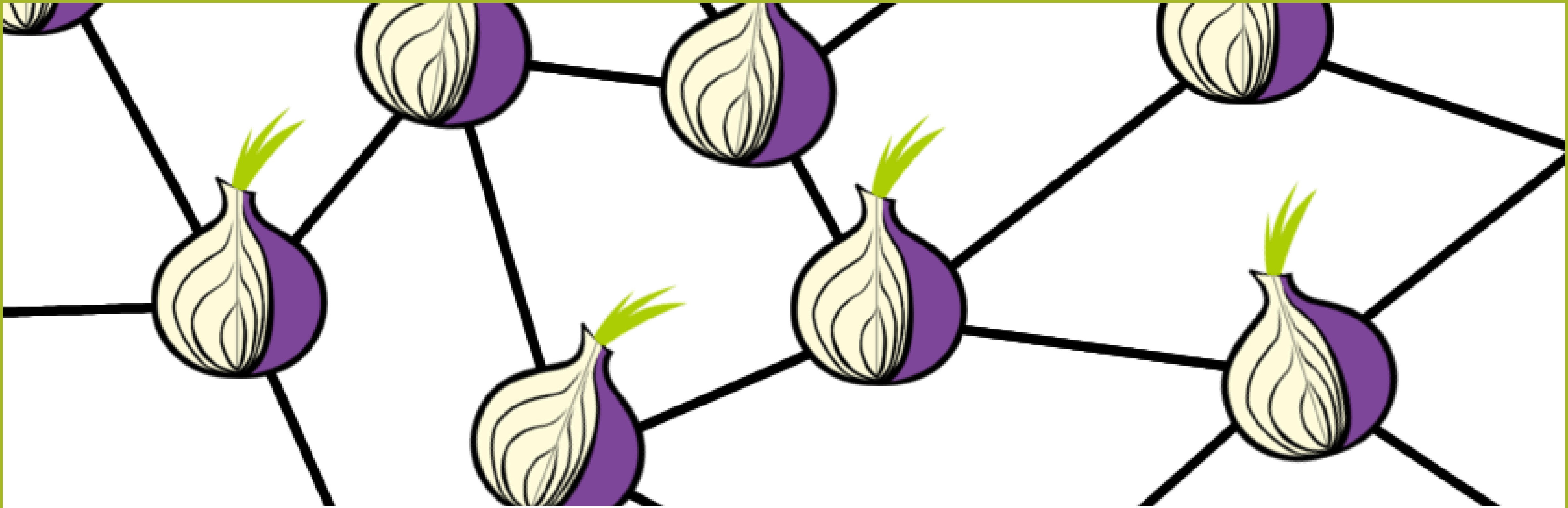


WHO’S CHOPPING ONIONS IN HERE??

An Intro to Tor & Privacy-Preserving Technology

muteki, Onion Chopper

- Azure/O365 SysAdmin with a focus on Security
- Computer Science Grad Student
  (aka glutton for punishment)
- Blue Team Village Organizer
- Jack of All Trades but nerdy for scripting, Python & cloud security / serverless microservices
- Lives for international travel, scuba diving, powerlifting, woodworking, jigsaw puzzles and baking

Cassandra Young aka muteki

Pronouns: she/her
Twitter: @muteki_rtw
LinkedIn: linkedin.com/in/cassandray
GitHub: github.com/muteki-apps (go here for slides & talk links!)

