Information Systems Security (SOEN321)

Anonymous Communications

Dr. Amr Youssef

Concordia Institute for Information Systems Engineering (CIISE)
Concordia University
Montreal, Canada

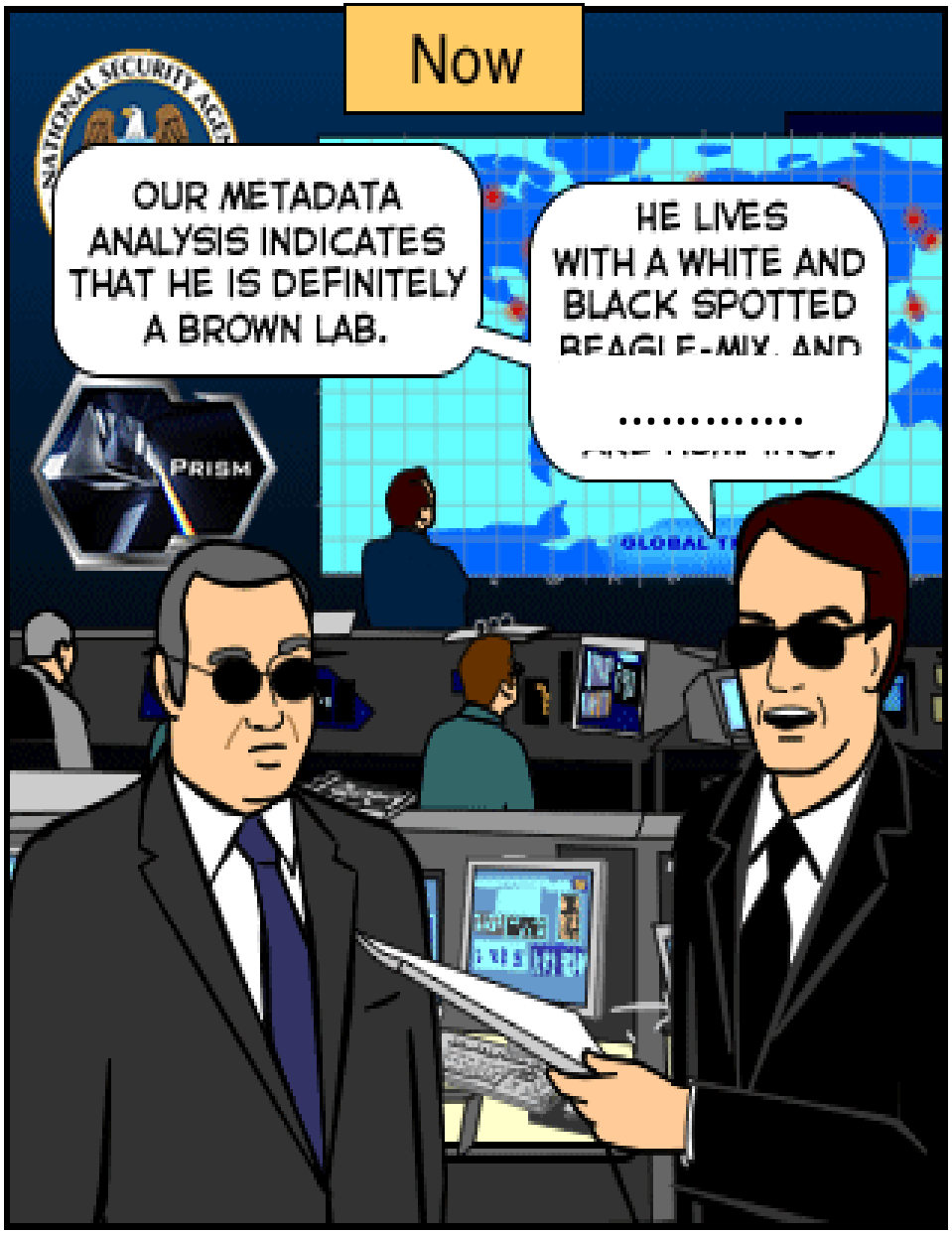
youssef@ciise.concordia.ca

Note: Many of these slides are collected/modified from different books and online resources

