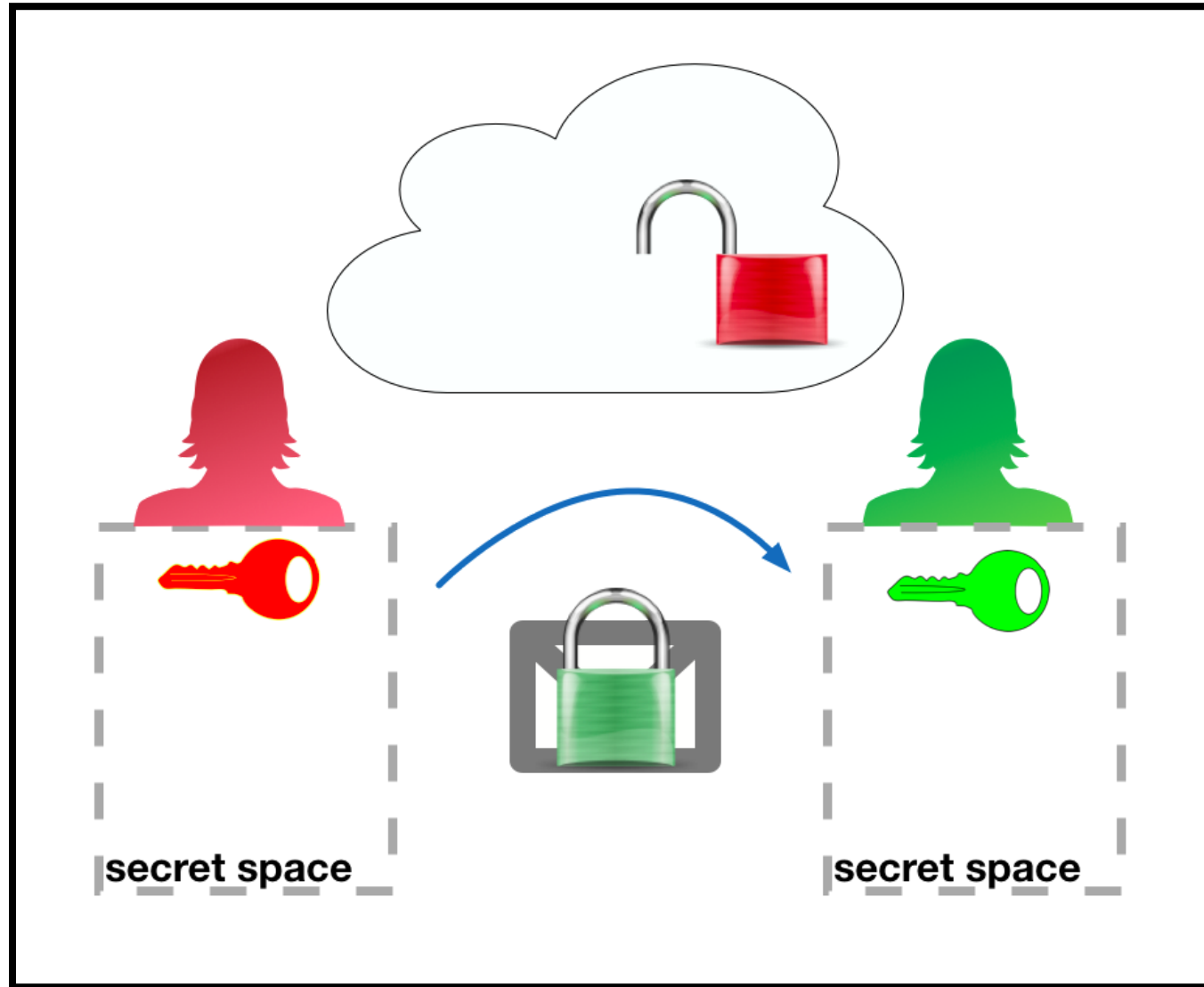
Red has a secret message for Green



