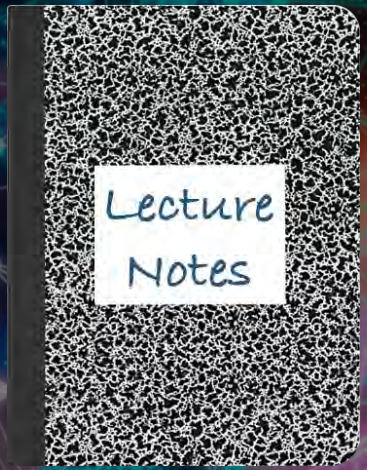
CS 419: Computer Security



Week 13: Hiding Communication

Part 2: Anonymous Connectivity

Paul Krzyzanowski

Anonymous & Hidden Communication

Authentication is a big theme in computer security

But anonymity and secrecy are also important

Anonymous communication

Communicate while preserving privacy

Often considered bad: “only criminals need to hide

- Spammers & scammers
- Illegal goods: drugs, guns
- Hit men
- Stolen identities
- Counterfeit $
- Stolen credit cards
- Hacking
- Money laundering via cryptocurrency
- Fraud

Anonymous communication

Communicate while preserving privacy

But there are legitimate uses

- **Avoid consequences (social, political, legal)**
  - Accessing content in oppressive governments
  - Political dissidents, whistleblowers, crime reporting
- **Avoid geolocation-based services**
- **Hide corporate activity (who's talking to whom)**
- **Perform private investigations**
- **Hide personal info**
  - Searching for information about diseases, loans, credit problems

Some services retain information about you

- **Accounts, configuration settings**
  - Identity
  - Purchase data
- **Cloud storage**
  - Files, email, photos, blogs, web sites
  - Encryption so the server has no access not always possible
- **Sites may know your interests, browsing history, messages**
  - Web sites visited (via tracking cookies)
  - Important for data mining & targeted advertising
  - E.g., Facebook, Google

Cookies on the web

- **Local *name=value* data stored at the browser & sent to a server**
  - Avoids having to log in to a service repeatedly
  - Keeps track of session, shopping cart, preferences
- **Associated with the site (same-origin policy)**
  - Facebook cookies don't get sent to Google … and vice versa
- **Tracking cookies (third-party cookies)**
  - Websites can embed resources from another site (e.g., bugme.com)
    - Via an ad in an iFrame or a 1x1 pixel image – https://bugme.com/pixel.png?pageid=1127
  - bugme.com's cookies will be sent to bugme.com
    - HTTP message contains a *Referer* header, which identifies the encompassing page
  - Lots of different sites may use bugme.com's services
    - bugme.com can now build a list of which sites the visitor has visited
- **Most browsers have policies to block third-party cookies**

Private Browsing

- **Browsers offer "private" browsing modes**
  - Apple *Private Browsing*, Mozilla *Private Browsing*, Google Chrome *Incognito Mode*, Microsoft *InPrivate* browsing
- **What do these modes do?**
  - Do not send stored cookies
  - Do not allow servers to set cookies
  - Do not use or save auto-fill information
  - Do not save info on downloaded content
  - At the end of a session
    - Discard cached pages
    - Discard browsing & search history

Does not protect the user from viruses, phishing, or security attacks

Is private browsing private?

- **It doesn't leave too many breadcrumbs on your device**
- **It limits the ability of an attacker to use cookies**
- **But**
  - Your system may be logging outbound IP addresses
  - Web servers get your IP address ⇒ *they can also correlate with past traffic*
  - Proxies know what you did … so do firewalls & routers
  - Your ISP knows who you are and what domains you accessed
  - DNS servers know what addresses you're looking up
    - Some store and use this data

Answer: *not really*

Improvements to Chrome's Incognito Mode

Detecting Incognito mode allows websites to block users if they cannot be tracked

- **Services had a simple trick to determine whether a user is using Incognito Mode**
  - Use FileSystem API – Chrome-specific method that gives a website a sandboxed file system for its own use
  - The API is completely disabled in Incognito mode
- **Google's fix (early 2019)**
  - Create a virtual file system in RAM
  - Erased when the user leaves Incognito Mode

Other browsers used similar detection mechanisms

- **Firefox, IE 10 & Edge (older)**
  - `IndexedDB` is not available
  - Attempts to access it causes it to throw an `InvalidStateError`
- **Safari**
  - Disables its `localStorage` API in Private Browsing
  - An attempt to call the `setItem` method throws an exception
- **Other techniques exist, too**
  - Services can send code to check for private browsing modes and block users if they cannot be tracked

Detection mechanisms get patched … no reliable way to detect incognito mode!

Just like detecting VMs & sandboxes, attackers will try to find workarounds

Cell tower, Wi-Fi & Bluetooth tracking

- **Mobile devices scan for Bluetooth devices & Wi-Fi access points**
  - They broadcast their MAC address
  - ISPs and hotspots can track users by their MAC addresses
- **Apple's fix**
  - Provide a different MAC address each time the device connects to each new network

Opinion | THE PRIVACY PROJECT

In Stores, Secret Surveillance Tracks Your Every Move

As you shop, "beacons" are watching you, using hidden technology in your phone.