Intro & Agenda

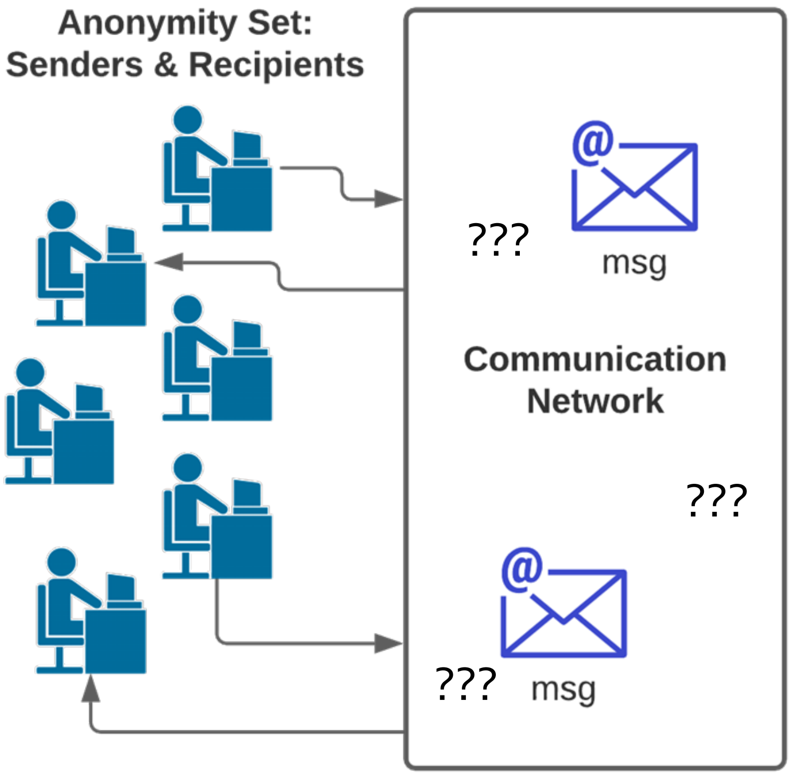
- What this talk is:
  - An introduction to concepts of privacy & anonymity
  - A brief overview of how Tor works to anonymize users
- What this talk is not:
  - A discussion about Audit & Compliance
  - An analysis of every cool privacy/anonymity tool out there (if only!)
- Sections:
  - Part One: Privacy & Anonymity
  - Part One: Q&A
  - Part Two: Tor & Onion Encryption
  - Part Two: Q&A

Part One: Privacy and Anonymity

- What is Privacy?
  - Dictionary: “the state or condition of **being free from being observed** or disturbed by other people”
  - In tech: the **protection & obfuscation of personal data** relating to the individual’s identity, past & present
- What is Anonymity?
  - A person/entity is anonymous when they **cannot be identified out of a set** of other users/entities

Part One: Privacy and Anonymity

- **Key Terms**
  - **Anonymity Set:** Any group of users/entities using a service
  - **Sender Anonymity:** The anonymity of one sender within the set of all senders
  - **Recipient Anonymity:** The anonymity of one recipient within the set of all recipients
  - **Unlinkability:** A state in which an attacker cannot reasonably determine (ie with statistical likelihood) if two items of interest are related.
  - **Global vs. Individual Anonymity:**
    - Global Anonymity: anonymity provided by the system to all its users together – stronger when all users in the system are statistically equally likely to relate to an item of interest.



Part One: Privacy, Anonymity.. & security?

- Privacy in the context InfoSec:
  - Protecting identity
  - A user's right to control access to their own personal data and how it is used, within contractual agreements
- Security:
  - Protecting data
  - Securing users' private data against **unintended disclosure** such as a data breach
- Regulatory acts such as HIPAA provide **standards for the lawful use and disclosure of personal data** (PII, PHI), and outline frameworks for securing it.
- Beyond that, many users choose to protect themselves via anonymity…

Why Anonymity?

- Online status indicators can be used to analyze patterns of behavior
  - InfoSec use case: patterns of behavior can be combined with social engineering for an attack
- Your data is being sold whether you see ads or not
  - 32% of paid apps shared the exact same sensitive data with 3rd parties as free versions
- Law enforcement investigation may involve comparison of unencrypted data sets that expose data of untargeted users
- IoT devices such as smart speakers may accidentally capture private conversations when misactivated
- With GPS location data, one study found a home-finding algorithm correctly identified plausible home locations of 85% of the drivers tracked
- & many, many more unnerving statistics…