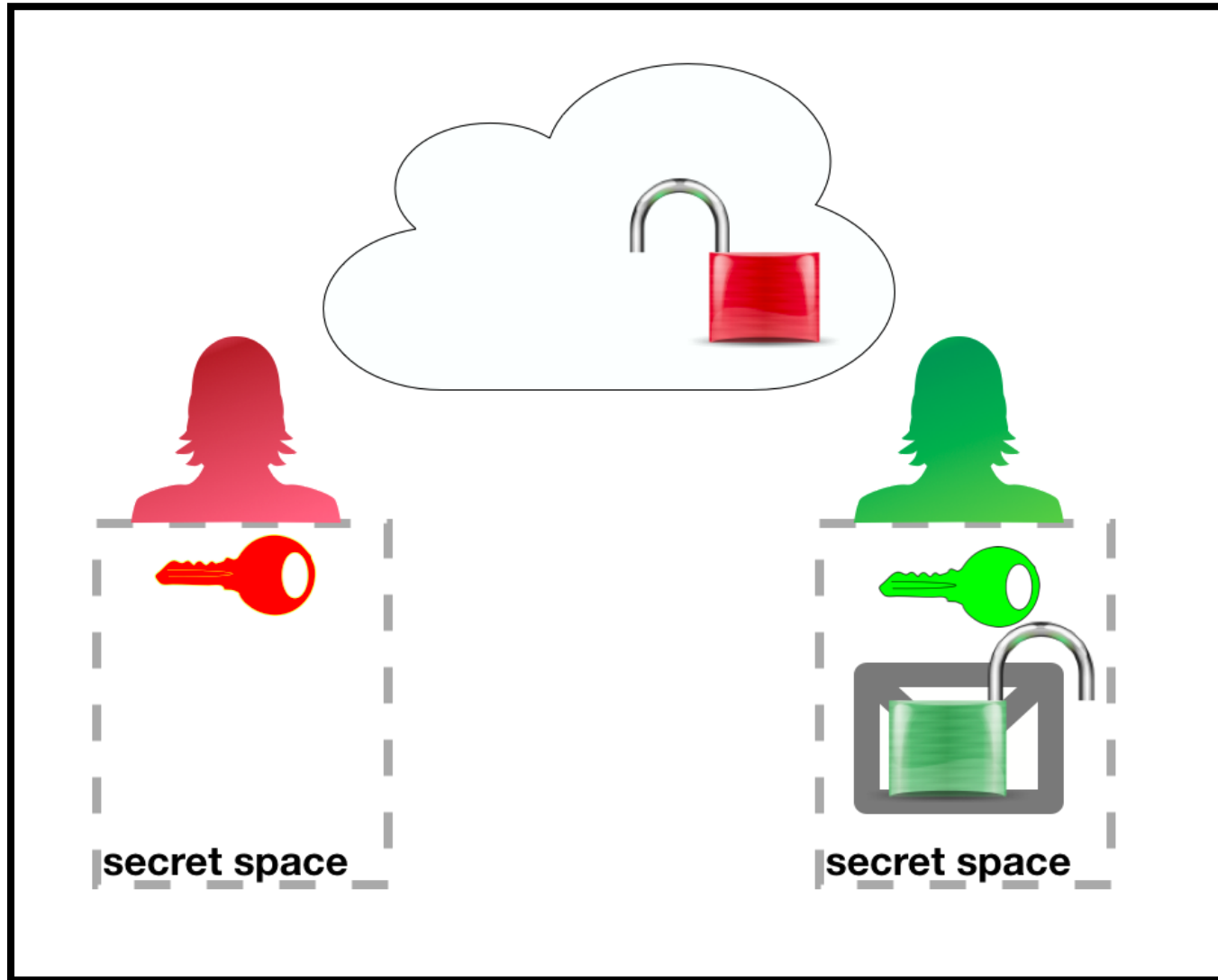
Red encrypts message with Green's public padlock