By Michael Kwet
Graphics by Tala Schlossberg
Illustrations by Max Guther

https://www.nytimes.com/interactive/2019/06/14/opinion/bluetooth-wireless-tracking-privacy.html

Encrypted sessions?

Great … eavesdroppers can't see the plaintext

But they can see where it's coming from and where it's going

ISPs and companies know your IP address & can track you

If you use a commercial VPN service (e.g., ExpressVPN), the ISP and receiver won't know your IP address, but the VPN provider will

Classic Covert Communication Techniques

Shortwave Numbers Stations

- Certain shortwave radio stations read off lists of random numbers
- These are messages encrypted with a one-time pad
- Signals have been traced to the U.S., Russia, Cuba, Israel, North Korea – but no government acknowledged them
- Benefits:
  - The receiver can receive them anywhere and leave no trace of accessing the data
  - Signals are hard to jam and don't rely on Internet infrastructure

Dead Drops

- Leave a message or item at a secret location for someone else to retrieve without direct contact
- Digital equivalent: post a message in a public forum (e.g., Instagram, eBay, discord, …)

See: https://johnwlittle.com/covert-contact-118-shortwave-numbers-stations/

Covert Channels

Any attack that allows the attacker to transfer information when processes should not be allowed to communicate

Can use

- **Side-channel attacks** – getting information indirectly: timing, power changes, electromagnetic leaks, acoustics
- **Content Steganography** – hides secret information within innocent content
- **Network Steganography** – hide secret information within the network protocol

Examples

- **Measure CPU Load**: Process 1: alter system load; Process 2: monitor changes in load
- **Measure Packet Timing**: Modify delays between packets
- **Choose TCP fields**: Set specific initial sequence numbers
- **DNS queries/responses**:
  - Do DNS queries on subdomains with specific names; the DNS server decodes them as content
  - Send data via TXT records – often used for malware delivery from a C&C server

Surface Web
Deep Web
Dark Web

The different types of web

- **Surface Web**
  - Web content that can be indexed by mainstream search engines
  - Search engines use web crawlers
    - Go through a list of addresses from past crawls
    - Access pages provided as sitemaps by website owners
    - Traverse links on pages being crawled to find new content
- **Deep Web**
  - Web content that a search engine cannot find
  - Unindexed content, often from dynamically-generated pages
  - E.g., query results from libraries, govt and corporate databases

Dark Web

Part of the Deep Web that has been intentionally hidden

- **Not accessible through standard browsers**
  - Need special software, such as a Tor browser
- **Servers do not register names with DNS**
  - Sometimes use a .onion pseudo-top-level domain
- **Still uses**
  - HTML web pages
  - HTTP & FTP for moving content

Dark Web

Legitimate & illicit services

- **Drugs, stolen identities, counterfeit currency, etc.**
- **Blackbook (similar to Facebook), recipes, books**
- **Anonymous access to news access:**
  - ProPublica: https://www.propub3r6espa33w.onion/
  - NY Times: https://www.nytimes3xbfgragh.onion/
  - BBC News: https://www.bbcnewsd73hkzno2ini43t4gblxvycyac5aw4gnv7t2rccijh7745uqd.onion
- **DuckDuckGo:** http://3g2upl4pq6kufc4m.onion/
- **SecureDrop – leak info anonymously:** https://secrdrop5wyphb5x.onion/
- **CIA:** ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion

.onion domains

- **What's a domain like `ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion`?**
- **Each service generates a public/private keypair**
- **The public key is hashed: base32 + checksum + version code**
- **This encoded value becomes the domain name**
- **Prefixes like "ciadotgov" or "propub" are just the result of the hash:**
  - These are called vanity addresses
  - The service has to repeatedly generate keys, hash them, and see if the result contains the string they want
  - It typically takes around 3.5B attempts to get 7 chosen characters
  - It's just trial and error – like a Bitcoin proof-of-work

BBC

BBC News launches 'dark web' Tor mirror

23 October 2019

The BBC has made its international news website available via the Tor network, in a bid to thwart censorship attempts.

The Tor browser is privacy-focused software used to access the dark web.

The browser can obscure who is using it and what data is being accessed, which can help people avoid government surveillance and censorship.

Countries including China, Iran and Vietnam are among those who have tried to block access to the BBC News website or programmes.

- BBC News in Ukrainian: https://www.bbcweb3hytmzhn5d532owbu6oqadra5z3ar726vq5kgwwn6aucdccrad.onion/ukrainian
- BBC News in Russian: https://www.bbcweb3hytmzhn5d532owbu6oqadra5z3ar726vq5kgwwn6aucdccrad.onion/russian
- BBC News internationally: https://www.bbcweb3hytmzhn5d532owbu6oqadra5z3ar726vq5kgwwn6aucdccrad.onion

Technology explained: What is the dark web?

