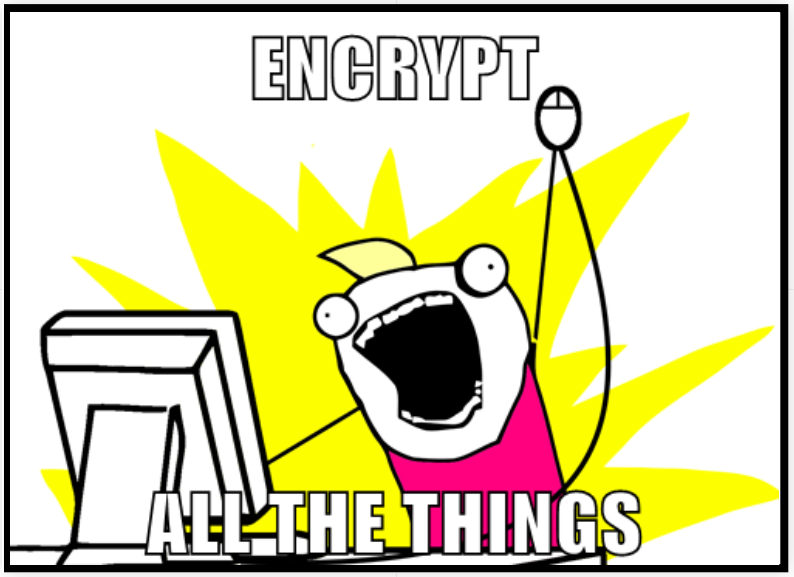


... but don't forget your keys.

(Digital Privacy & Security for Researchers)

DMRC Summer School Workshop 2019, 11-15 February

Brenda Moon

image: http://blog.serverfault.com/files/2016/02/encrypt-all-the-things1.png (based on original by http://hyperboleandahalf.blogspot.com.au/)

https://qut-dmrc.github.io/encrypt_all_the_things/

@brendam | @flxvctr

Why are we here?

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

Activity!