Try this before we start

- http://whatismyipaddress.com/
- Try any online proxy
  - E.g., https://hide.me/en/proxy
- Then try http://whatismyipaddress.com/
- Try any Anonymous remailer
    - E.g., http://ultimate-anonymity.com/web-based-remailer.htm
- Think of how you can send me an anonymous email while you are at Concordia
  - Assume that I have full control on IITS/AITS

by Nitrozac & Snaggy



© 2013 Geek Culture

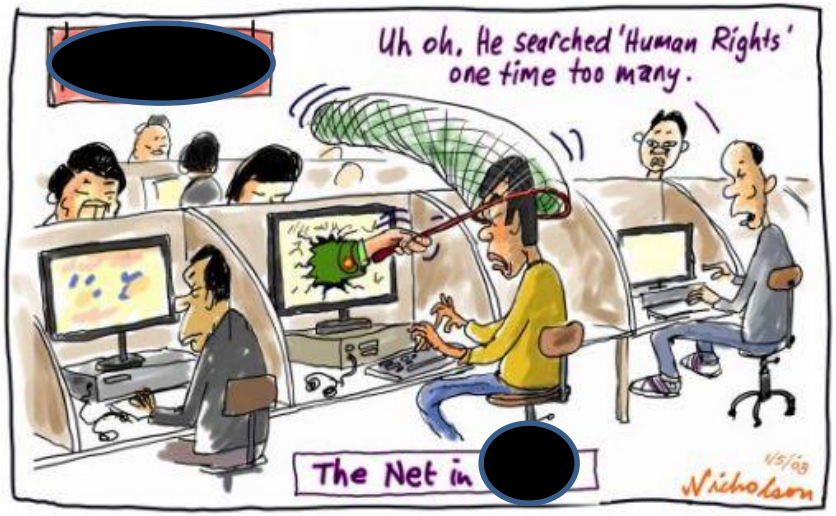
You Are Not Anonymous

- Your IP address can be linked directly to you
  - ISPs store communications records
  - Usually for several years (Data Retention Laws)
  - Law enforcement can subpoena these records
- Your browser is being tracked
  - Cookies
  - Browser fingerprinting
- Your activities can be used to identify you
  - Unique websites and apps that you use
  - Types of links that you click

Yahoo in China

- Provided data to identify and imprison Chinese human right activists
  - 2001: Wang Xiaoning
  - 2002: Jiang Lijun
  - 2003: Li Zhi
  - 2005: Shi Tao

- 2007: Lawsuit against Yahoo → public apology



Wiretapping is Ubiquitous

- Wireless traffic can be trivially intercepted
  - Airsnort, etc.
  - Wifi and Cellular traffic!
  - Encryption helps, if it's strong
    - WEP and WPA are both vulnerable!
  - NSA, GCHQ, "5 Eyes"
    - Focus on encrypted traffic

Who Uses Anonymity Systems?

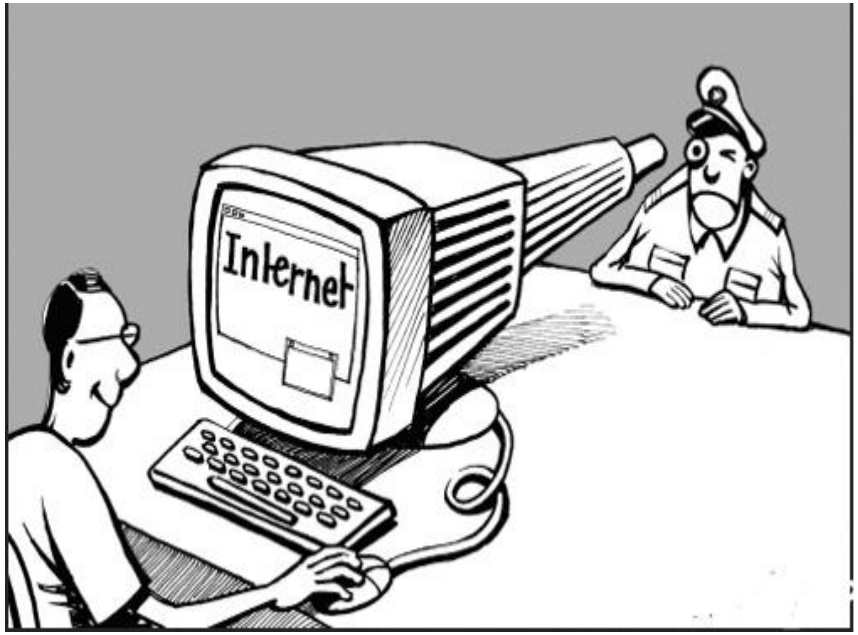
- "If you're not doing anything wrong, you shouldn't have anything to hide."
  - Implies that anonymous communication is for criminals. Is this true?
- The truth: who uses Tor for example?
  - Journalists
  - Law enforcement
  - Human rights activists
  - Normal people