Instead of visiting bbc.co.uk/news or bbc.com/news, users of the Tor browser can visit the new site here: https://www.bbcnewsd73hkzno2ini43t4gblxvycyac5aw4gnv7t2rccijh7745uqd.onion/

https://www.bbc.com/news/technology-50150981

Tor & Anonymous Connectivity

Tor = The Onion Router

- **Tor Browser = preconfigured web browser that uses Tor**
  - Provides anonymous browsing
- **Hosted on a collection of relays around the world**
  - Run by non-profits, universities, individuals
  - Currently a bit over 9,000
- **~4.7 million directly-connecting users**
  - Exact data unknown – it's anonymous
  - Routing ~300 Gb per second

Statistics at https://metrics.torproject.org

History

- **Onion routing developed in the 1995 at the U.S. Naval Research Laboratory to protect U.S. intelligence communications**
  - Goal: develop a way of communicating over the Internet without revealing who is talking to whom … even if someone is monitoring their network
- **Patented by the U.S. Navy in 1998**
  - Naval Research Laboratory released to code for Tor under a free license
- **The Tor Project**
  - Founded in 2006 as a non-profit organization with support of the EFF

What is anonymity?

- **Unobservability**
  - Inability of an observer to link participants to actions
  - ISO definition:
  - *being able to "use a resource or service without others, especially third parties, being able to observe that the resource or service is being used."*

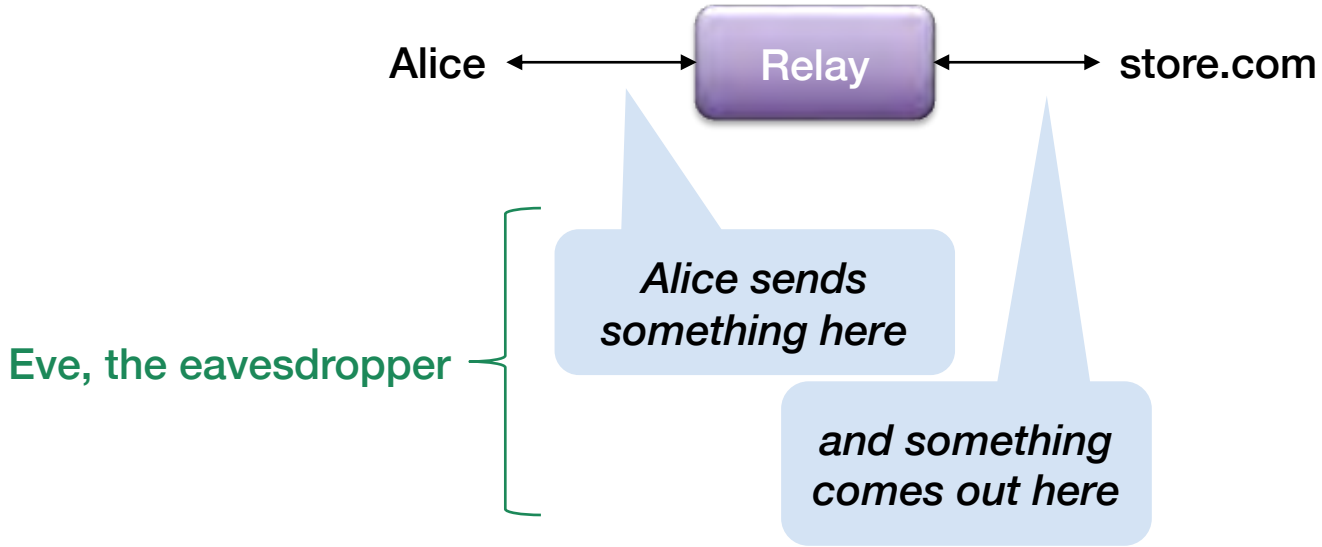
- **Unlinkability**
  - Inability to associate a multiple actions as being related
  - ISO definition: *"a user may make multiple uses of resources or services without others being able to link these uses together."*

Relay

We can use encrypted connections (TLS) to encrypt network traffic
…but the communication path isn't a secret

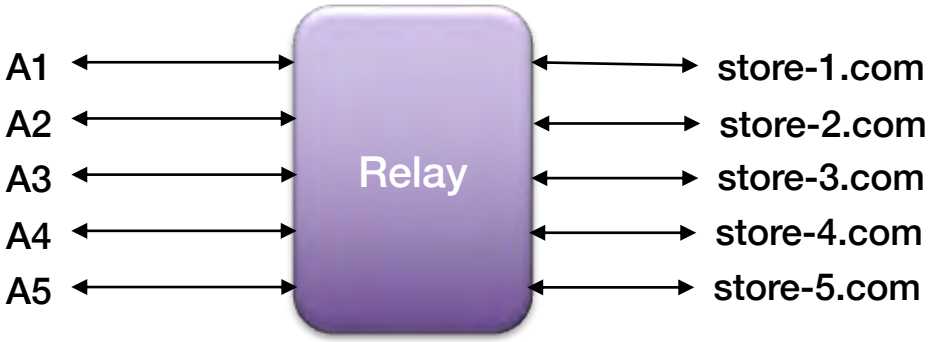
This is what commercial VPNs provide.