visit https://browserleaks.com

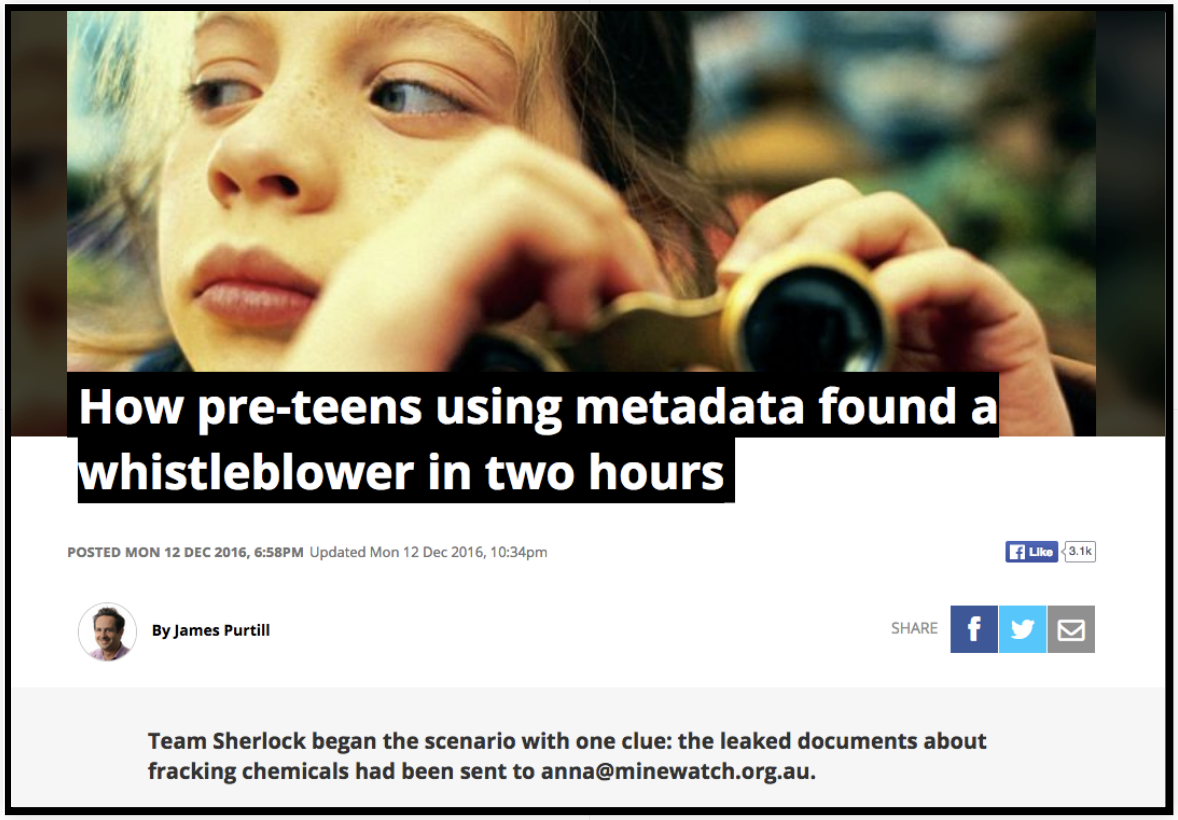
unencrypted communication

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

Metadata retention



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 Purtill

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-whisteblower-using-metadata/8113668)

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

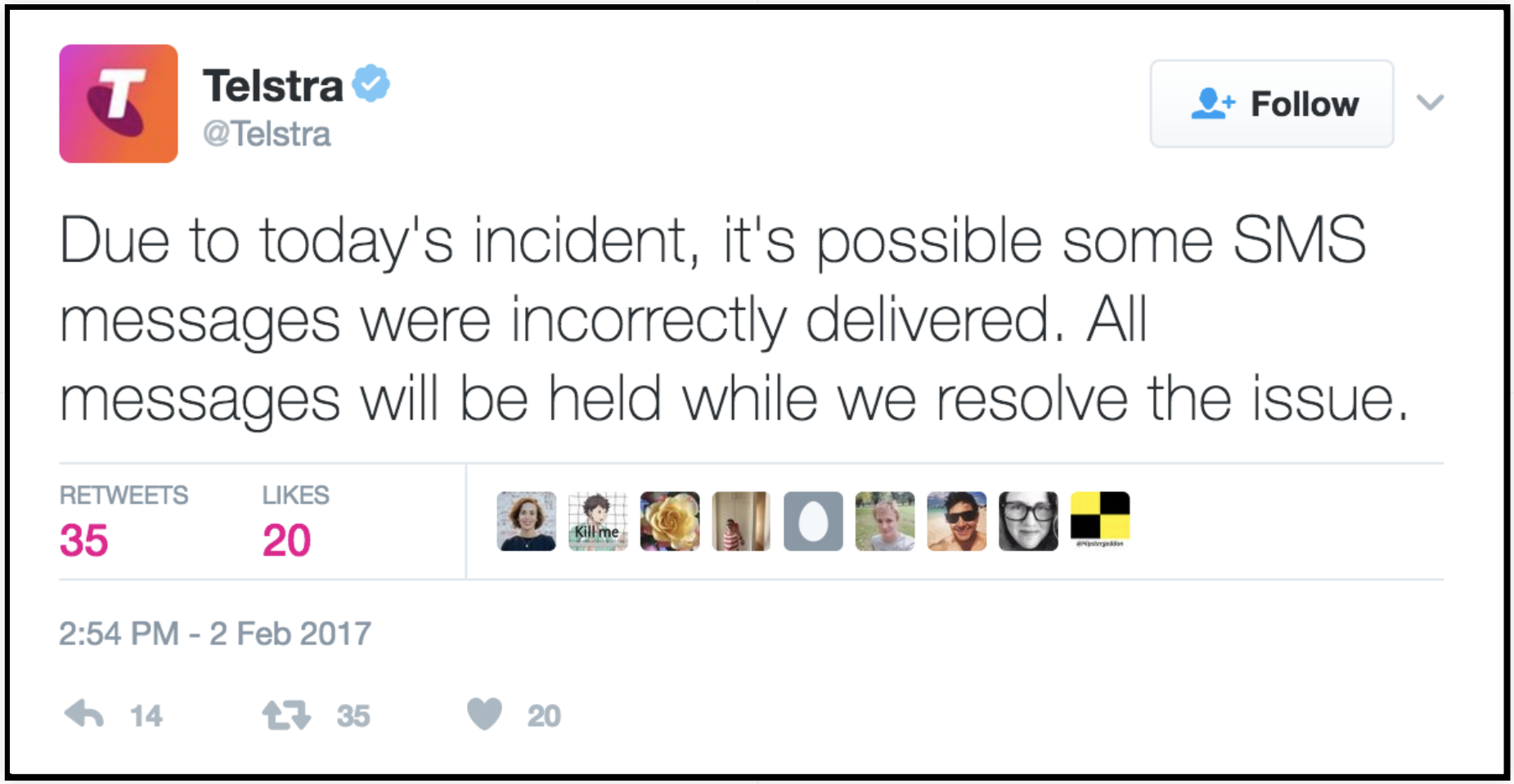
Solution #2:

