# Late Night

goo.gl/q71wPv


John Gallias
JohnGallias.com
@JohnGallias

Breanna Hamm
BreannaHamm.com
@hammbh

First Published: April 28, 2017
Last Updated: April 28, 2017
Expiration Date/Best By: October 2017

# Welcome!

goo.gl/q71wPv

- **All are welcome to attend this workshop!**
- **Codes of Conduct:**
  - https://2017.penguicon.org/code-of-conduct/
- **The provided note cards and pens are for questions. Please submit them to Breanna, and they'll be added to the Google Slide questions.**
- **The QR code is a link to this Google Slides Presentation**

# Large QR Code Link to This Presentation

# Who are we?

**John Gallias**
johngallias.com
Twitter: @johngallias

**Breanna Hamm**
breannahamm.com
Twitter: @hammbh

# Agenda

1) **This Presentation: ~30 minutes**
2) **Live Demo: ~30 minutes**
3) **Open Workshop: Remaining Time**
    - I'll use this time to answer the most popular questions and help you make your own Tails flash drive.

# What is Tails?

Tails: The amnesic incognito live system

- **amnesia**, noun: forgetfulness; loss of long-term memory.
- **incognito**, adjective & adverb:
  - (of a person) having one's true identity concealed.
- **live system**, noun:
  - A complete boot-able operating system which runs fully within a computer's memory, rather than loading from a disk drive

# What is Tails? Explained

- ***A*mnesia, *I*ncognito, what?**
  - By design Tails purposely *forgets* what you did with it after reboot/power-off, and tries the best it can to help you stay *anonymous* and *blend in* while online
- ***L*ive *S*ystem, huh?**
  - Tails loads into memory from CD/DVD/USB media on most Debian compatible computers.
  - We will help you create and use a Tails USB as part of this Workshop!

# Why use Tails?

- Use “anywhere” but leave no trace
- State-of-the-art cryptographic tools
- Online anonymity and censorship circumvention

# Do I Need Tails?

- **You should perform threat modeling (AKA risk assessment) to determine if something like Tails would be helpful to you specifically.**
- **Using Tails effectively also requires Operational Security and Information Security basics (i.e. basic digital hygiene).**

# Threat Modeling / Risk Assessment

- What do you want to protect?
- Who do you want to protect it from?
- How likely is it that you will need to protect it?
- How bad are the consequences if you fail?
- How much trouble are you willing to go through in order to try to prevent those?

# Updates

- **UPDATES**
  - Keep everything you have as up-to-date and as quickly as possible.
  - If you can no longer obtain security updates to your device, it should no longer be  used.

- **Updates vs Upgrades**
  - Updates typically provide security and bug fixes: 2.10, 2.11, 2.12, etc
  - Upgrades may make major changes, include new features, and/or add additional new requirements: 3.x, 4.x, 5.x, etc.

# Passwords

## Strong, Unique, Managed Passwords

- **Strong:** random, different characters, as long as possible.
  - Use Diceware when you need strong, memorable phrases:
    - Quick, Digital Tool: rempe.us/diceware
    - Real world physical Diceware method: eff.org/dice
- **Unique:** Never reuse passwords!
- **Managed:** Use a Password Manager!
  - KeePass (Included in Tails), PasswordSafe, LastPass, etc.
    - Most include a Password Generator: USE IT!