Relay



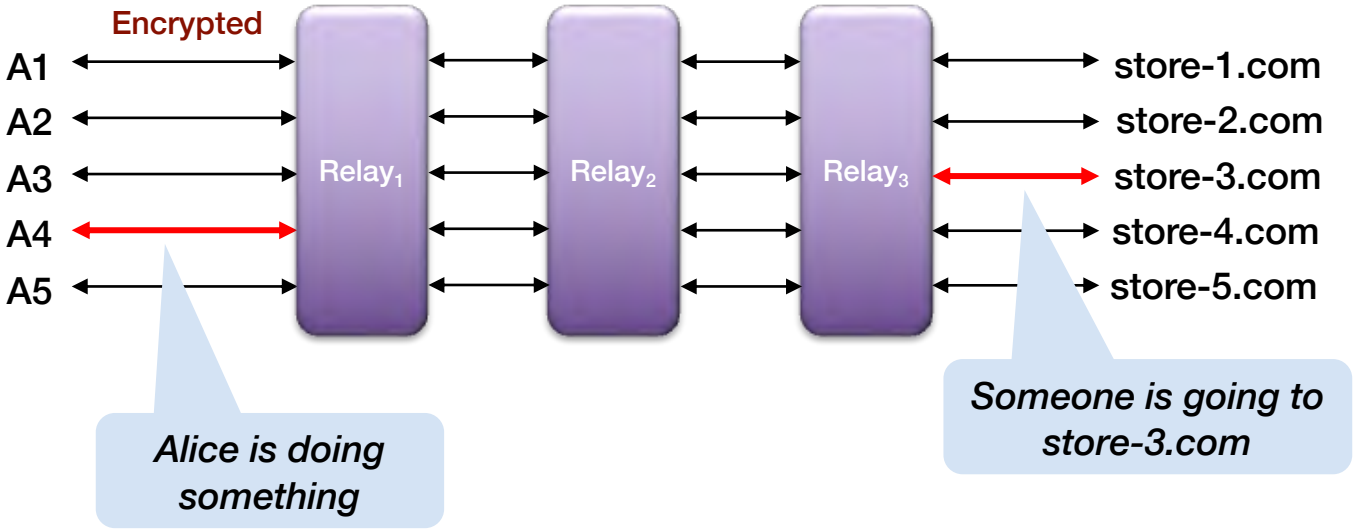
Correlation is really easy

Shared relay with multiple parties



What if someone eavesdrops on the relay?
They can still see who is talking to whom:
correlation is more difficult but still possible possible

Multiple relays



Tor uses (by default) three layers of relays.

This makes it more difficult to know where to look.

Correlation – by message time & size – is still possible

… but difficult since the relays are scattered across ISPs and across the world

Correlation Attack

If an eavesdropper watches entry & exit of data

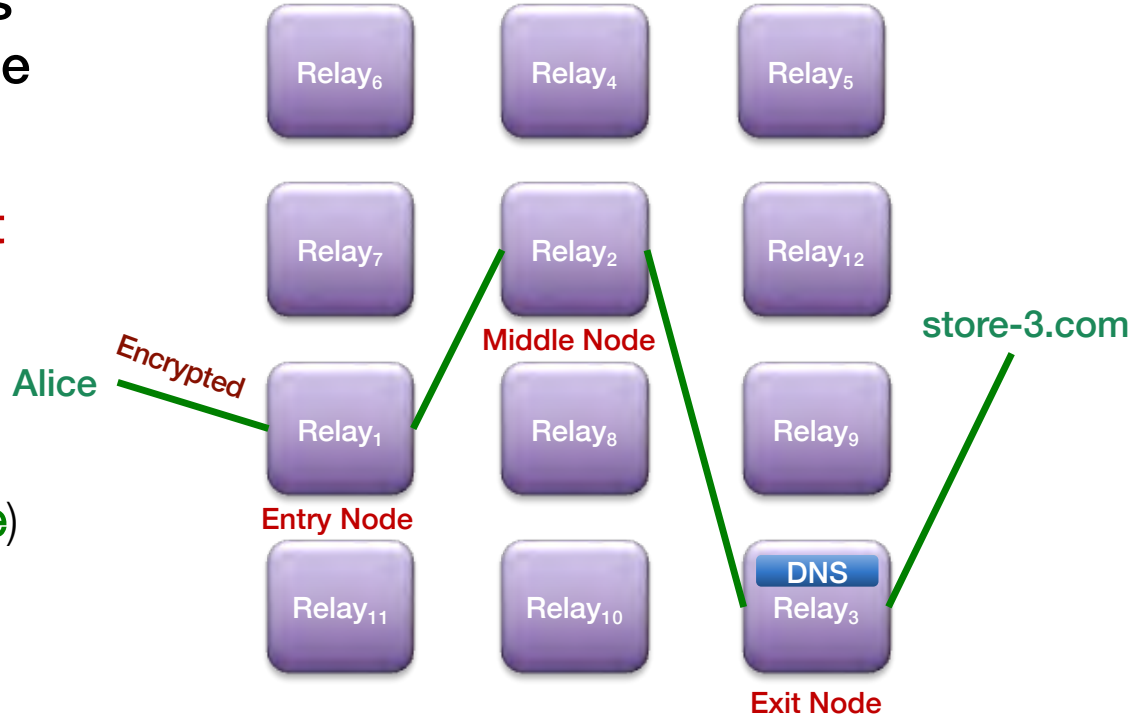
- She can correlate timing & size of data at the 1st relay with outputs of the last relays
- If **Alice** sends a 2 KB request to **Relay$_1$** at 19:12:15
  and **Relay$_3$** sends a 2 KB request to **store-3.com** at 19:12:16
  and **store-3.com** sends a 150 KB response to **Relay$_3$** at 19:12:17
  and **Alice** receives a 150 KB response at 19:12:18
  … *we're pretty sure Alice is talking to store-3.com*