  - Business executives
  - Military/intelligence personnel
  - Abuse victims
- Fact: Tor was/is developed by the Navy

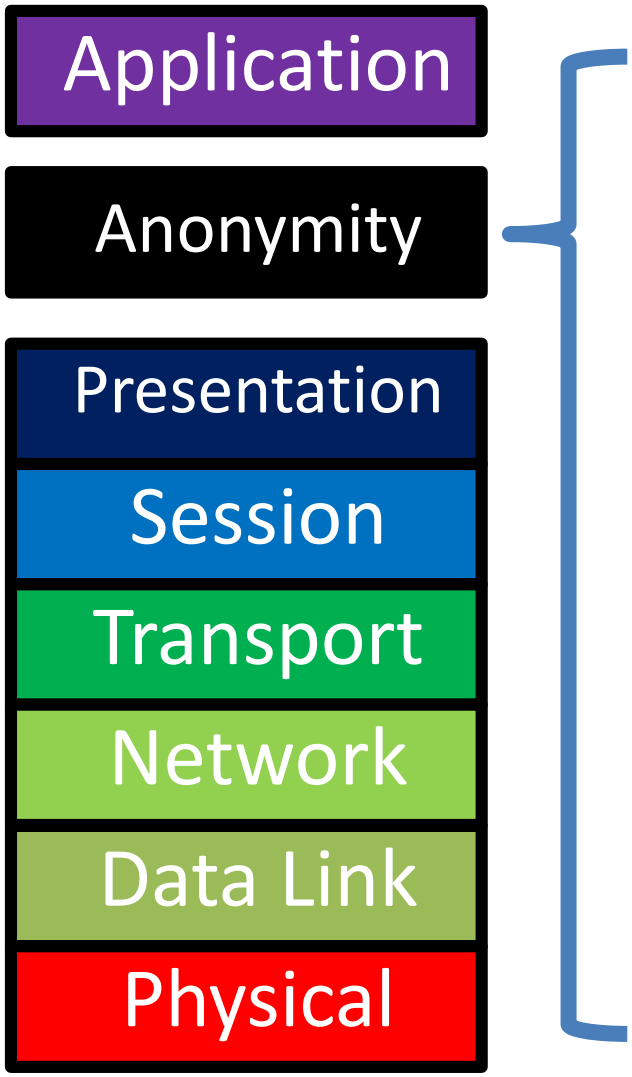
Why Do We Want Anonymity?

- To protect privacy
  - Avoid tracking by advertising companies
  - Viewing sensitive content
    - Information on medical conditions
    - Advice on bankruptcy
- Protection from prosecution
  - Not every country guarantees free speech
  - Downloading copyrighted material (Controversial?)
- To prevent chilling-effects
  - It's easier to voice unpopular or controversial opinions if you are anonymous

SECURITY vs. PRIVACY
1
WHY IS IT EVERY TIME I COME UP AGAINST THIS GUY, I LOSE?!
PRIVACY
6/11 2013
PARKER
COLUMBIA DAILY TRIBUNE
CAGLECARTOONS.COM


