# Security Basics

Paula Graham Gazzard | Fossbox

@pmgazzx

@fossbox

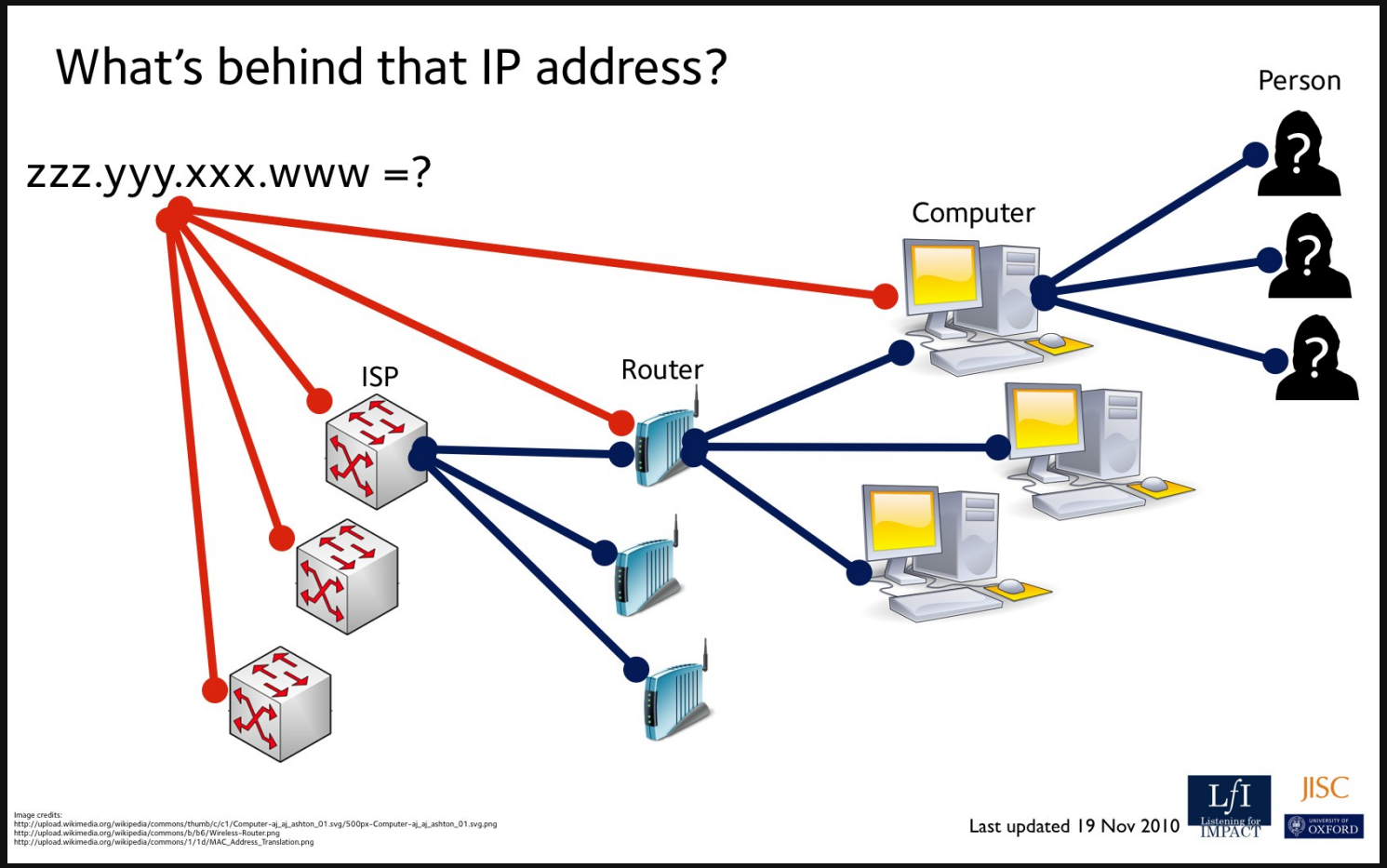
# Should I care?

- Security used to be about keeping people out of your computer
- Now it's best to assume your computer/phone might be breached
- What data do you have? – contacts, passwords, identity, networks, history
- Who might want it? What stops them?