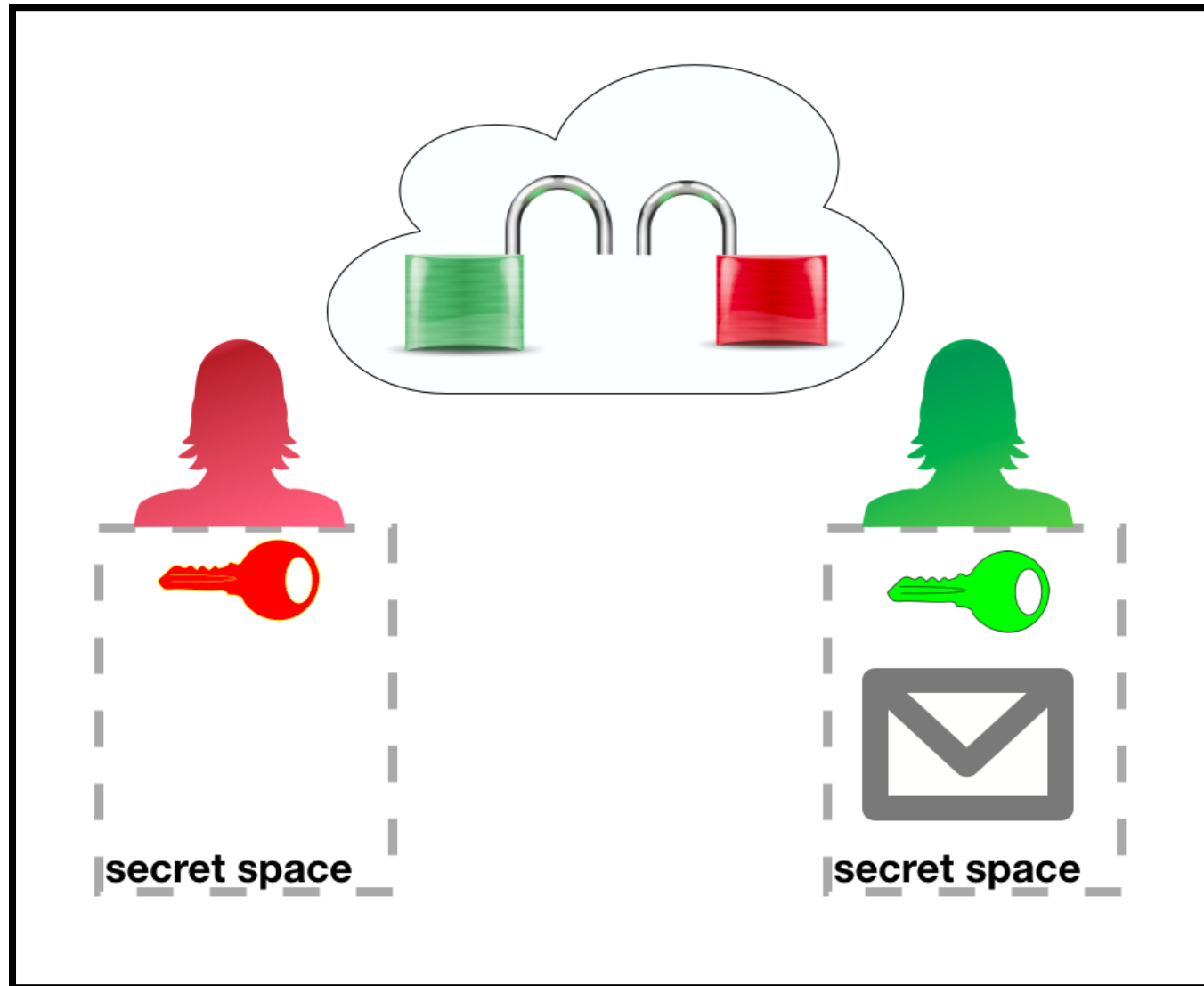
Sent message is unreadable without Green's secret key



Green decrypts the message with their secret key



Done :)



Using PGP to sign things

As well as encrypting messages and files, PGP can be used to sign things:

- PGP signature verifies content and sender of item
- can be used to certify unencrypted emails or files
- will fail if message or file is changed

Using PGP to verify identities

PGP can also be used to verify peoples public keys - by signing a public key you are saying you are confident that the key belongs to the person it says it belongs to.

On keybase this is done by following people. Consider following some of the other people in this workshop while you know that the account is really them.

And how does signing work?

That's where the metaphor stops working. Ask later :)

Solution #3:

Secure messenger / private messaging

What is a secure messenger?