Making Correlation Attacks More Difficult

- **You can make a correlation attack difficult**
  - Pad or fragment messages to be the same size
  - Queue up multiple messages, shuffle them, and transmit them at once
- **This works in theory but is a pain in practice**
  - Extra latency, traffic
  - You still need *A LOT* of users to ensure anonymity
- **Relays should be hosted by third parties to get many different groups as input**
  - E.g., a relay within `fbi.gov` implies that input to it comes from `fbi.gov`

Circuits

- Alice selects a list of relays through which her message will flow
- This path is called a circuit
- No node knows if the previous node is the originator or relay
  - Only the final node (exit node) knows it is the last node

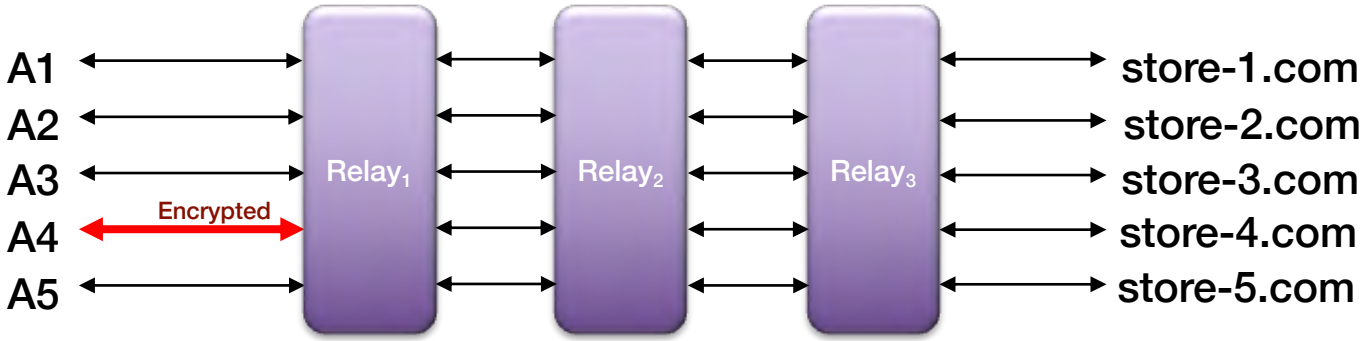


Relay Keys and the Tor Consensus Document

- **Every relay has a public-private key pair**
  - Remember: .onion domain names were created by hashing the public key
- **The *Tor Consensus Document* is signed & updated hourly**
  - Describes the entire Tor network
  - All valid relays
  - Their public keys
  - Their IP addresses, ports, bandwidth, etc.
  - Which authorities agree on each relay's status
    - Trusted **directory authorities** vote on the network

A user bootstraps by downloading this directory information

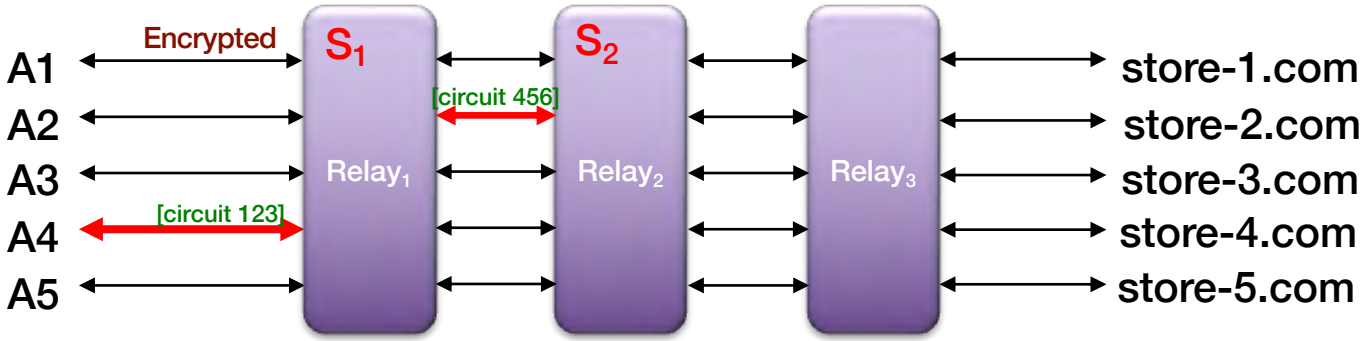
Setting up a circuit – first relay



Alice connects to Relay1

- Sets up a TLS link to $Relay_1$
- Does a one-way authenticated key exchange with $Relay_1$ – agree on a symmetric key, S_1
- Alice and the $Relay_1$ agree on a random circuit ID (e.g., 123)