Use 2-factor authentication

What is 2-factor authentication?

- 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!



SMS problems

- mis-delivery
- 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)
- Authenticator (Windows Phone 7)
- Authy

Which services provide 2-factor-authentication?

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

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 had a long term high reputation. The new ProtonVPN by the team behind ProtonMail seems to be good too.

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 TorBrowser for high risk research, not for everyday use.

Activity!

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

Tor Browser: https://www.torproject.org/download/download.html.en

Data storage

Main risks

when storing data:

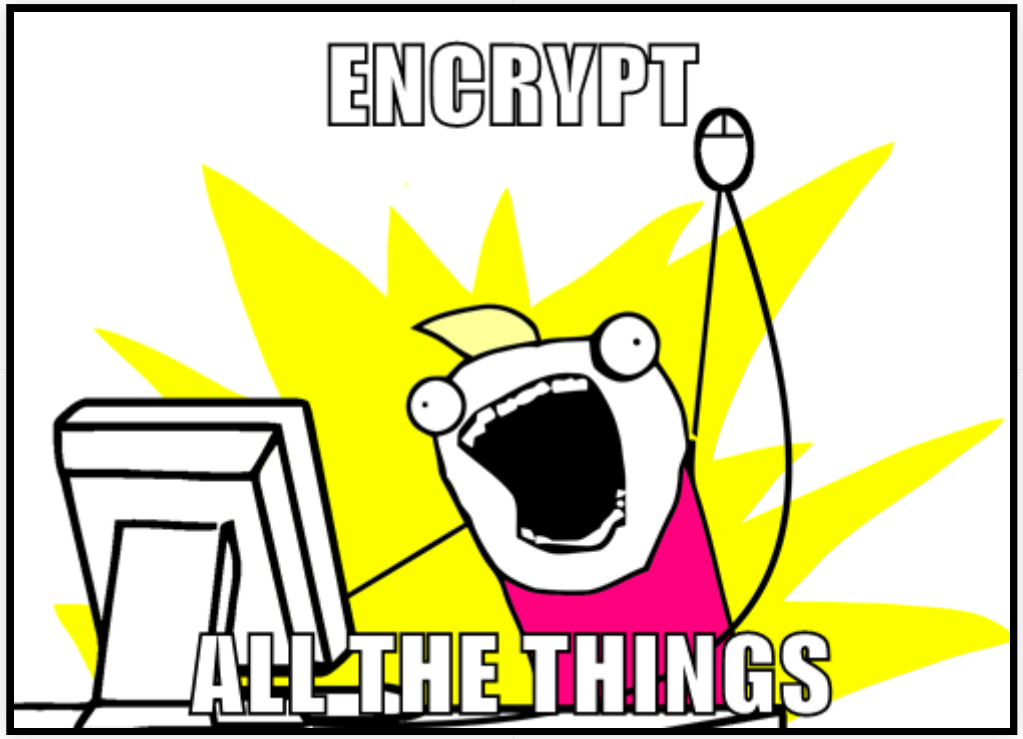
- unauthorised access to data, e.g. in the cloud
- unwanted access to devices, e.g. if stolen or taken by authorities
- data loss
- lost access

Solution

backup, backup, backup, backup

3 independent copies, 2 locations, 1 offline

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.

