Protecting your Digital Identity

Me

- James O’Keefe
- History/Econ Grad
- Breaking computer software for a living since 1990
- Teaching Computer Privacy since 2011
- Chair, Massachusetts Pirate Party
- Reach me at: jokeefe@jamesokeefe.org

In the physical world we:

- Close and lock our doors;
- Put up blinds or window shades;
- Cover ourselves with a towel when we get out of the shower (well most of us);
- Require police to have a warrant to enter our houses.

Threats

- You know about the threats to your physical security that you face and how you can protect yourself;
- You can identify the threats you face on-line
- There exists a balance between being paranoid and locking your computer and life down and between throwing up your hands and saying you have no privacy.

Threat Modeling

- What do you want to protect?
- Who do you want to protect them from?
- What harm would come to you if it happened?
- What measures can you can take to protect them?

The threats a teen faces are different from an adult. Those an adult faces are different a senior.

See: https://masspirates.org/wiki/images/e/e0/Threat-model.pdf

Possible Threats

- Your hard disk crashes? – Back up your data frequently
- Someone breaking into your bank, PayPal, investment account? – Long, complex passwords
- You accidentally download malware that encrypts your computer and charges you a Bitcoin ransom? – Back up your data frequently
- Someone committing credit fraud on you? – Freeze your credit

Possible Threats

- ISP monitoring your traffic? – Use a VPN
- Ad Trackers are everywhere – Install NoScript Browser Plugin / Clear your cookies / Use Tor
- Phone GPS tracking? - Remove apps that are part of ad networks (Facebook/Google) or turn your phone off sometimes
- Wary of Google tracking you? - Try DuckDuckGo.com or StartPage.com for search or protonmail.com for e-mail

Secure Yourself

- Apply security patches to your computer/phone
- Update the software you use with security patches
- Get a virus checker and keep it up to date
- Back up early and often

Passwords

- We have too many accounts, resulting in too many passwords
- Too many people use simple passwords or use the same password for multiple accounts
- Don’t do that as it puts you at risk

Passphrases not passwords

- Don’t think of them as passwords. Think of them as passphrases
- The longer and more random the passphrase the better
- A 40 character passphrase made up of lower case letters beats a 10 character password using special characters always: 3.97 * 10^56 vs 2.82 * 10^18

Passphrases

- The longer and more random the better
- Never use a single word or common password like password or 1234, since those are easy to crack
- When you need to remember your passphrase, pick four or five random words and turn them into a phrase
- NEVER repeat the same passphrase with different accounts or devices

Manage your Passphrases

- A password/phrase manager is a database of your account details that saves the database as an encrypted file that you unlock with its own pass phrase
- They can also generate a long random passphrase for you
- Some Apps: KeePass.info, LastPass, 1Password
- Depending on the threats you face, a notebook that is always with you or is kept in a secure place may also work

Don’t rely on just passphrases

- Besides using good passphrases, you should turn on two factor authentication (2FA) if the service supports it
- 2FA requires that you enter your userid, password and a random number that is either sent to you by a text message or generated on an app you have, like Authy or Google Authenticator. 2FA via text message is better than nothing, but isn’t as good as an app such as Authy

See if your credentials are in the wild

- You can search haveibeenpwned.com to see if your email address (and password) has been leaked
- They also have a service that will notify you if your email address appears in any future leaks

Encrypted Drives

- Often the drives of your computer or phone are left unencrypted & anyone can attach them to another computer and read them
  - Such as someone breaking into your house or a border guard
- Enabling drive encryption keeps your data secure as long as you have turned off your computer or phone

Encrypted Drives

- Drive encryption is on for iPhones
- You need to turn it on for most other phones and Windows, MacOS and Linux computers
- Reminder: only works when the computer has been turned off, not when it is asleep or when you have logged out

Beware of Being Phished

- No, not the band: phishing attacks
- Be careful of all emails that appear to come from banks, utilities, email provider, etc.
- If they ask you to login by clicking on a link in the email, don’t
- Check the link by hovering over it with your mouse pointer. The full link will appear at the bottom left of the browser window. If you see something like www.paypal.com.hack-you-for-the-lols.com, don’t click on it
- Always login in a separate window using the url you stored in your password manager

Signal

- A free secure text, voice and video communication application
- Works for Android, iPhone, Mac & Windows
- WTF! No Linux????
- Find it at signal.org
- Paid for by donations

Signal

- Signal messages and calls are end-to-end encrypted, which means that they can only be read or heard by your intended recipients.
- The Signal service does not have access to the contents of any messages or calls sent or received by Signal users.