Internet

Anonymity Layer



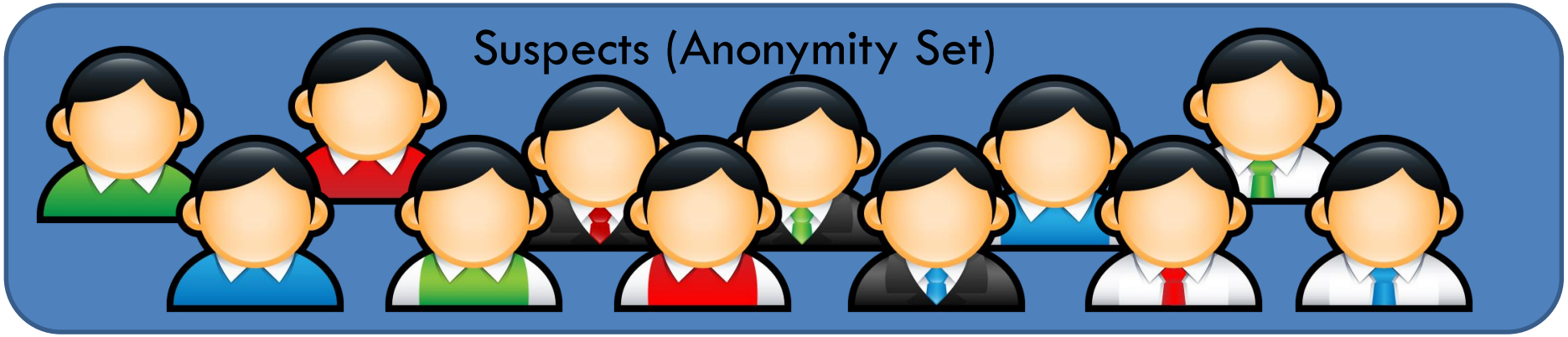
- Function:
  - Hide the source, destination, and content of Internet flows from eavesdroppers
- Key challenge:
  - Defining and quantifying anonymity
  - Building systems that are resilient to deanonymization
  - Maintaining performance