Communication

Main risks

While transmitting sensitive information: the men in the middle (MTM)

- 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:

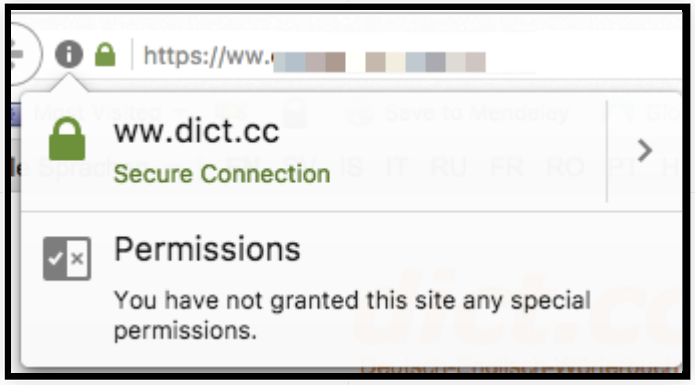
https

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 for MacOS
- GPG4win for Windows
- Enigmail for Thunderbird
- email clients with GPG support

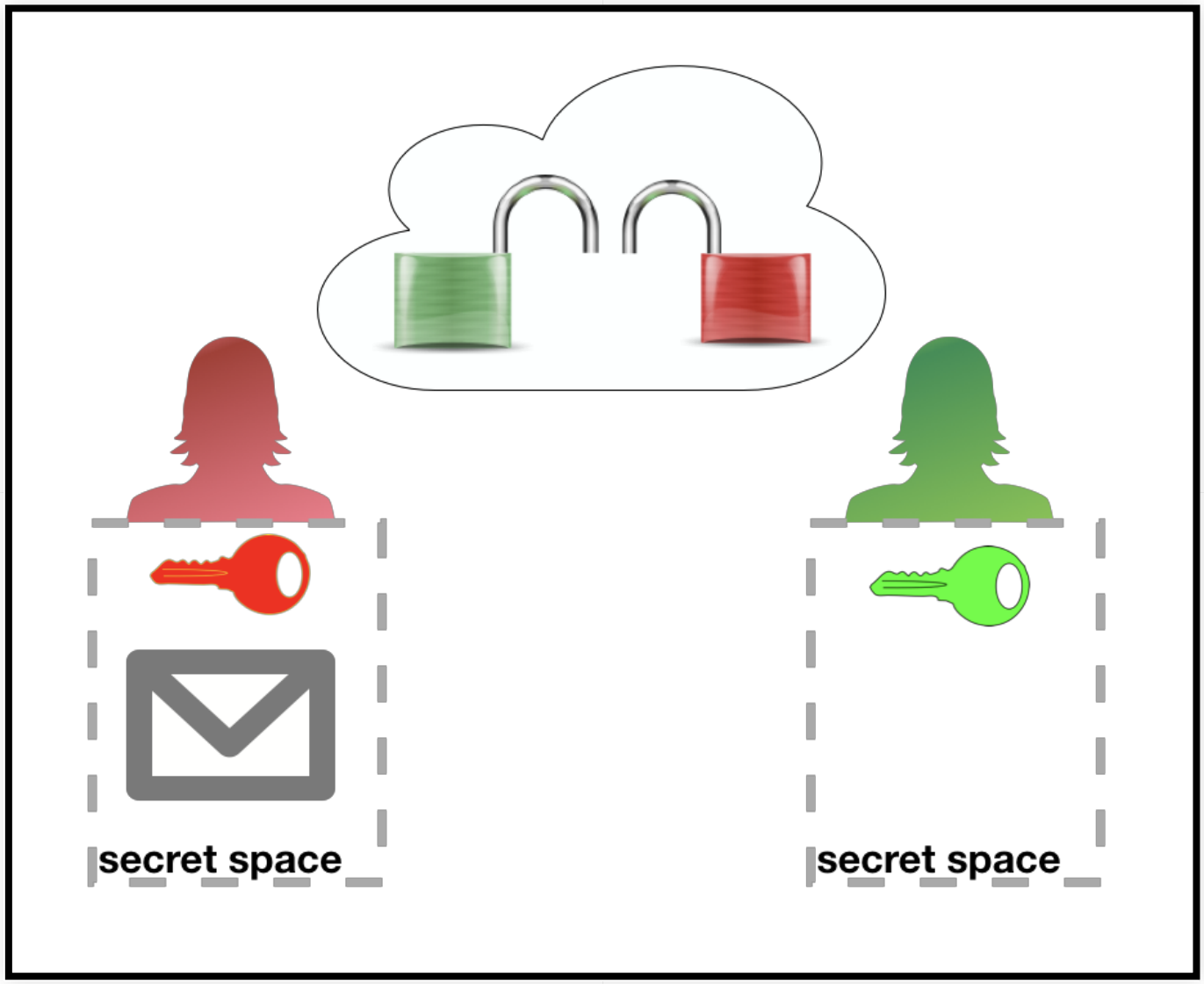
Using Keybase

With an account on keybase.io it is easy to encrypt a message to somebody else. Let's try it!

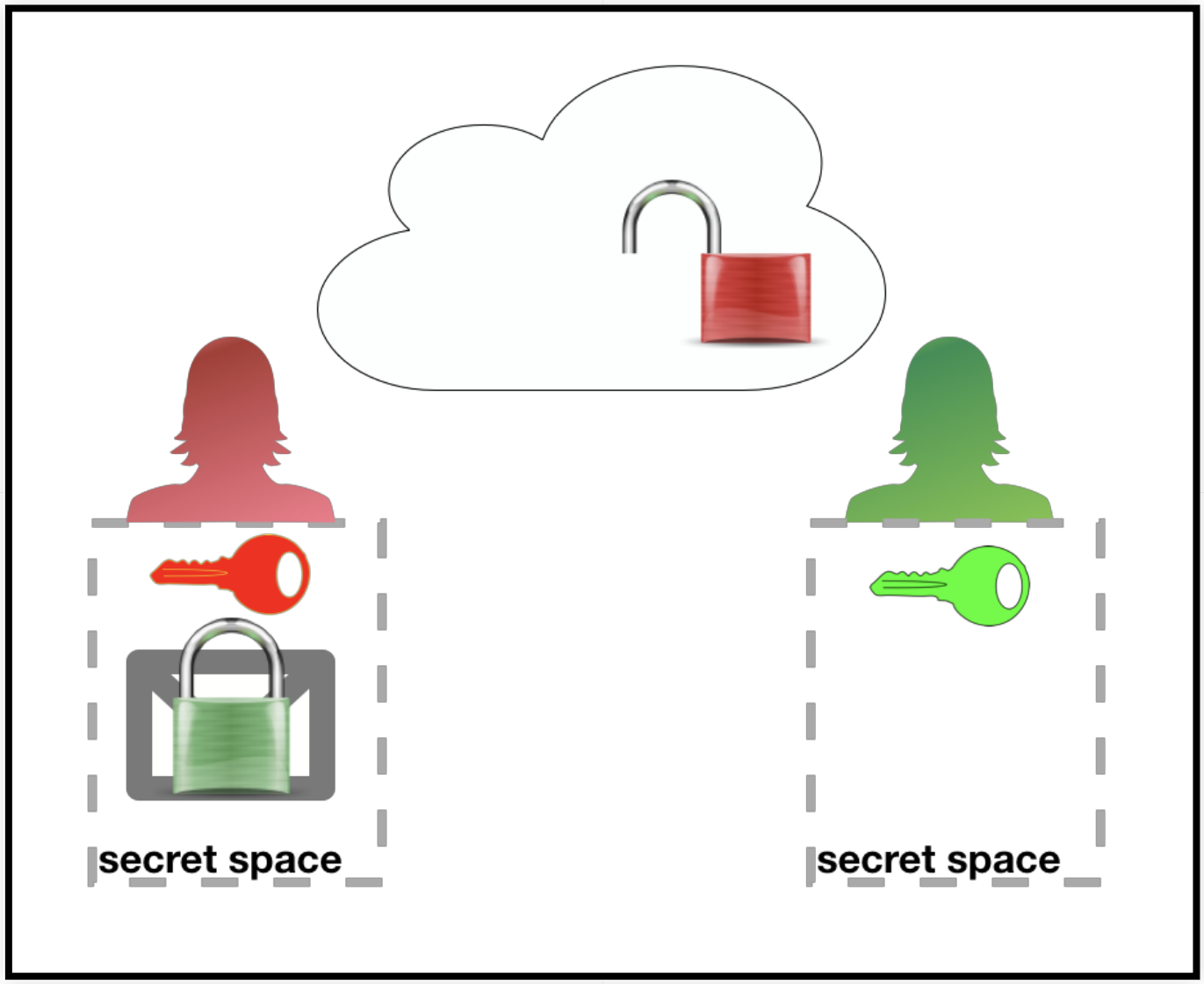
Whoot! So how did that work?