A Privacy-Focused Systematic Analysis of Online Status Indicators: https://camillec.com/PETS_OSIs.pdf
The Price is (Not) Right: https://www.petsymposium.org/2020/files/papers/issue3/popets-2020-0050.pdf
Open, Privacy-Preserving Protocols for Lawful Surveillance: https://arxiv.org/pdf/1607.03659.pdf
When Speakers are All Ears: https://www.petsymposium.org/2020/files/papers/issue4/popets-2020-0070.pdf
A Survey of Computational Location Privacy: https://www.microsoft.com/en-us/research/wp-content/uploads/2016/12/computational-location-privacy-preprint.pdf

THIS IS FINE.

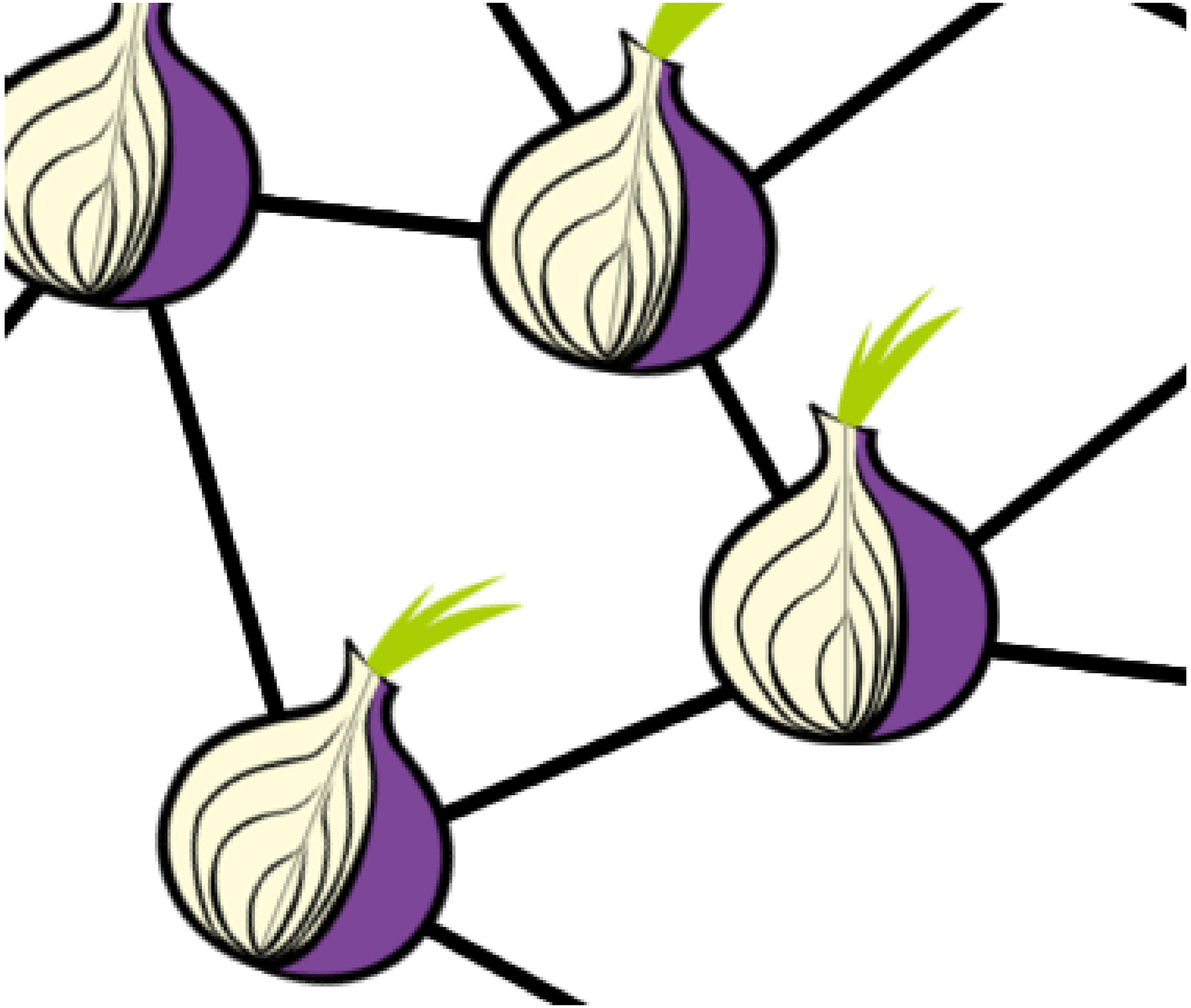
How does this relate to InfoSec?