# You don't leave your front door open – lock your data!

- Passwords – Keepassx: http://www.keepassx.org/
- Key encryption (asymmetric): http://is.gd/CxYyVB
- Keys and keyrings – Mail keys: Enigmail key manager (http://is.gd/XboWCT ), Linux key manager: Seahorse (http://is.gd/dDiTHT ), Android key manager: Openkeychain ( http://is.gd/fVuK9t ), KeySync https://guardianproject.info/apps/keysync/

# Everything on the internet has a number



# MAC addresses

- A Media Access Control identifier is a unique number
- It identifies every device connected to a network
- Your network cards have MACs
- Your cam, mic and other 'on board' devices may also have MACs
- MACs and IP addresses are used as part of your unique digital identity

# Location:

- Networks (cellnet towers) and time-difference
- Location sensors – A-GPS chip
- Wifi, ultra-wideband-tracking (pulse radio), Bluetooth, RFID (near-field),
- Location is inadvertently leaked through social and dating networks etc

# Email is like a postcard – put it in an envelope!

- Enigmail with GNUPG
- Data retention (RIPA) http://is.gd/p0CsS9 – 100,000 RIPA requests every year, including private individuals and journalistic sources http://is.gd/pkduex
- ISPs who don't retain your mails eg
  - Riseup: http://riseup.net/
  - Autistici: http://is.gd/EO2C9t

# Wifi is a polluted fishbowl

- Aircrack is used for cracking wifi, capturing data, intercepting/impersonating communications
- Firesheep can see/hijack your social networks
- 'Darkhotel' uses cracked wifi to offer fake software upgrades infected with malware and steal data
- Spoofing can use your device identifier to crack paid wifi (and do god-knows-what) with your ID
- Use a VPN (L2TP/IPsec: 256-bit AES) and openVPN client, choose a provider who logs minimal data about you and your activity and check server location – https://privatevpn.com/ service has a good reputation

# How can they see tiny me?

- Every day, FB now generates 300 petabytes of data
- In 2008, Google processed around 20 petabytes of data per day
- Your browser leaks uniquely identifiable information
- This can be used to match up your digital trail and automate creation of profiles (digital shadow) exchanged by corporations, security services and criminals
- More: http://is.gd/gzkT2I http://is.gd/dmbDpX

# Lightbeam

- Cookies are small amounts of data stored by your web browser which tracks your activity and can be read
- Third-party or 'tracking' cookies are used to bring browsing history data from the different cookies together to profile individuals
- https://www.mozilla.org/en-US/lightbeam/

# Reduce your browser's blabbing!

- http://www.browserleaks.com/
- Flash, Java, WebRTC and Adobe Reader leak badly: Flashcontrol (Chrome) or Flashblock (Firefox)
- Disable WebRTC in firefox: about:config and set media.peerconnection.enabled to false
- Disable geo location in Firefox: about:config set geo.enabled to 'false'
- Noscript, Vanilla (Chrome), Self-Destructing Cookies (Firefox), Adblock

# Anonymity

- VPNs secure your communications but don't anonymise
- If you want to be anonymous use The Onion Router (TOR) – easiest way to use TOR is Tails
- Bear in mind that if you log into **anything** with your normal login, you've de-anonymised yourself
- Tails OS – great for beginners: https://tails.boum.org/
- Tor Browser Bundle (if you know what you're doing): http://is.gd/u19omF

# Smartphones

- All of the above applies in excelsis to smartphones
- Most smartphone apps leak identifiable information ('device indentifier') which can track you across different apps
- The Guardian Project offers a suite of apps to help secure communications https://guardianproject.info/
- VPNs can also be used on mobiles, openvpn client for Android: http://is.gd/2U7yZN

# Can I be totally protected?

- No

# Isn't this a lot of hassle?

- Yes!

# Is it worth it?

- Significantly reduced exposure
- Try to avoid exposing your friends' data without their consent
- Understanding is important – we need an open and informed debate
- There needs to be an ethical framework for 'big data' – thank you for helping us research this!

# Stay in touch!

- info@fossbox.org.uk
- Follow @fossbox on Twitter (Paula's personal handle is @pmgazzx )
- Fossbox mailing list: http://is.gd/HNUhzs
- Fossbox website: www.fossbox.org.uk