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

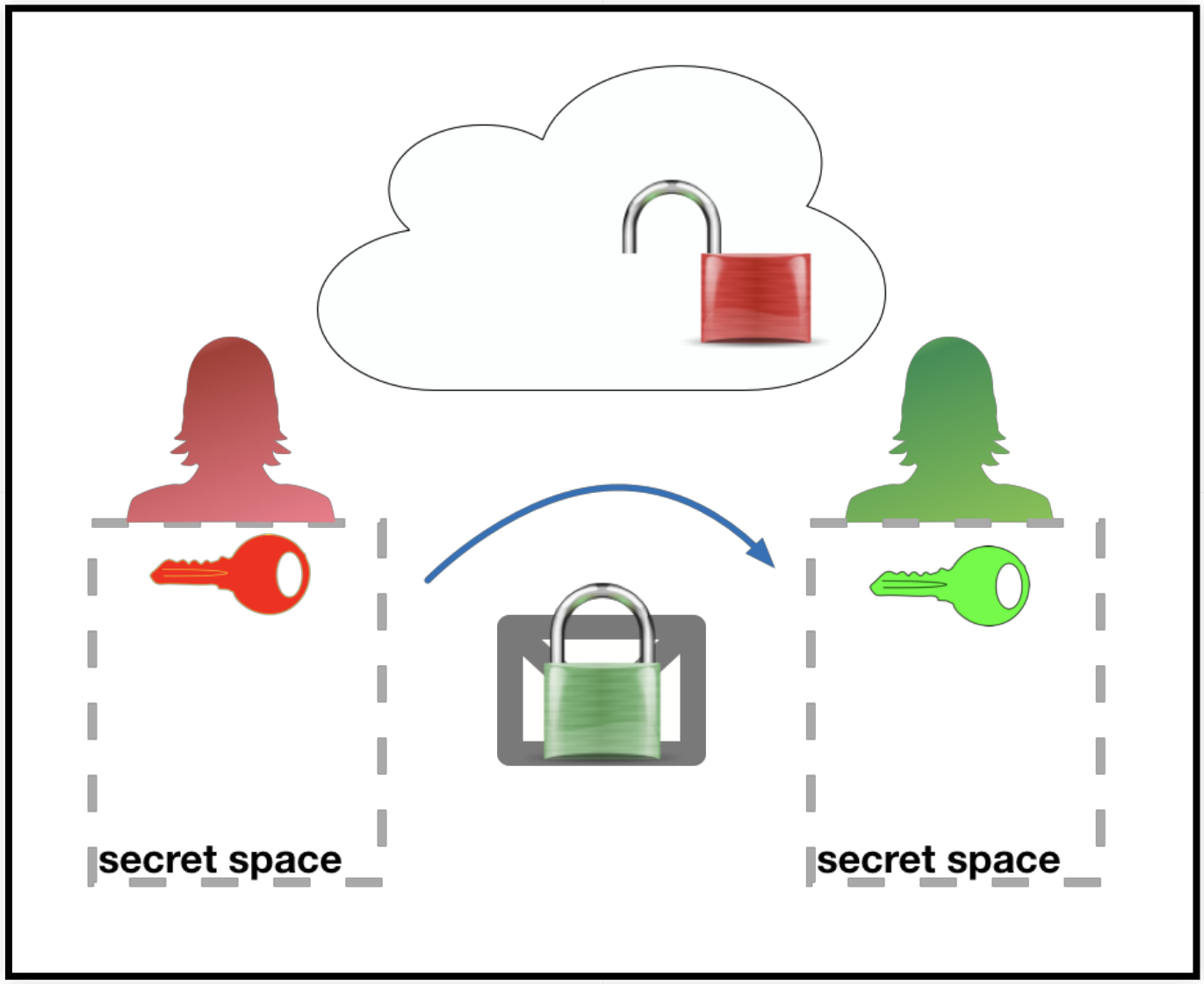
Red has a secret