- TL;DR: Anonymity is not just for criminals and hackers!
- The use of privacy-preserving technology should not be the sole basis for suspicion
  - Use of a VPN can render location-based alerts useless
  - Many VPNs and other tools piggyback off Tor
- Privacy + Security = better protection of users, and a smaller blast radius
  - Don't retain unnecessary user data
  - Identity and better protect PII

A Brief Survey of Anonymity Tech

- Commonly used tools:
  - Incognito mode, browser plugins, etc.
  - Secure messaging apps (ie Signal)
  - Pseudonyms, temporary email addresses, etc.
- The more involved side:
  - VPNs, proxy servers
- Down the rabbit hole:
  - Tor & Tor-based tools (next up!)
  - Tails OS

.... Questions so far?



PART TWO: THE TOR PROJECT

& Onion Encryption

Tor: **T**he **O**nion **R**outing Project

- 1990s: Onion Routing developed, primary by Navy / DARPA
- 2004: Tor paper comes out
- 2004: EFF (Electronic Frontier Foundation) starts funding Tor
- 2008: Tor Browser developed
- 2015: Tor Messenger released (later discontinued)

- Average users: 2.5 million
  - Spiked in late 2013 … maybe thanks to NSA / Edward Snowden?

Tor

- Designed for user anonymity
- More than just a browser
- Utilizes onion encryption and a multi-node routing setup to anonymize data
- Messages sent in fixed-size cells
- Travel from Entry Node, through Relay Node, and finally Exit Node
- Limited number of authoritative Directory Servers

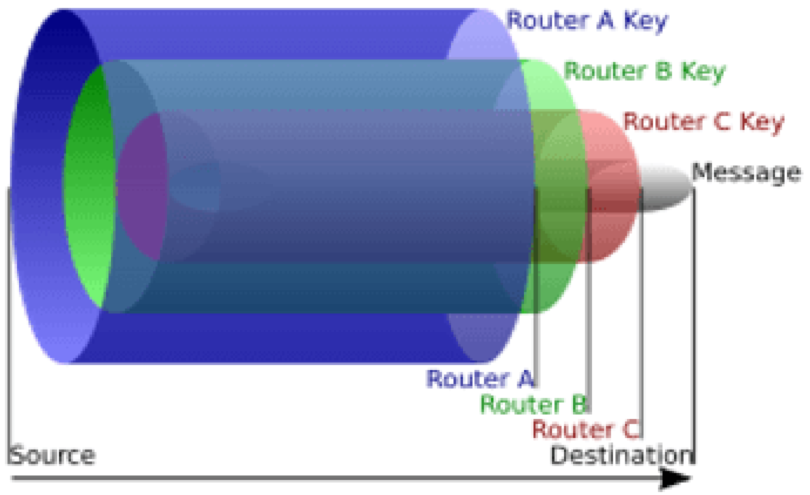
Goals & Assumptions of Tor

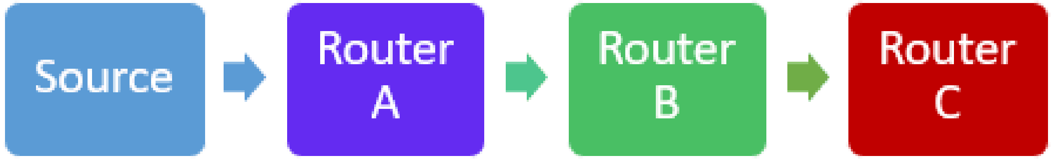
- Tor's Goals (after anonymity!):
  - Deployability, Usability, Flexibility, Simple Design
  - Why is this important? The anonymity set!
- What assumptions does Tor make about an attacker? Why is this important?
  - Threat Model: attacker sees some portion of network traffic
  - Defense against traffic analysis, but not traffic confirmation attacks