# Two Factor Authentication

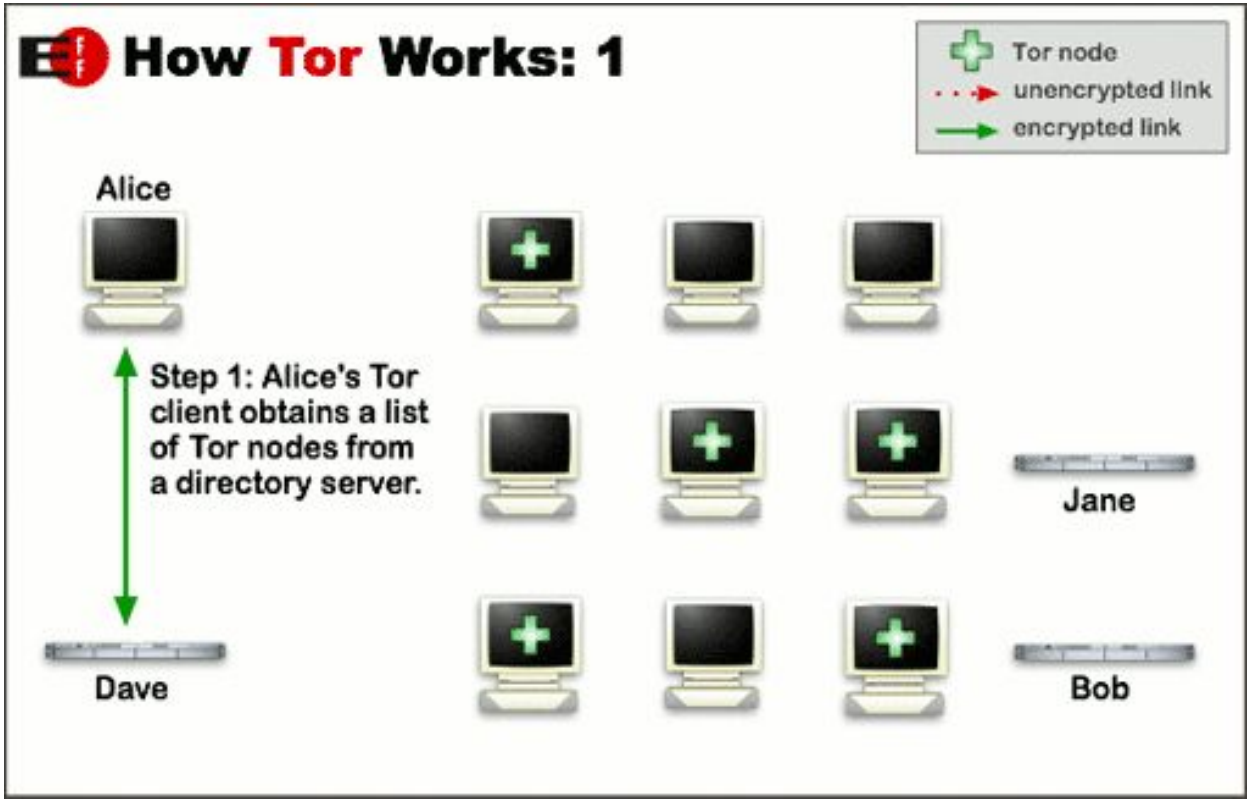
- **Turn on Two Factor Authentication for as many services as possible**
- **turnon2fa.com for step-by-step screenshot how-tos**
- **I personally recommend Authy to keep Google Authenticator style codes**
  - Authy allows separation from the password manager, but requires trust in another third-party cloud service.
  - DUO Security is also recommended when available.

# Tor

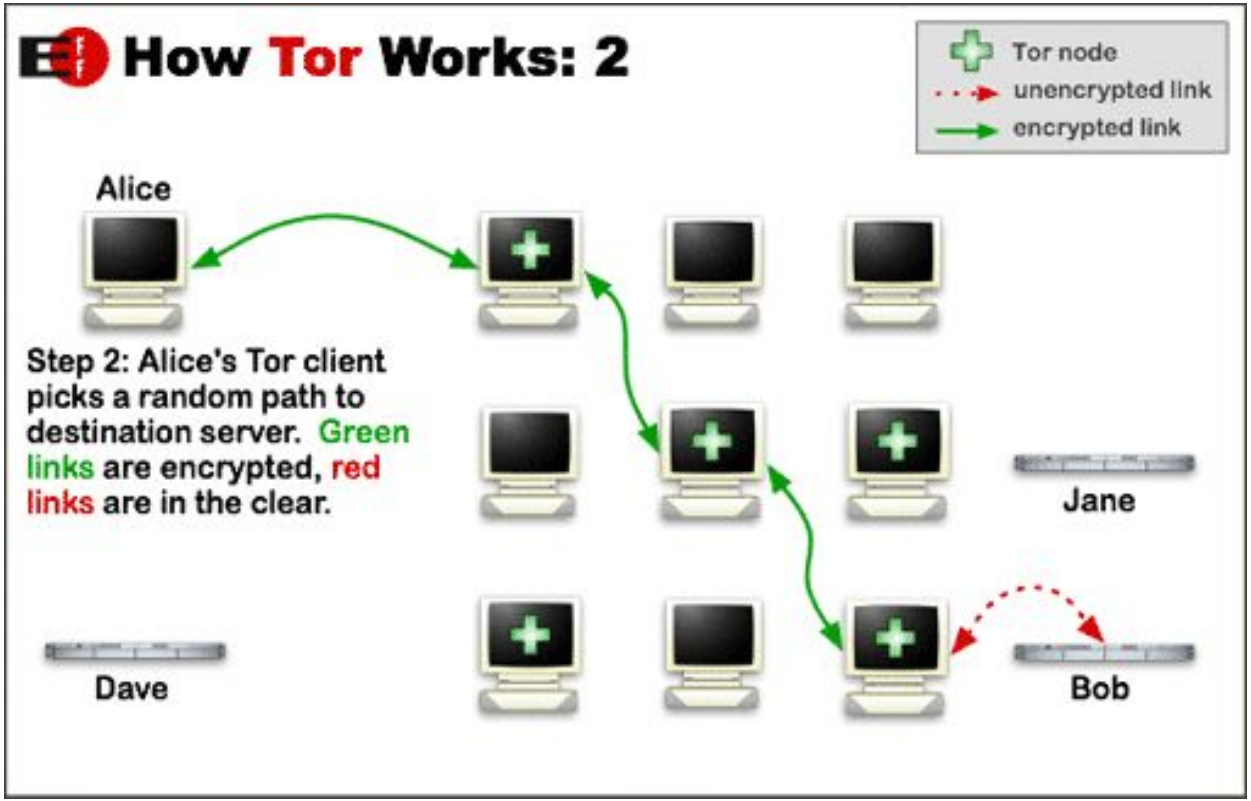
- **Once connected to the Internet, Tails will enable and force all browser traffic through Tor for your protection.**