OUTLINE

- ❑ Definitions and Examples
- ❑ Crowds
- ❑ Chaum Mix / Mix Networks
- ❑ Tor

Quantifying Anonymity

- How can we calculate how anonymous we are?
  - **Anonymity Sets**

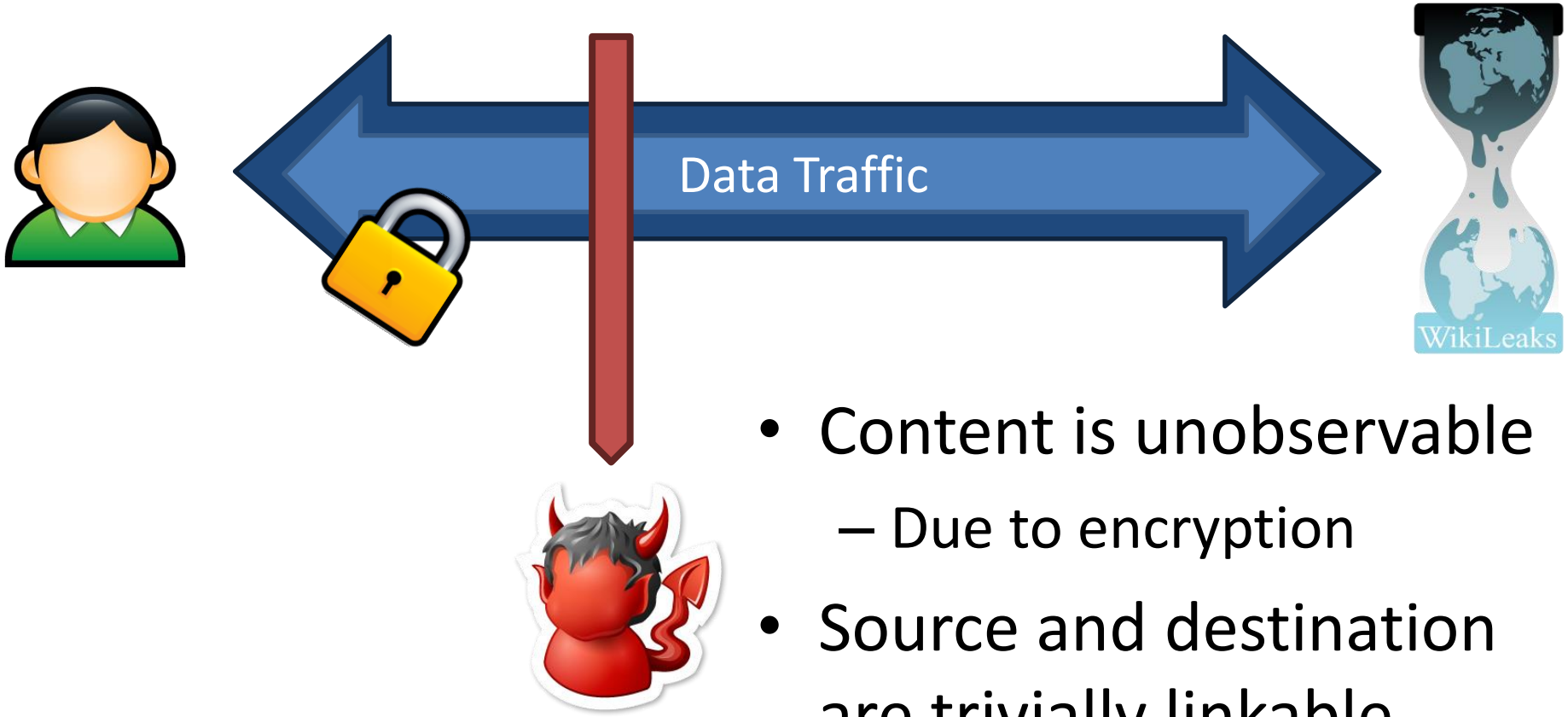


- Larger anonymity set = stronger anonymity

Other Definitions

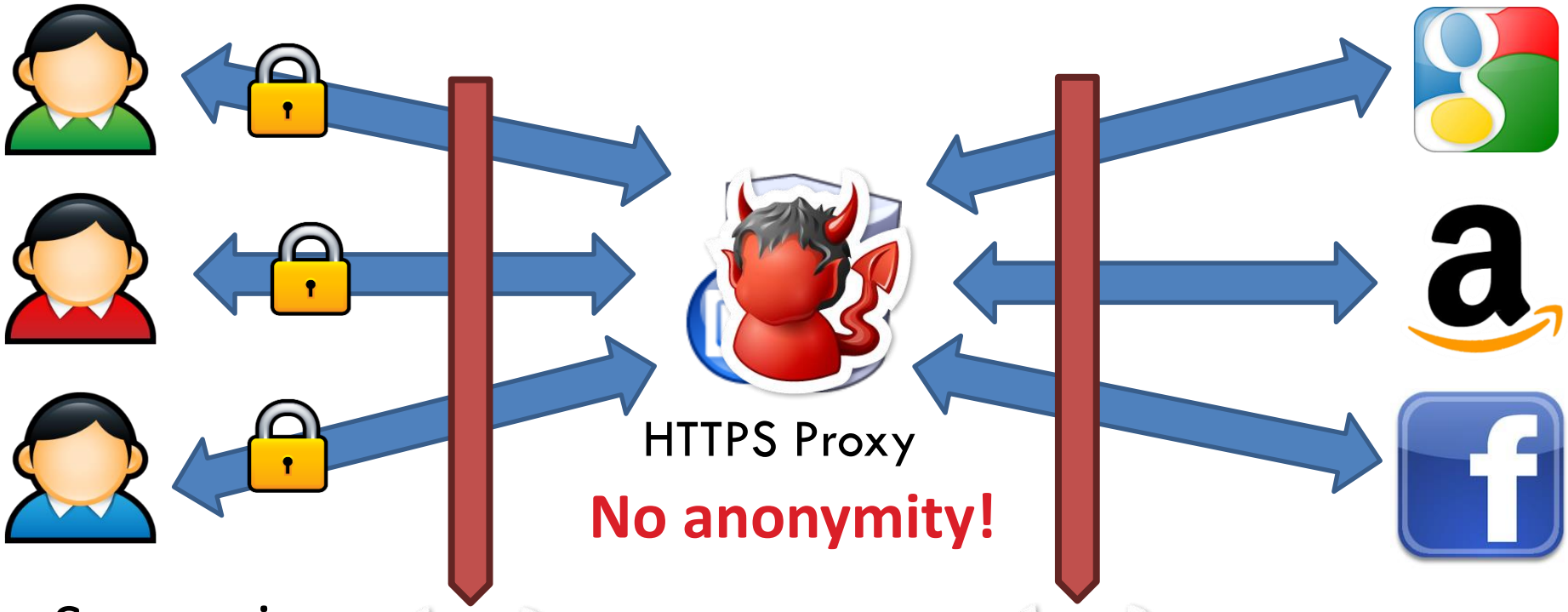
- Unlinkability
  - From the adversaries perspective, the inability to link two or more items of interest
    - E.g. packets, events, people, actions, etc.
  - Three parts:
    - Sender anonymity (who sent this?)
    - Receiver anonymity (who is the destination?)
    - Relationship anonymity (are sender A and receiver B linked?)
- Unobservability
  - From the adversaries perspective, items of interest are indistinguishable from all other items

Crypto (SSL)



- Content is unobservable
  - Due to encryption
- Source and destination are trivially linkable
  - No anonymity!