- encrypts message end-to-end per default (i.e. messages are only readable by sender and recipient, not by the message service provider)
- explicitly does not store activity records (metadata)
- is open source
- optional: has self-destructing messages (i.e. messages are deleted on both ends after a pre-defined timespan)

We recommend

Signal

Safely using secure messaging and encryption

- make sure you confirm that the account you are dealing with (Public Key or Signal account) is who you expect to be at the other end
 - verify using separate channel
 - for chat, make sure encryption is working before exchanging any critical information
- your Keybase account is good for improving security, but you should create fresh PGP keypairs for very secure communications

Researcher
privacy

Main risks

when researching on the internet:

- activity record (metadata) retention (by state/institution/ad networks)
 - by IP address (like a 'phone number' for your computer)
 - by browser cookies (like customer cards in shops, just for your browser)
- revealing of personal details to website owners
- other forms of browser finger printing

Activity!

visit <https://browserleaks.com>

Solution #1:

Virtual Private Network (VPN) 'tunnel'

What is a VPN?

- prevents eavesdropping, e.g. in an open WiFi
- hides your IP address (i.e. location, internet provider, other visited websites) from servers you communicate with
- can make you appear to be in another country and circumvent DNS or geo-blocking
- does NOT replace https

We recommend

Choose a VPN service which:

- claims not to store activity records (hard to verify)
- uses OpenVPN
- has servers in safe jurisdictions
- not insert advertising into your browsing stream

Remember that if it's too cheap you might be paying in other ways.

[NordVPN](#) and [Private Internet Access](#) both have a long term high reputation

Solution #2:

Tor Browser

What is Tor Browser?

- provides secure browser that doesn't leave traces (e.g. it does not store cookies)
- onion-network (encrypted tunnel through encrypted tunnel through encrypted tunnel ...)
- does not prevent you from disclosing your identity e.g. by logging into Facebook

We recommend

Use for TorBrowser high risk research, not for everyday use.

Group activity!

Install Tor Browser and visit <https://browserleaks.com> again.

Tor Browser:

<https://www.torproject.org/projects/torbrowser.html.en>

Data storage

Main risks

when storing data:

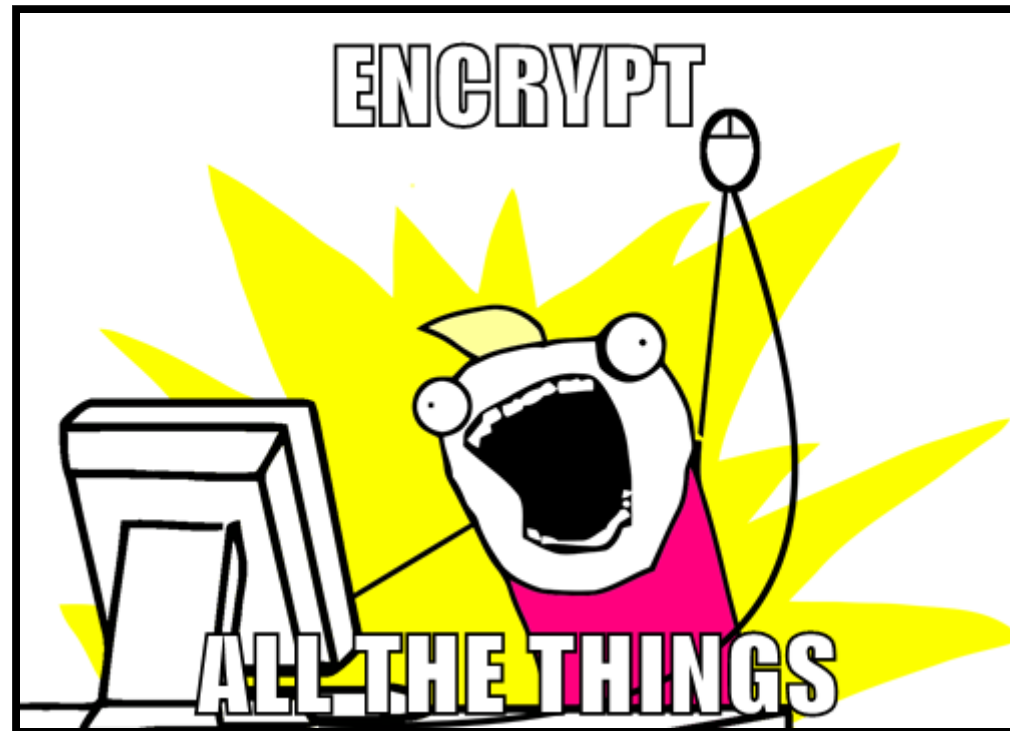
- unauthorised access to data, e.g. in the cloud
- unwanted access to devices, e.g. if stolen or taken by authorities
- data loss
- lost access