- **Tor is free software and an open network**
  - It helps you defend against traffic analysis, a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security.

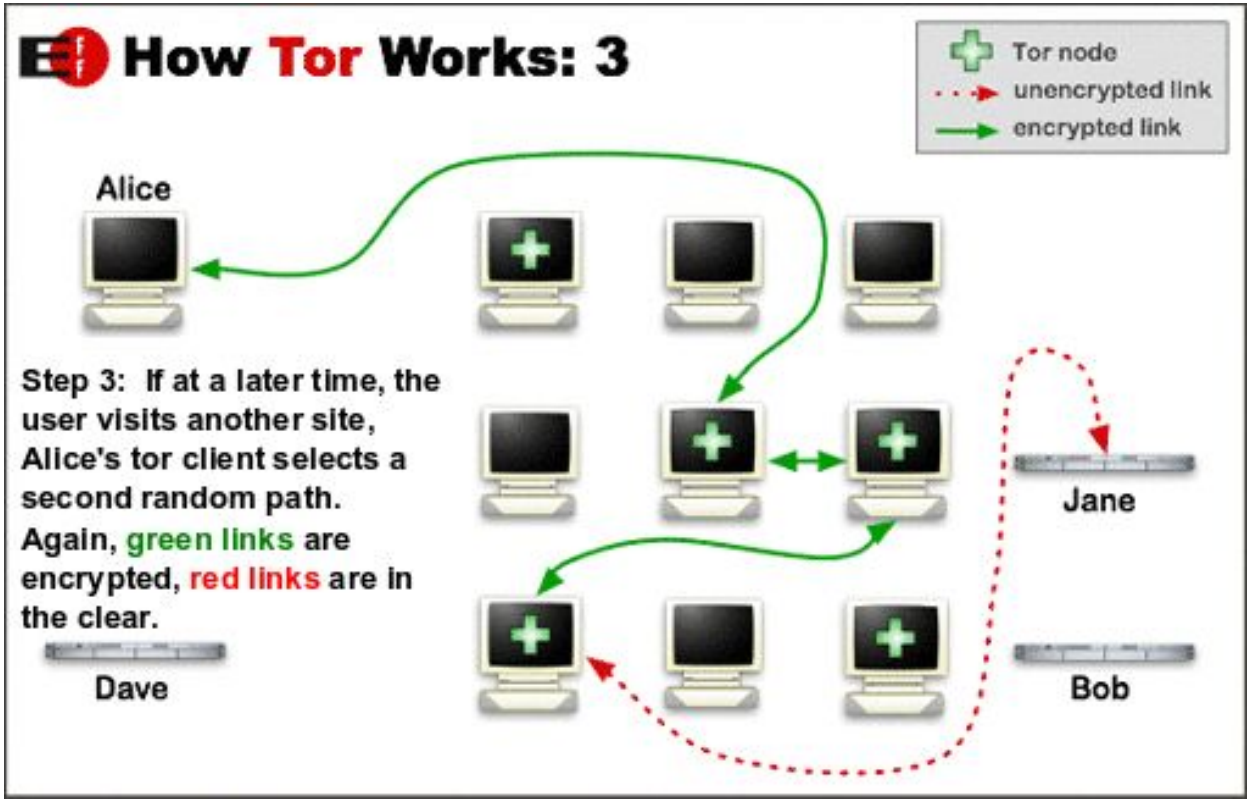
# How Does Tor Work?