Packaged Messages: Onion Encryption

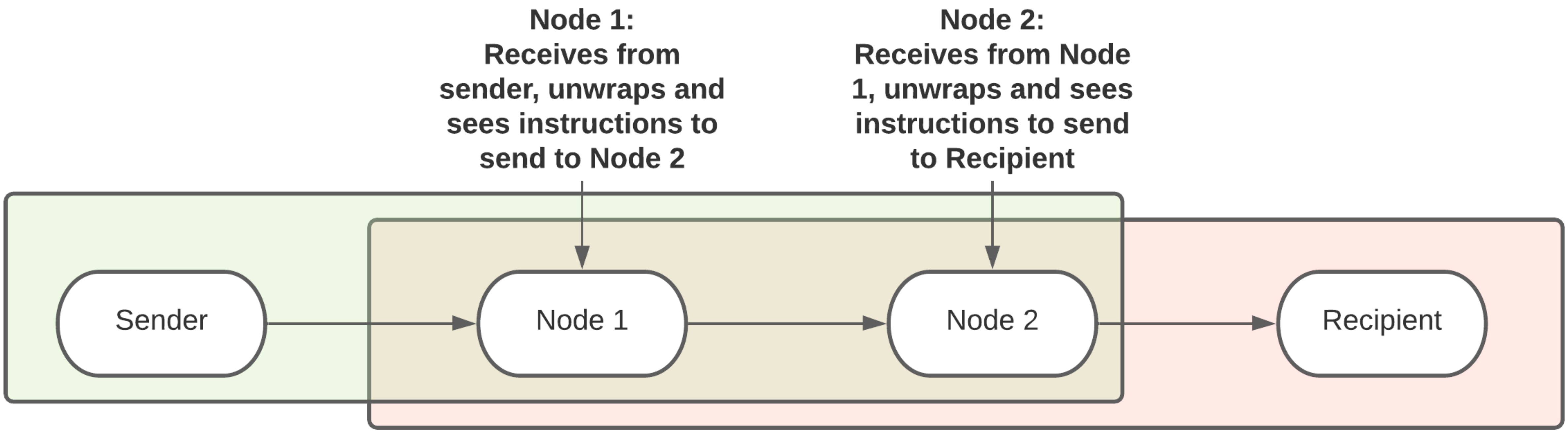
- It's the key idea of Onion Routing / Tor
- Encryption in layers, like an onion!
- Many different keys for the many hops on the route
- Keys are frequently rotated
- Session keys are symmetric, so messages sizes remain smaller
- Users create a route (a circuit) to reuse