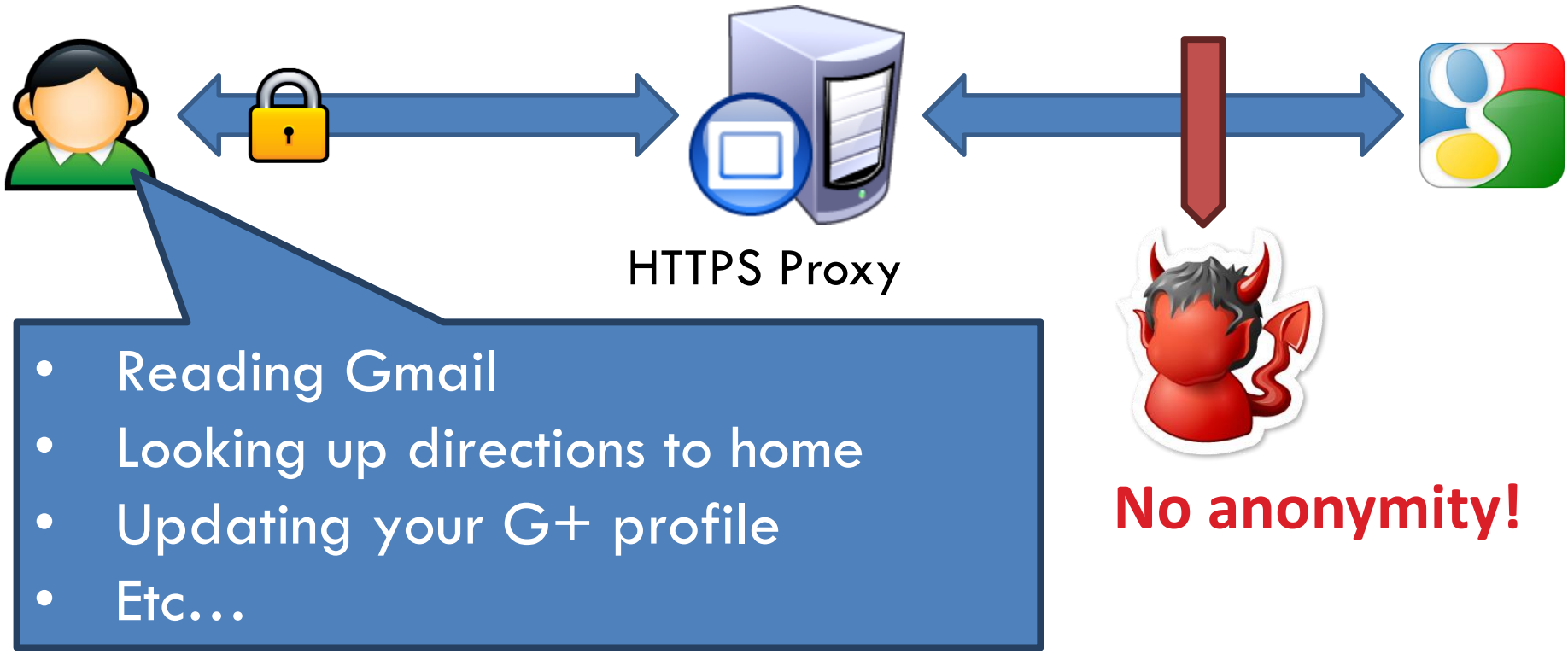
Anonymizing Proxies



- Source is known
- Destination anonymity

- Destination is known
- Source anonymity

Using Content to Deanonymize



- Fact: the NSA leverages common cookies from ad networks, social networks, etc. to track users

Data To Protect

- Personally Identifiable Information (PII)
  - Name, address, phone number, etc.
- OS and browser information
  - Cookies, etc.
- Language information
- IP address
- Amount of data sent and received
- Traffic timing