Solution

backup, backup,
backup

3 independent copies

AND



... but don't forget your keys. (*hint: use a password manager*)

We recommend

- full device/disk/USB stick ... encryption (mostly provided by OS)
- for files in the cloud:
 - [Cryptomator](#)
 - [keybase](#)
 - disk image encryption by your operating system

MAKE SURE YOU NEVER LOOSE YOUR KEYS OR
PASSPHRASES!!! Or all will be lost.

How to choose a
tool?

Things to consider

1. Open Source?
2. Reputation?
3. Independent security audit?
4. Will you actually use it?

Where to from here?

At end of the presentation there is a list of all the software we've mentioned today and a list of useful websites for more information.

- Start using some of these tools!
- Use the suggested websites to become better informed!
- Keep your devices' software & application software up to date!

Get expert advice

Depending on the level of risk to you or your research participants you may need to seek advice from a security/privacy expert before you begin your research.

Group activity!

Discuss in your groups how what we have covered today applies to your research.

Questions?

Resources

Password manager

- 1Password <https://1password.com/>
- KeePass <http://keepass.info/>
- KeePassX <https://www.keepassx.org/>
- KeeWeb <https://keeweb.info/>

2-factor-authentication

- Amazon AWS MFA (Android)
<https://www.amazon.com/gp/product/B0061MU68M>
- Authenticator (Windows Phone 7)
<https://www.microsoft.com/en-us/store/p/authenticator/9wzdncrfj3rj>
- FreeOTP <https://freeotp.github.io/>
- Google Authenticator (Android/iPhone/BlackBerry)
<https://support.google.com/accounts/answer/1066447?hl=en>
- Authy <https://www.authy.com/app/>

Privacy

- Browser leaks <https://browserleaks.com>
- HTTPS Everywhere <https://www.eff.org/https-everywhere>
- NordVPN <https://nordvpn.com/>
- Private Internet Access
<https://www.privateinternetaccess.com/>
- Tor Browser:
<https://www.torproject.org/projects/torbrowser.html.en>

file/device/communication encryption

- Cryptomator <https://cryptomator.org/>
- Enigmail for Thunderbird
<https://www.enigmail.net/index.php/en/>
- GPGTools <https://gpgtools.org/>
- keybase <https://keybase.io/>
- Signal <https://whispersystems.org/>

websites

- CryptoParty <https://www.cryptoparty.in/>
- Electronic Freedom Foundation (EFF)
 - Privacy <https://www.eff.org/issues/privacy>
 - Surveillance Self-Defense <https://ssd.eff.org/> This has overviews, tutorials, and detailed guides for specific situations.
- Snitch Hunt Game
<http://whistleblower.network/snitch/index.php>
- Snitch Hunt news article
<http://www.abc.net.au/triplej/programs/hack/how-team-of-pre-teens-found-whistleblower-using-metadata/8113668>
- Examples of Bad SSL certificates <https://badssl.com/>

Glossary of terms

- browser cookies: like customer cards for your browser to store information about you that can be read by the website when you return
- encryption: making data practically unreadable without another piece of data (see keyfile) and/or password that's usually kept secret
- end-to-end encryption: encryption from a senders device to a recipient device without intermediaries being able to decrypt

Glossary of terms

- https: HTTP over SSL <https://en.wikipedia.org/wiki/HTTPS>
- IP address: number to identify your computer/router to another computer, mostly a server serving you a website
- keyfile: think of it as a password, but in a file.
- metadata: activity records
(<https://twitter.com/Snowden/status/66130556696756224>
or more detailed: <https://ssd.eff.org/en/glossary/metadata>)
- ssl or tsl: Secure Sockets Layer / Transport Layer Security
https://en.wikipedia.org/wiki/Transport_Layer_Security



@brendam @flxvctr

QUT DMRC Summer School 2017