Layers of the Onion



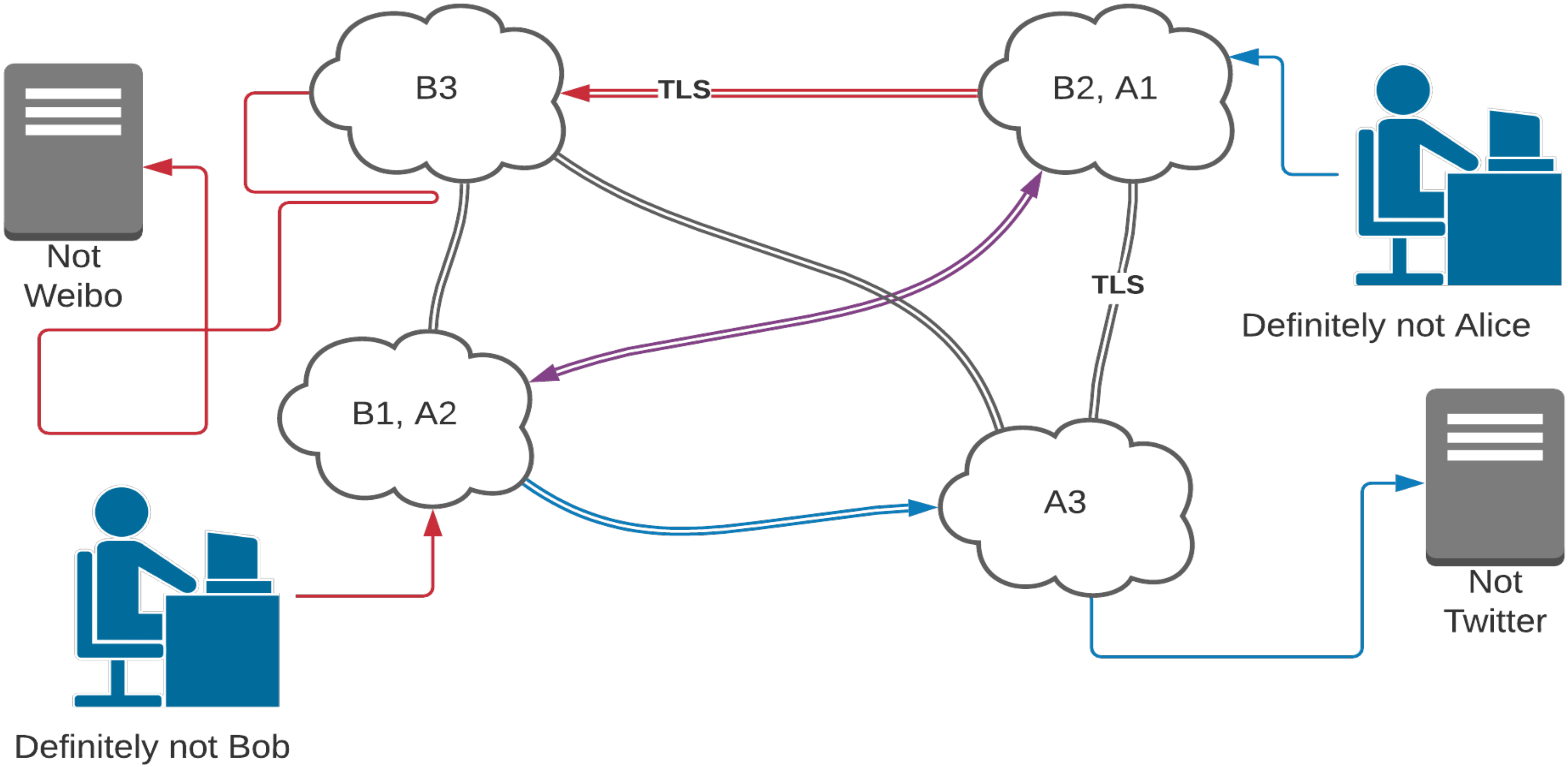


Onion Encryption in Action



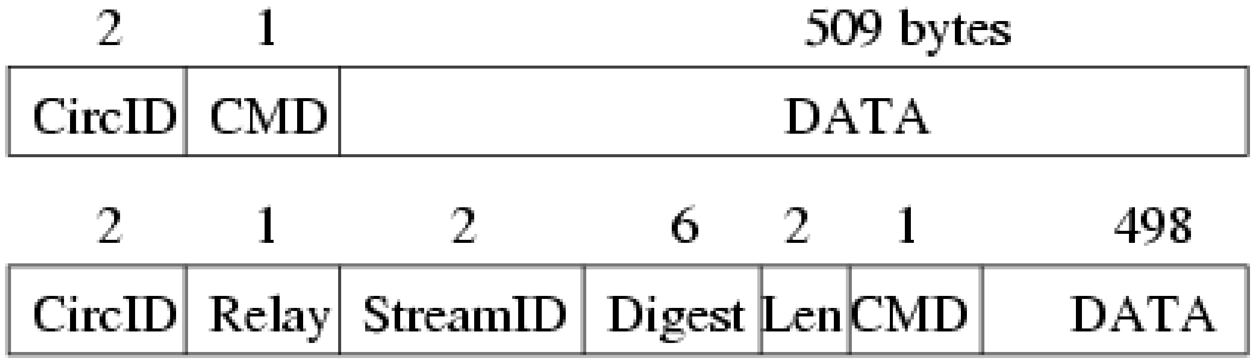
Node 1:
Receives from sender, unwraps and sees instructions to send to Node 2