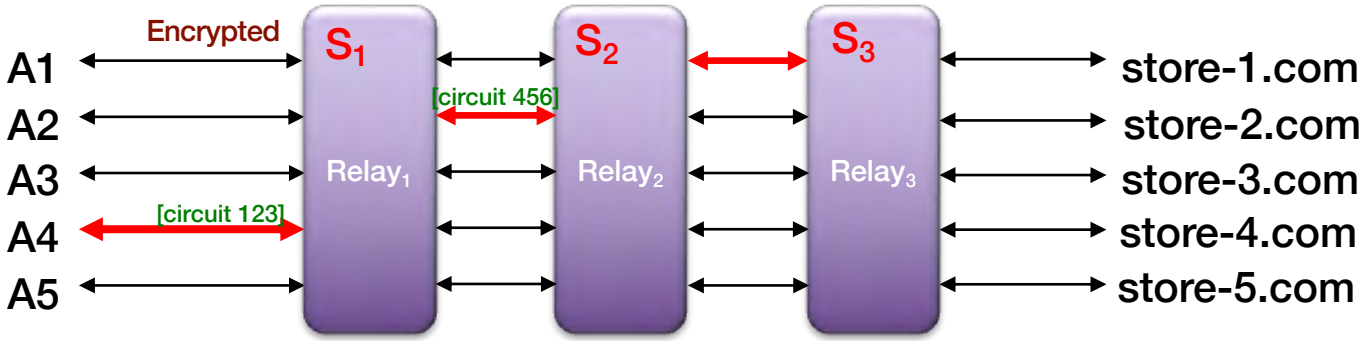
Setting up a circuit – extend to second relay



Alice extends the relay to $Relay_2$

- Alice sends a message to $Relay_1$:
  1st part = "on circuit 123, send *Relay Extend* to $Relay_2$" – the message is encrypted with S_1
- $Relay_1$ establishes a TLS link to $Relay_2$ (if it didn't have one)
- 2nd part of the message from Alice: **initial handshake with $Relay_2$, encrypted with $Relay_2$'s public key**
- $Relay_2$ picks a random circuit ID for identifying this data stream to $Relay_2$, e.g., 456
  - Circuit 123 on $Relay_1$ connects to Circuit 456 on $Relay_2$
- Does a one-way authenticated key exchange with **$Relay_2$** – agree on a symmetric key, **S_2**
  - All traffic flows through **$Relay_1$** and is encrypted with **S_1**

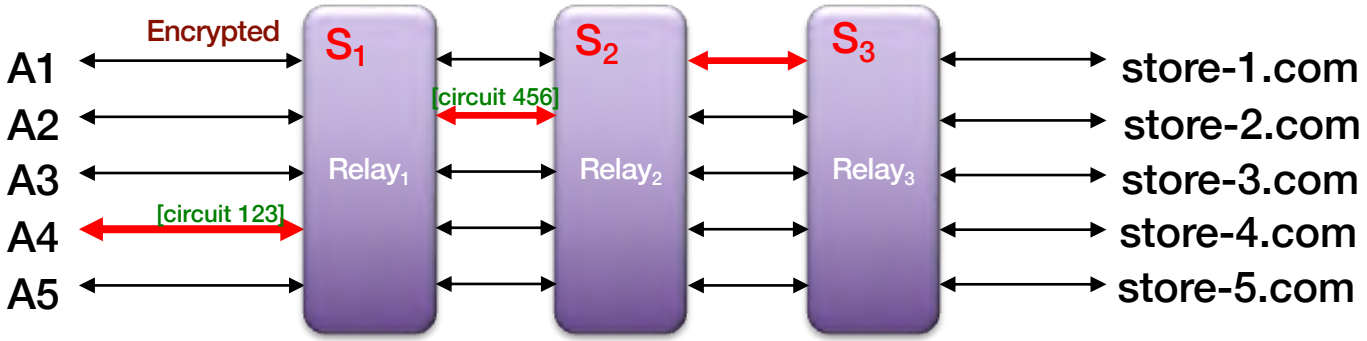
Setting up a circuit – extend to third relay



Alice extends the relay to $Relay_3$

- Same process – Alice sends a ***Relay Extend*** message to $Relay_2$
- Alice's messages to $Relay_2$ are encrypted with S_2 and then with S_1: $E_{S1}(E_{S2}(M))$
- $Relay_1$ decrypts the message to identify its circuit (123)
- Routes message to $Relay_2$ on circuit 456
  - Circuit 123 is connected to circuit 456

Sending a message via the circuit

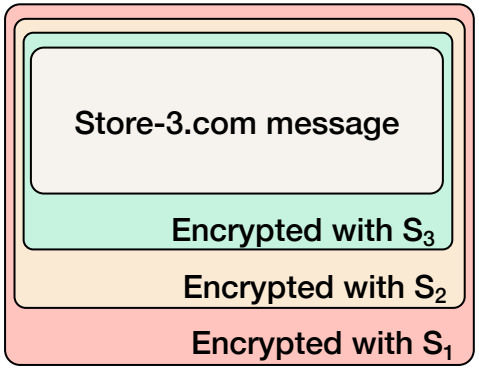


Alice sends a message to store-3.com

Each relay strips off a layer of encryption

At the end:

- Directive to S_3 to open a TCP connection to store-3.com
- Send messages
- Get responses



Not a VPN – more like a TLS session

- **Neither IP nor TCP packets are transmitted in the message**
  - It does not encapsulate IP packets but rather sends data streams back and forth.
  - It would be too easy to identify the type of system by looking at TCP formats and responses
- **Just take contents of TCP streams and relay the data**
- **End-to-end TLS between source and destination works fine**
  - TLS sits on top of TCP … it's just data going back and forth

Finding nodes

- **Ideally, everyone would use some of the same relays**
  - Otherwise, traffic would be distinguishable
- **Multiple trusted parties supply node lists**
  - Tor project provides a relay search using aggregated data
  - Scripts check health & bandwidth of relays
  - Trusted relays = entry guards
    - Recommended for use as entry nodes

Is Tor anonymous?