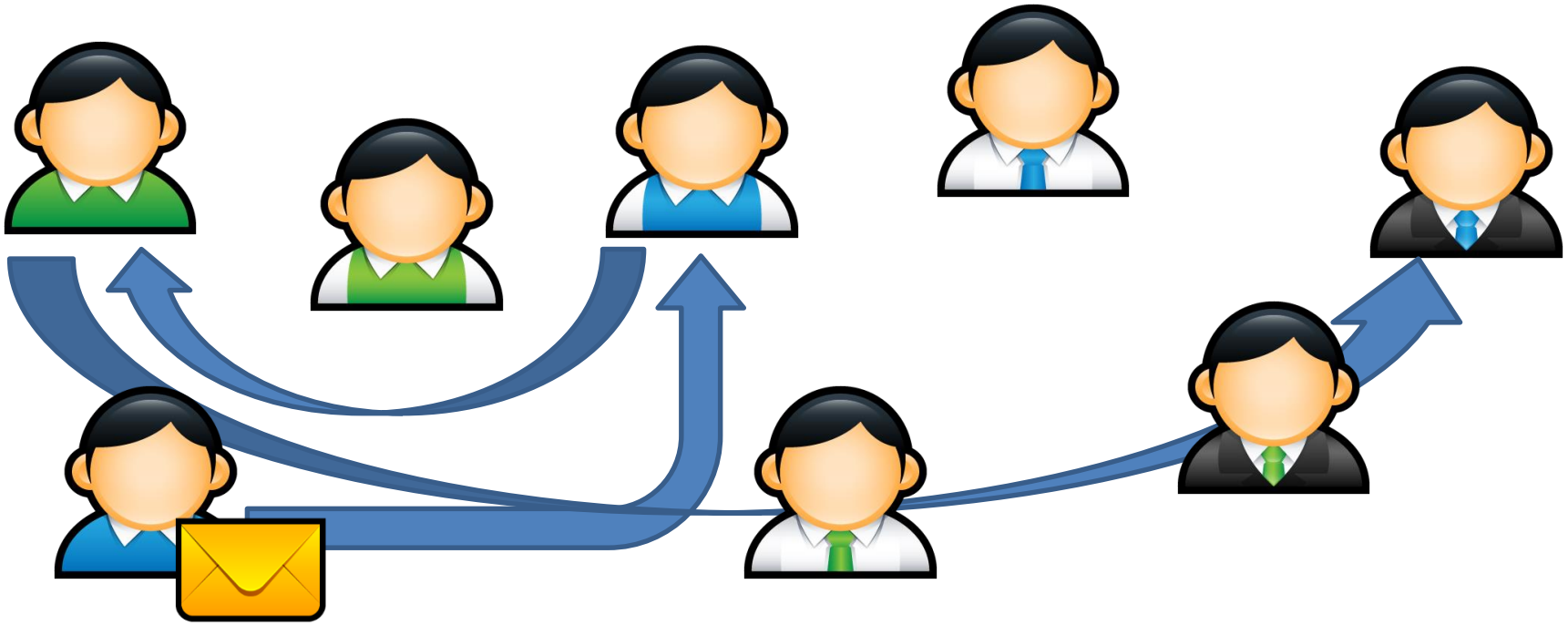
OUTLINE

- ❑ Definitions and Examples
- ❑ Crowds
- ❑ Chaum Mix / Mix Networks
- ❑ Tor

Crowds

- Key idea
  - Users' traffic blends into a crowd of users
  - Eavesdroppers and end-hosts don't know which user originated what traffic
- High-level implementation
  - Every user runs a proxy on their system
  - Proxy is called a jondo
    - From "John Doe," i.e. an unknown person
  - When a message is received, select $x \in [0, 1]$
    - If $x > p_f$: forward the message to a random jondo
    - Else: deliver the message to the actual receiver