Signal

- How do we know?
- Their client and server source code is available for anyone to look at and find insecurities
- Also, the app makes is very easy to verify the keys of the people who you talk with. If their key changes (get a new phone say), it warns you so you can reconfirm their key, perhaps in person.

Signal

- Let’s try it out!

Virtual Private Networks (VPNs)

- VPNs take the data you send out on the internet, encrypt it and send it to somewhere else to get on to the Internet
- Most useful when you don’t trust the local WiFi network, such as at cafes or events.
  - Also, when you don’t trust your ISP not to monitor you or inject adds into the insecure websites you visit
- Often used to provide secure access to a work network

Virtual Private Networks (VPNs)

- Why else? Getting around country copyright blocks. Want so see BBC shows for free? Get a VPN the exits in the United Kingdom.
- Traveling, but want to watch a US streaming service or play a US game, get a US VPN that exits in the US.
- To get home. You can run a VPN that exits at your home network.

Virtual Private Networks (VPNs)

- Usually you would use a monthly service. Your choices are free to expensive, but of course nothing is free so check out what data they gather.
- Check them out at ThatOnePrivacySite.net. Click on the VPN Section.

Virtual Private Networks (VPNs)

- Let’s try one out:
  - whatismyip.com
    - Local
    - With VPN

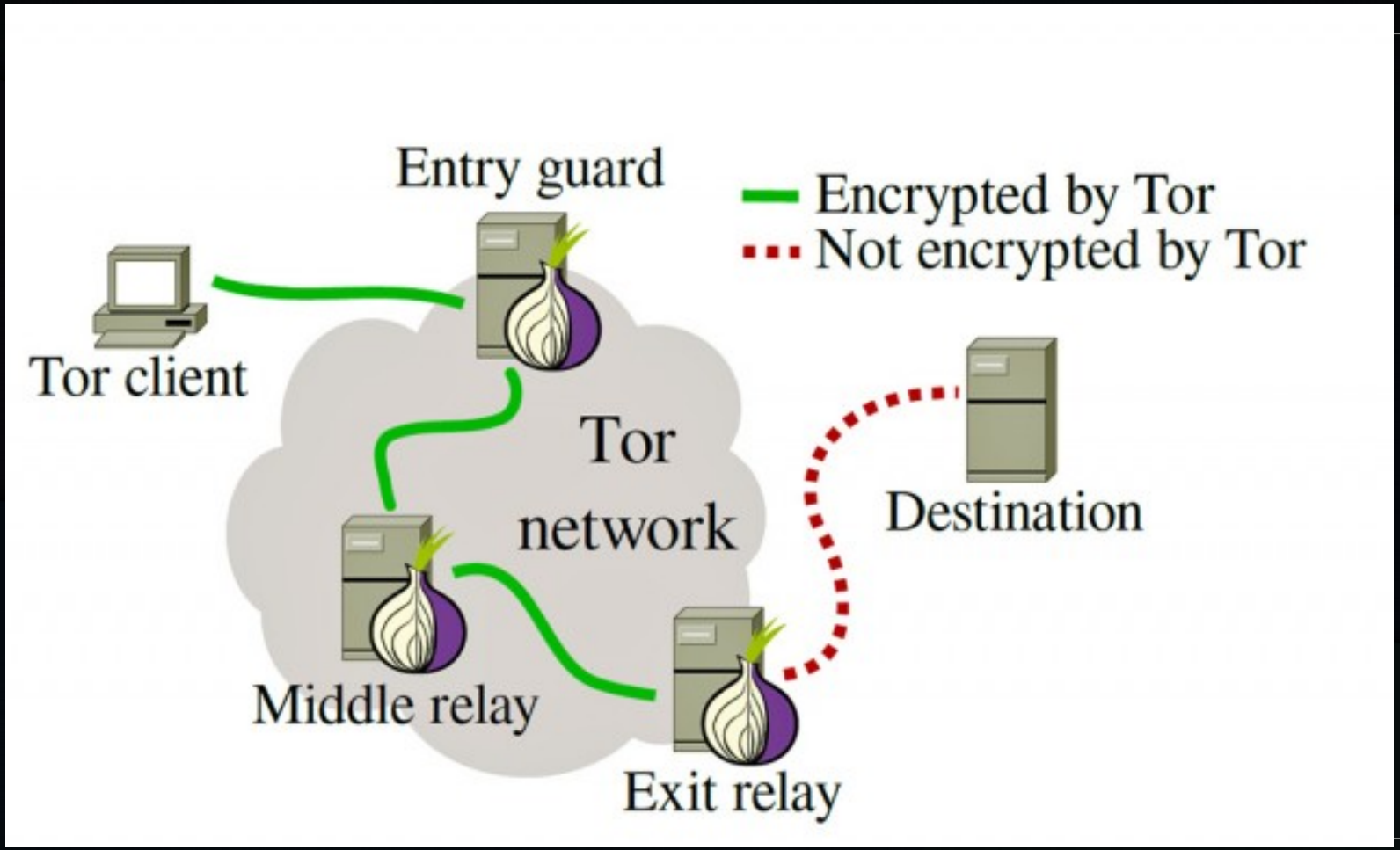
Tor

- Tor was setup by the US Navy so their spies could access US Navy sites in other countries without the local country being able to monitor or stop them
- Since spun out into the Tor Project
- Still gets a lot of funding from US government
- Last we knew the NSA hadn’t broken it

Tor: How it Works

- Tor Browser Bundle merges Firefox with the Onion router and is easy to setup
- Why reinvent the wheel. Let’s look at Steve Revilak’s Massachusetts Pirate Party Tor presentation:
  - https://masspirates.org/blog/wp-content/uploads/2015/01/tor-20150110.pdf

Tor: How it Works Review



Tor Limitations

- Tor is slower than using an ordinary web browser so don’t torrent over it.
- Web sites that rely heavily on Geolocation (e.g., Google) might get confused about your “unusual location”.
- It won’t save you if you login to a site with an account you use outside of Tor.