# How Does Tor Work? Continued...



# How Does Tor Work? Continued...



# Who Can/Should Use Tor?

- **Normal people, Journalists, Law enforcement, Activists, Whistle-blowers, High/low profile people, Business executives, Bloggers, Military, IT Professionals, Anyone, YOU!**

# Why Tails + Tor?

- **Using Tor through Tails helps you access websites safely.**
  - It works at the Operating System level to help maintain anonymity and prevent possible leaking of personally identifiable information.

- **Why can’t I just use Tor Browser Bundle?**
  - Tor Browser Bundle alone cannot protect against tracking and fingerprinting. Simply opening a PDF that bypasses the Tor Browser Bundle connection could result in your computer and identity being revealed.

# Keep Tails Up To Date!

- **Remember our Basic Digital Hygiene from earlier: UPDATES!**

- **Tails will automatically check for updates each time it connects to Tor. Please always allow it to perform updates as soon as possible! This is important for both bug fixes as well as security!**

# Tails “Encrypted persistence”

- **Allows you to save data that will survive reboot (persistent) to the same USB drive that Tails is installed to.**

# Tails “Encrypted persistence” Disclaimer

**WARNINGS:**

- The persistent volume is not hidden.
- Changing the default configurations can break your anonymity.
- Installing additional programs may introduce unpredictable problems and may break the protections built-in Tails.
- If you install other plugins or change their configuration, you can break your anonymity.
- Use the persistent volume only when necessary and to the minimum.
- It is possible to open the persistent volume from other operating systems, but it might break your security.


tl;dr

# Why a persistent volume then?

## Provided you accept the risk, Persistence features include

- Personal Data, GnuPG, SSH Client, Pidgin (Chat, OTR, XMPP), Icedove (E-mail), GNOME Keyring, Network Connections, Browser bookmarks, Printers, Bitcoin Client, APT Packages, APT Lists, Dotfiles, Additional software packages

# Warning: Do you trust the Hardware?

- **LightEater Demo: Stealing GPG keys/emails in Tails via remote firmware infection (Published on Jun 5, 2015):**
  - https://youtu.be/sNYsfUNegEA

- **What this means is:**
  - Tails can be compromised via malicious use of SMM (System Management Mode) in the EFI/BIOS.
  - Do NOT boot and use Tails on unknown/unverified hardware.
  - Chain of custody is very important!

# What's Next? / What Now?

- **CryptoParties!**
  - Ann Arbor CryptoParty: a2crypto.party
  - Find a CryptoParty: cryptoparty.in/location
- **EFF Surveillance Self-Defense**
  - ssd.eff.org
- **Other great sites:**
  - GetProtected.io, PrivacyTools.io

# What's Next? / What Now? (Continued)

## Great people to follow on Twitter:

- matt mitchell ( @geminiimatt )
  - Follow @geminiimatt's "THE LIST" on Twitter for ongoing infosec community news and updates.
- Micah Lee ( @micahflee )
- Brain Kerbs ( @briankrebs )
- EFF (@eff )

# How do I use Tails?

- **Tails must be booted in BIOS mode (No UEFI) and Secure Boot must be disabled.**
- **Most Debian compatible systems will work**
  - Lenovo 11e Series works great
- **Tested, Known Working Flash Drives:**
  - Lexar JumpDrive S75 16GB USB 3.0 Flash Drive – LJDS75-16GABNL
  - Kingston DataTraveler G4 DTIG4/16GB

# Live Demo / Hands-on Workshop

- If you have a Windows computer, we can walk through it together!
  - I also have macOS and Debian Linux Laptops available to help download, verify, and create Tails from.
- Bring us at least a 4GB Flash Drive, and we'll make it run Tails!

# Sources

goo.gl/q71wPv

**Tails – About:** tails.boum.org/about/index.en.html

**Tails – Encrypted persistence:**

tails.boum.org/doc/first_steps/persistence/index.en.html

**Tor: Overview:** torproject.org/about/overview.html.en

**Tor – Inception:** torproject.org/about/torusers.html.en

**Cute tl;dr cat:** blogs.vmware.com/tam/2016/01/tldr.html

# Sources (Cont.)

goo.gl/q71wPv

**Threat Modeling Questions:**
ssd.eff.org/en/module/introduction-threat-modeling

**How to Lead a Digital Security Workshop:**
motherboard.vice.com/en_us/article/how-to-give-a-digital-security-training

**Digital Security Training Resources for Security Trainers, Spring 2017 Edition:**
https://medium.com/cryptofriends/digital-security-training-resources-for-security-trainers-spring-2017-edition-e95d9e50065e

# Sources (Cont.)