- **Not really**
- **You may be able to do a correlation attack**
  - ISPs know who's talking to whom
  - May need to access logs from multiple ISPs
  - Can be *really difficult* if nodes have a lot of traffic (and it's similarly dense)
- **Compromised exit node**
  - Exit node decrypts the final layer and contacts the service
  - Tor encourages content to service to be encrypted but that's not always the case

Some problems

Searching is difficult

- Search engines, such as **Grams**, often give bad results
- **Hidden Wiki** (http://thehiddenwiki.org) – Directory of Tor .onion sites
  - Often full of bad links

Users are the weakest link

- Sites constantly changing addresses to avoid DDoS attacks
- Lots of scammers
- Honeypots set up by law enforcement
- Many ISPs block access to Tor

Sites can get found & shut down

- Silk Road 2.0: shut down by the FBI & Europol on Nov 6 2014
- Silk Road 3.0: went offline due to loss of funds in 2017
- AlphaBay (largest source of contraband): shut down in July 2017
- Hansa Market (competitor to AlphaBay): also shut down in 2017 by Dutch police
- And many more … it just takes more effort to locate the services

ars technica

Tor is under threat from Russian censorship and Sybil attacks

30 April 2022

Tor Project leaders disconnect rogue nodes and call on volunteers to bypass censorship.

The Tor anonymity service and anticensorship tool has come under fire from two threats in recent weeks: The Russian government has blocked most Tor nodes in that country, and hundreds of malicious servers have been relaying traffic.

Russia's Federal Service for Supervision of Communications, Information Technology, and Mass Media, known as Roskomnadzor, began blocking Tor in the country on Tuesday. The move left Tor users in Russia—said by Tor Project leaders to number about 300,000, or about or 15 percent of Tor users—scrambling to find ways to view sites already blocked and to shield their browsing habits from government investigators.
…
Tor managers have responded by creating a mirror site that is still reachable in Russia. The managers are also calling on volunteers to create Tor bridges, which are private nodes that allow people to circumvent censorship. The bridges use a transport system known as obfs4, which disguises traffic so it doesn't appear related to Tor. As of last month, there were about 900 such bridges.

https://arstechnica.com/information-technology/2021/12/tor-is-under-threat-from-russian-censorship-and-sybil-attacks/

ars technica

Tor is under threat from Russian censorship and Sybil attacks

30 April 2022

Sybil Attack

Meanwhile, on Tuesday, security news site The Record reported on findings from a security researcher and Tor node operator that a single, anonymous entity had been running huge numbers of malicious Tor relays. At their peak, the relays reached 900. That can be as much as 10 percent of all nodes.

Tor anonymity works by routing traffic through three separate nodes. The first knows the user's IP address, and the third knows where the traffic is destined. The middle works as a sort of trusted intermediary so that nodes one and three have no knowledge of each other. Running huge numbers of servers has the potential to break those anonymity guarantees, said Matt Green, an encryption and privacy expert at Johns Hopkins University.

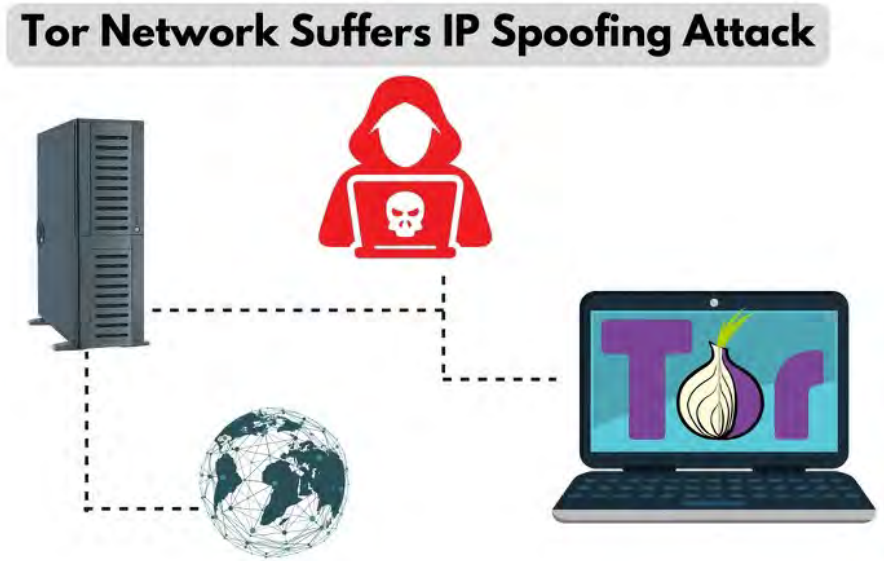
"As long as those three nodes aren't working together and sharing information, Tor can function normally," he said. "This breaks down when you have one person pretending to be a bunch of nodes. All [the attackers] have to be is in the first hop or the third hop." He said that when a single entity operates the first and third nodes, it's easy to infer the information that is supposed to be obfuscated using the middle node.

https://arstechnica.com/information-technology/2021/12/tor-is-under-threat-from-russian-censorship-and-sybil-attacks/

gbhackers.