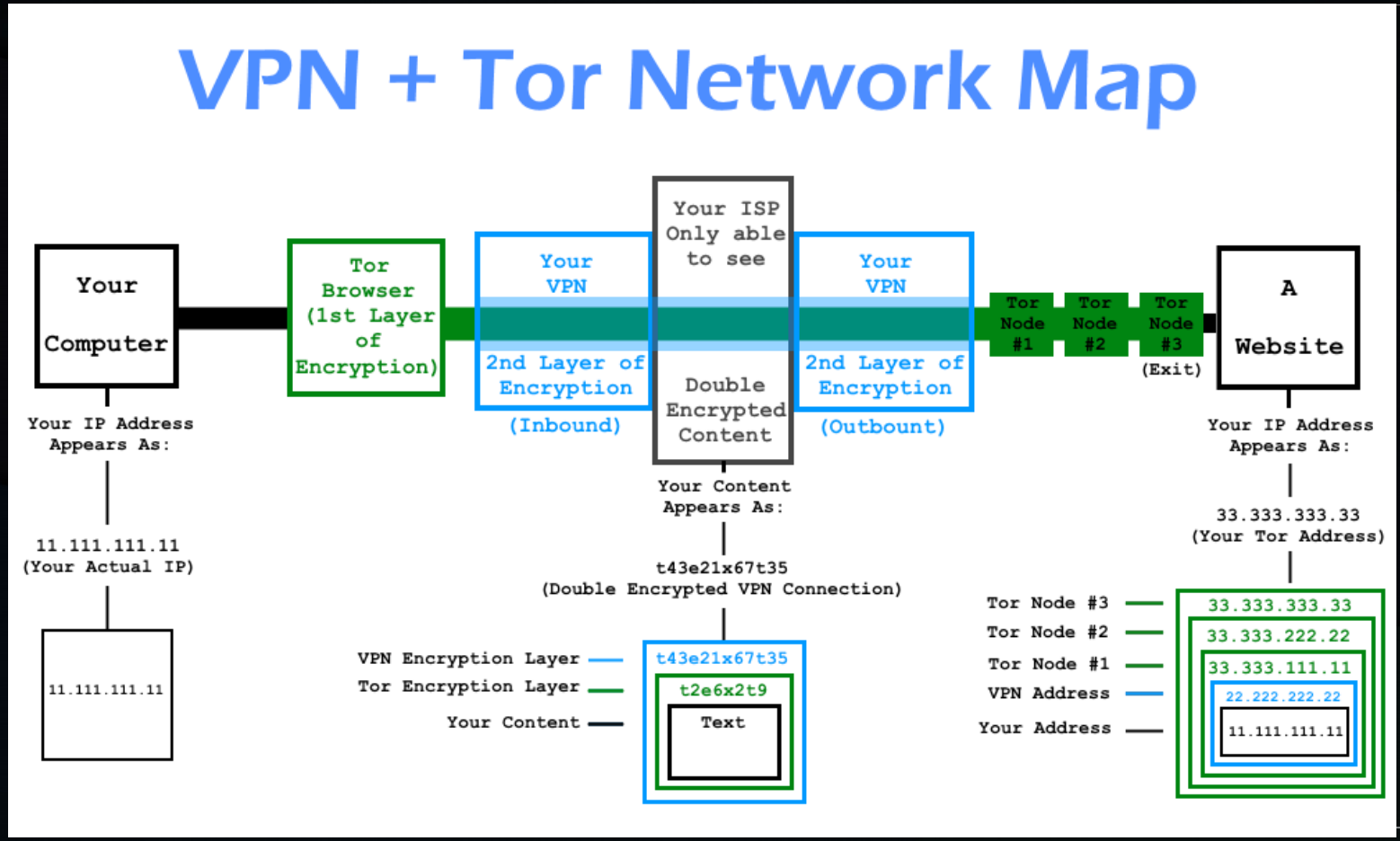
Tor Limitations

- You will need to change your browsing habits:
  - Don’t enable or install browser plugins
  - Use the HTTPS versions of websites (should do that everywhere, actually)
  - Don't open documents downloaded through Tor while online as it could phone home and id you
  - Try changing the size of your browser window each time you use Tor. Sites will fingerprint you from your browser window size among other browser characteristics.
  - Reminder: don’t login to sites with credentials you use outside Tor and don’t login with an email that you use outside of Tor.