Node 2:
Receives from Node 1, unwraps and sees instructions to send to Recipient


B3
TLS
B2, A1
Not
Weibo
TLS
Definitely not Alice
B1, A2
A3
Not
Twitter
Definitely not Bob

Tor Design

- Overlay Network
  - TLS connections between ORs (Onion Routers)
  - User's OP (Onion Proxy) manages connections, accepts TCP streams
- Data exchanged via Cells
  - Fixed size
  - CircID connects cell to circuit
  - Commands tell OR/OP what to do:
    - Control cells: interpreted by rec'ing node
    - Relay cells
      - carry end-to-end data
      - contain streamID



2	1	509 bytes
CircID	CMD	DATA

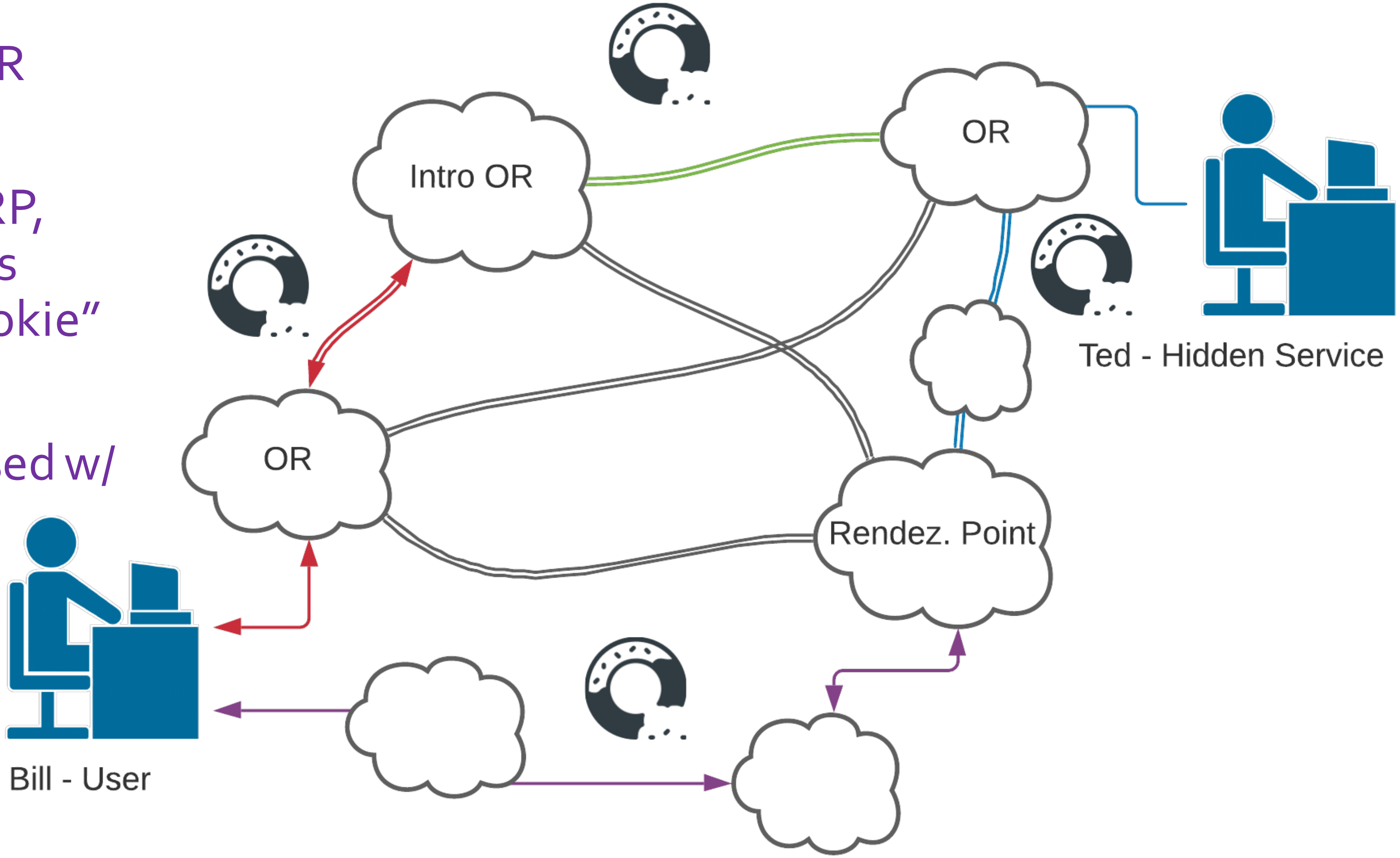
2	1	2	6	2	1	498
CircID	Relay	StreamID	Digest	Len	CMD	DATA