message for Green



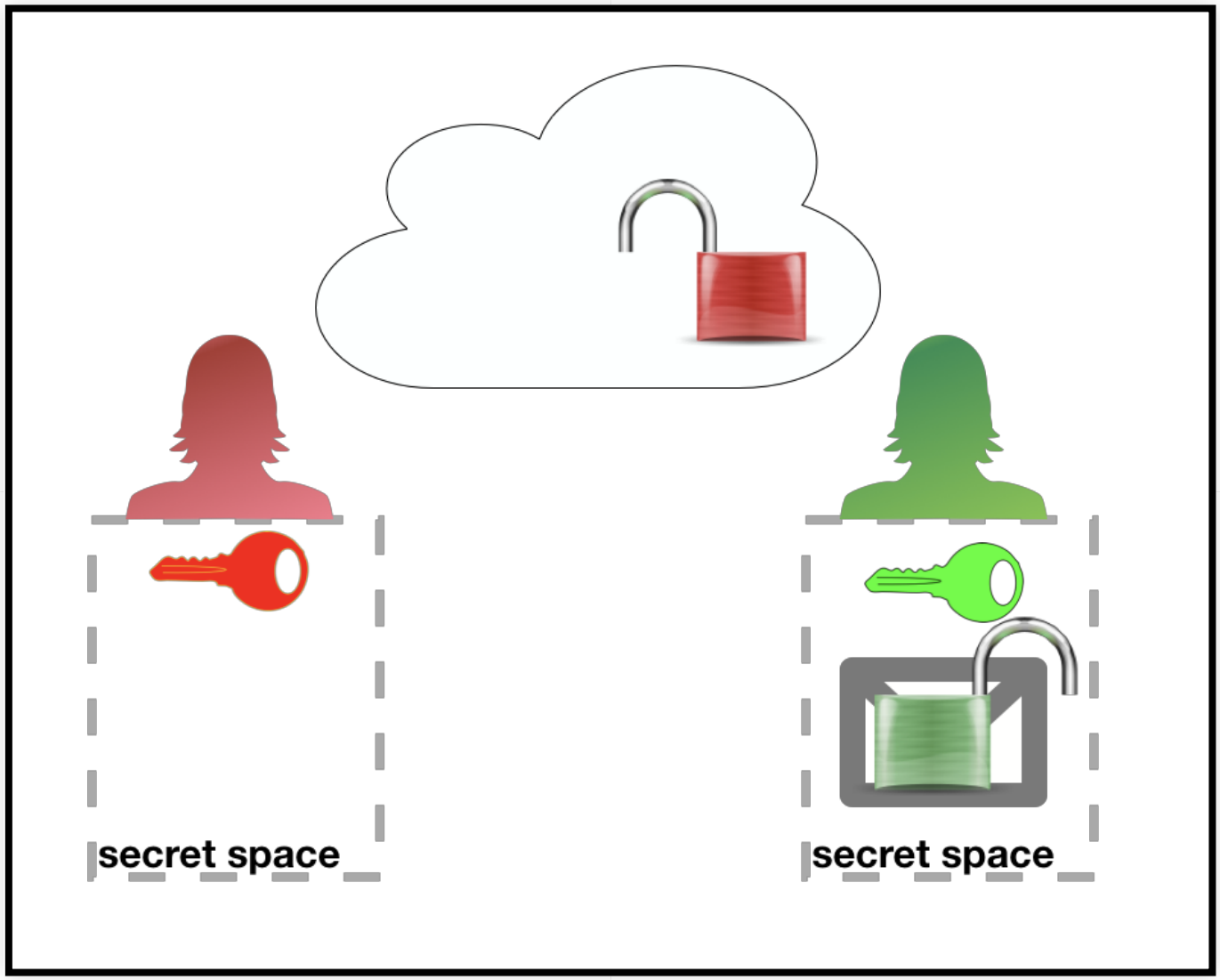
Red encrypts message with Green's public padlock