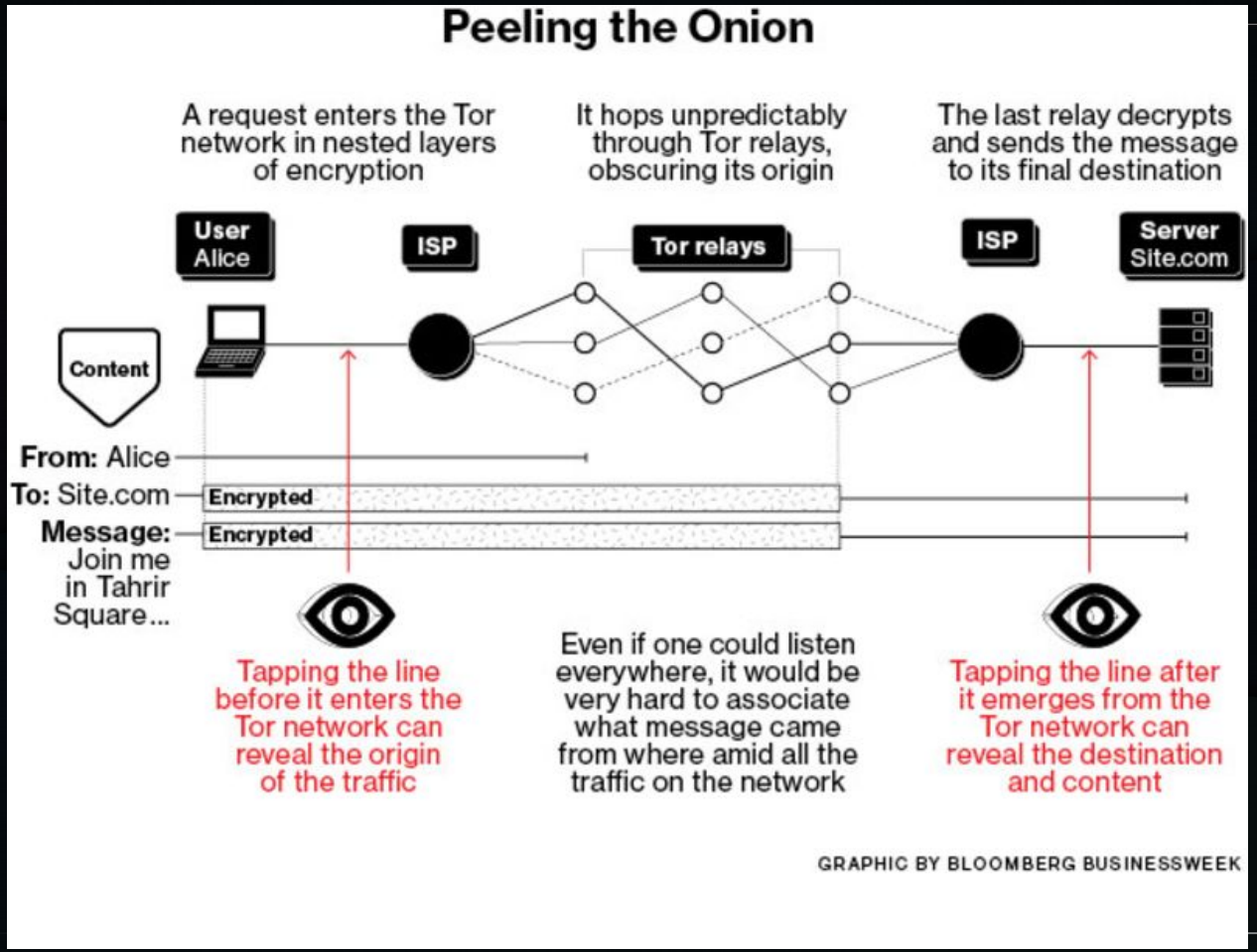
Tor

- Get it at TorProject.org
- Let’s try one out:
  - whatismyip.com or maxmind.com/en/geoip-demo
    - Local
    - With VPN
  - What if we change our circuit?

Tor & a VPN


VPN + Tor Network Map
Your Computer
Your IP Address Appears As:
11.111.111.11
(Your Actual IP)
11.111.111.11
Tor Browser (1st Layer of Encryption)
Your VPN
2nd Layer of Encryption
(Inbound)
Your ISP Only able to see
Double Encrypted Content
Your Content Appears As:
t43e21x67t35
(Double Encrypted VPN Connection)
VPN Encryption Layer
Tor Encryption Layer
Your Content
t43e21x67t35
t2e6x2t9
Text
Your VPN
2nd Layer of Encryption
(Outbount)
Tor Node #1
Tor Node #2
Tor Node #3
(Exit)
A Website
Your IP Address Appears As:
33.333.333.33
(Your Tor Address)
Tor Node #3
Tor Node #2
Tor Node #1
VPN Address
Your Address
33.333.333.33
33.333.222.22
33.333.111.11
22.222.222.22
11.111.111.11

Tor: Trying to Break It



Tor Hidden Services

- Tor Hidden Services provide an extra layer of protection by sending your traffic to a site from inside the Tor network
  - … and never on the Internet
- Tor hidden services have a special domain that only works in Tor.
- Often used by “Dark Sites”, but even Facebook has a Tor hidden service: facebookcorewwwi.onion

Tor Summary

- Using Tor is just as easy as using any other web browser.
- Tor protects you from surveillance by proxying web traffic through a network of Tor nodes.
- The network of Tor nodes conceals your location; encryption protects the content of your traffic.