Tor Design

- What makes Tor's circuit-building process & usage more secure?
  - "Telescoping", OR doesn't know who originator is, just prev node
  - Fresh key, forward secrecy
  - Circuits can be shared by streams
  - Circuits rebuilt periodically
- Does Tor's design prevent messages from being manipulated/modified?
  - TLS-enforced integrity checks on streams prevent *outsider* manipulation
  - End-to-end encryption of hashes across circuit
- How does Tor handle rate limiting & congestion?
  - Enforces average byte rates, allows for bursts – this mitigates user bandwidth issues
  - Throttling at circuit and stream levels – does this address D/DoS attacks?

Rendezvous Points & Hidden Services

- Only advertised Intro OR knows hidden service
- Circuit built w/ central RP, connection id'd by user's chosen "rendezvous cookie" (or donut, per diagram)
- Hidden Service advertised w/ .onion TLD, public key



Attacks and Defenses

- Are any Statistical (Passive) Attacks addressed by Tor?
  - Traffic confirmation attacks are outside the design goals ☹
  - Sybil Attacks: An actor can overwhelm network with large number of malicious nodes – limited protection against this!
- What are some notable Active Attacks?
  - DDoS: continue to be an issue that is actively worked on!
  - Key compromise: mitigated by key rotation, session keys
  - Distribute hostile code: mitigated by signing releases, publishing "known good"
  - …and many more
- Does Tor prevent attacks against Hidden Services / Rendezvous Points?
  - Many attacks are essentially [D]DoS attacks
  - Restricting request volume, rotating intro points, & intro point testing can mitigate

Bonus: 2014 Sybil/Traffic Attack!

- **Sybil + Traffic Confirmation Attack on Tor**: February-July 2014
- **Sybil** Attack: Malicious relays joined Tor at end of January
- **Traffic Confirmation**: Headers modified to exchange signals between malicious nodes

"the relay on one end injects a signal into the Tor protocol headers, and then the relay on the other end reads the signal. These attacking relays were stable enough to get the HSDir ("suitable for hidden service directory") and Guard ("suitable for being an entry guard") consensus flags. Then they injected the signal whenever they were used as a hidden service directory, and looked for an injected signal whenever they were used as an entry guard."

- End Goal: De-anonymize users who operated or used hidden services.
- Were they successful? It's unclear, but Tor "found no evidence that the attackers operated any exit relays". **What are the implications of that finding?**
- OF NOTE: "preventing traffic confirmation in general remains an open research problem"
- More info: https://blog.torproject.org/tor-security-advisory-relay-early-traffic-confirmation-attack

ONIONIZE