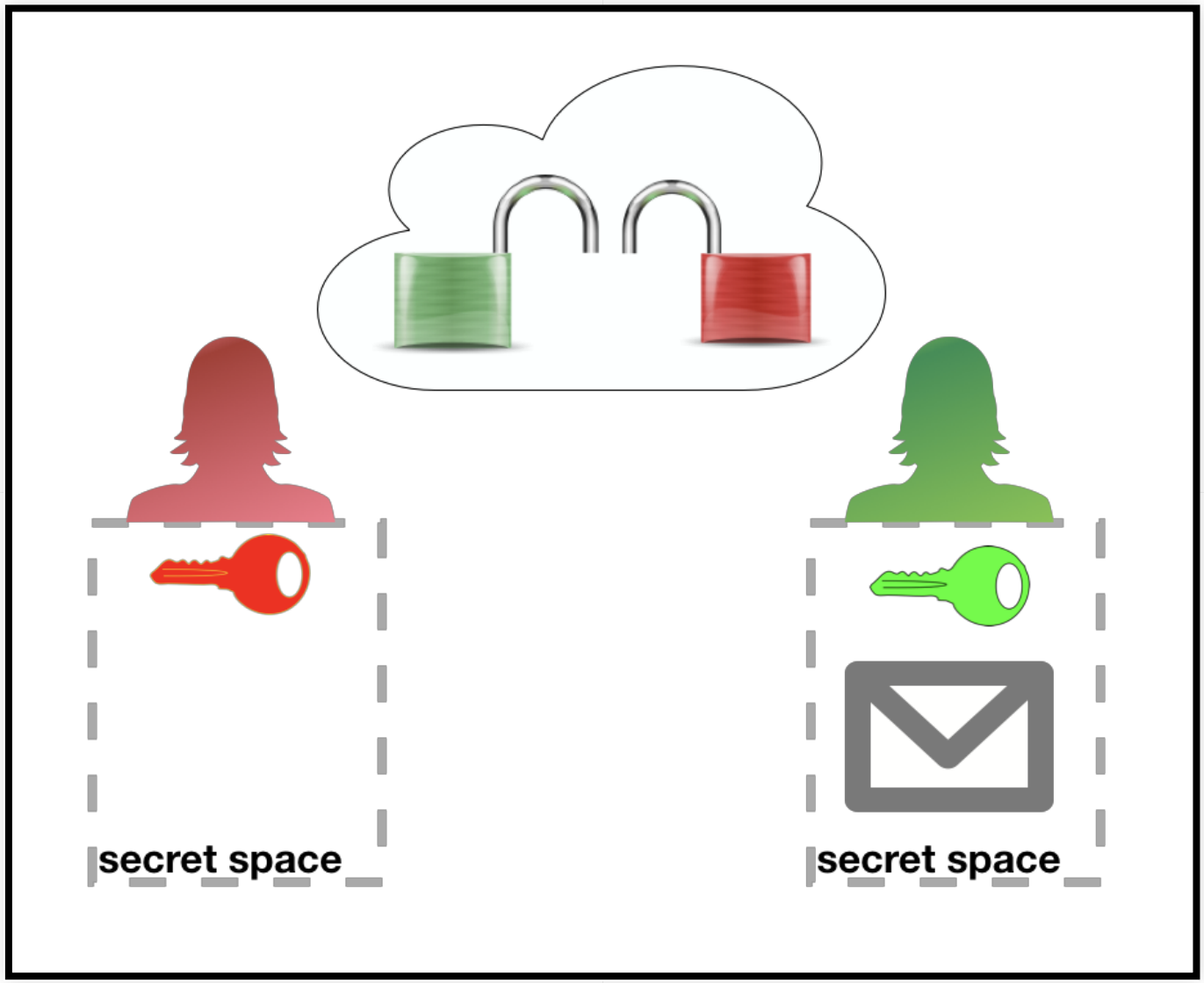
Sent message is unreadable without Green's secret key



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.

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

keybase

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 informaiton
- your Keybase account is good for improving security, but you should create fresh PGP keypairs for very secure communications

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

- What did you get out of this session?
- What privacy or security issues might effect your research?

Questions?

Resources

Password manager

- 1Password https://1password.com/
- KeePass http://keepass.info/
- KeePassXC https://keepassxc.org/
- KeeWeb https://keeweb.info/

2-factor-authentication

- 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
- detailed VPN comparison https://thatoneprivacysite.net/
- 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-whisteblower-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/661305566967562240) 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