Tor Network Suffers IP Spoofing Attack Via Non-Exit Relays

November 11, 2024



In late October 2024, a coordinated IP spoofing attack targeted the Tor network, prompting abuse complaints and temporary disruptions.

While the attack affected non-exit relays and caused some relays to be taken offline, the overall impact on Tor users was limited.

Tor directory authorities, relay operators, and the Tor Project sysadmin team began receiving numerous abuse complaints alleging unauthorized port scanning activity.

The complaints were traced to a sophisticated IP spoofing attack. Attackers spoofed Tor-related IP addresses, particularly non-exit relays, to trigger automated abuse reports.

Hidden Wiki .onion Urls Tor Link Directory

Category: / Tags: no tag / Add Comment

To browse .onion Deep Web links, install Tor Browser from http://torproject.org/

Hidden Service lists and search engines

http://3g2upl4pq6kufc4m.onion/ – DuckDuckGo Search Engine

http://xmh57jrzrnw6insl.onion/ – TORCH – Tor Search Engine

---

http://qc7ilonwpv77qibm.onion/ – Western Union Exploit

http://3dbr5t4pygahedms.onion/ – ccPal Store

http://y3fpieiezy2sin4a.onion/ – HQER – High Quality Euro Replicas

http://qkj4drtgvpm7eecl.onion/ – Counterfeit USD

http://nr6juudpp4as4gjg.onion/pptobtc.html – PayPal to BitCoins

http://nr6juudpp4as4gjg.onion/doublecoins.html – Double Your BitCoins

http://lw4ipk5choakk5ze.onion/raw/4588/ – High Quality Tutorials

Marketplace Commercial Services

http://6w6vcynl6dumn67c.onion/ – Tor Market Board – Anonymous Marketplace Forums

http://wvk32thojln4gpp4.onion/ – Project Evil

http://5mvm7cg6bgklfjtp.onion/ – Discounted electronics goods

http://lw4ipk5choakk5ze.onion/raw/evbLewgkDSVkifzv8zAo/ – Unfriendlysolution – Legit hitman service

I2P and Garlic Routing

I2P = Invisible Internet Project

- **Tor uses "onion routing"**
  - Each message from the source is encrypted with one layer for each relay
- **Garlic routing**
  - Combines multiple messages at a relay
  - All messages, each with its own delivery instructions going to one relay are bundled together
  - Makes traffic analysis more difficult
- **Tor circuits are bidirectional: responses take the same path**
- **I2P "tunnels" are unidirectional**
  - One for outbound and one for inbound: the client builds both
  - Sender gets acknowledgement of successful message delivery

Services on top of I2P

- **I2PTunnel: TCP connectivity**
- **Chat via IRC (Internet Relay Chat)**
- **File sharing**
  - BitTorrent
  - iMule (anonymous file sharing)
  - I2Phex: Gnutella over I2P
- **I2P-Bote: decentralized, anonymized email**
  - Messages signed by the sender's private key
  - Anonymity via I2P and variable-rate delays
  - Destinations are I2P-Bote addresses
- **I2P-Messenger, I2P-Talk**
- **Syndie: Content publishing (blogs, forums)**

Status

- **Tor: far more users (currently) → more anonymity**
  - Focused on anonymous access to services
- **I2P: focuses on anonymous hosting of services**
  - Uses a distributed hash table (DHT) for locating information on servers and routing
  - Server addressing
    - Uses cryptographic ID to identify routers and endpoint services

How do you communicate if the government monitors the Internet … or the Internet is not available?

Peer-to-peer communication

- **This was the problem the 2019 Hong Kong pro-democracy protesters faced**
- **Solution:**
  - Use a peer-to-peer mesh network that does not use the Internet
  - Discover neighbors who are running routing software via Bluetooth
  - Messages hop from phone to phone until they find their target
  - Supports private as well as broadcast messages
- **The solution was previously used to enable people to communicate at sporting events & concerts**
- **Also useful in areas hit by storms where Internet infrastructure is down**

Downloads for the Bridgefy app were up almost 4,000% over 60 days between July and Sept 2019

Forbes

Ukrainians Prepping For Internet Loss By Getting Apps For Offline, Private, Mesh Communications

John Koetsier • February 25, 2022

The top apps being downloaded in Ukraine right now are Signal, the private messaging app, Bridgefy, which enables communications without the internet via mesh networking, Maps.me, an offline mapping app, and several "walkie-talkie" apps that enable free communication without sign-ups or personal information.

In other words, Ukrainians are preparing for either the loss of the internet in their country, or the closure of the free internet behind a new digital iron curtain.

Apptopia's top 10 free apps by downloads today in Ukraine.

https://www.forbes.com/sites/johnkoetsier/2022/02/25/ukrainians-prepping-for-internet-loss-by-getting-apps-for-offline-private-mesh-communications/

The End