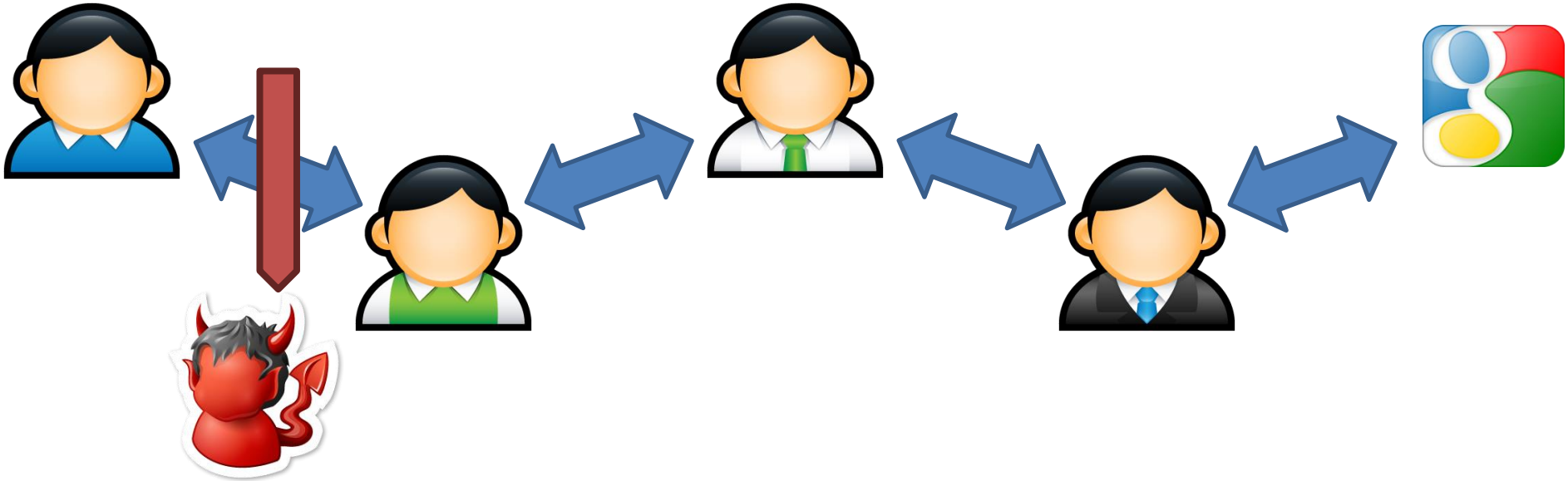
Crowds Example



- Links between users use public key crypto
- Users may appear on the path multiple times

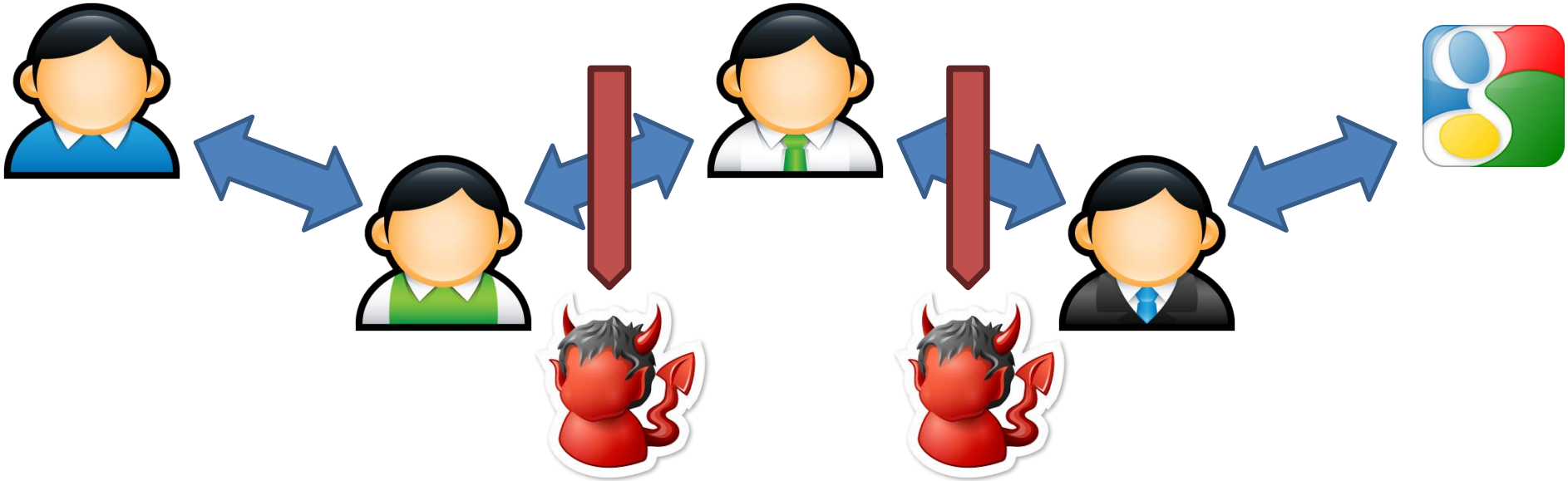
Final Destination

Anonymity in Crowds



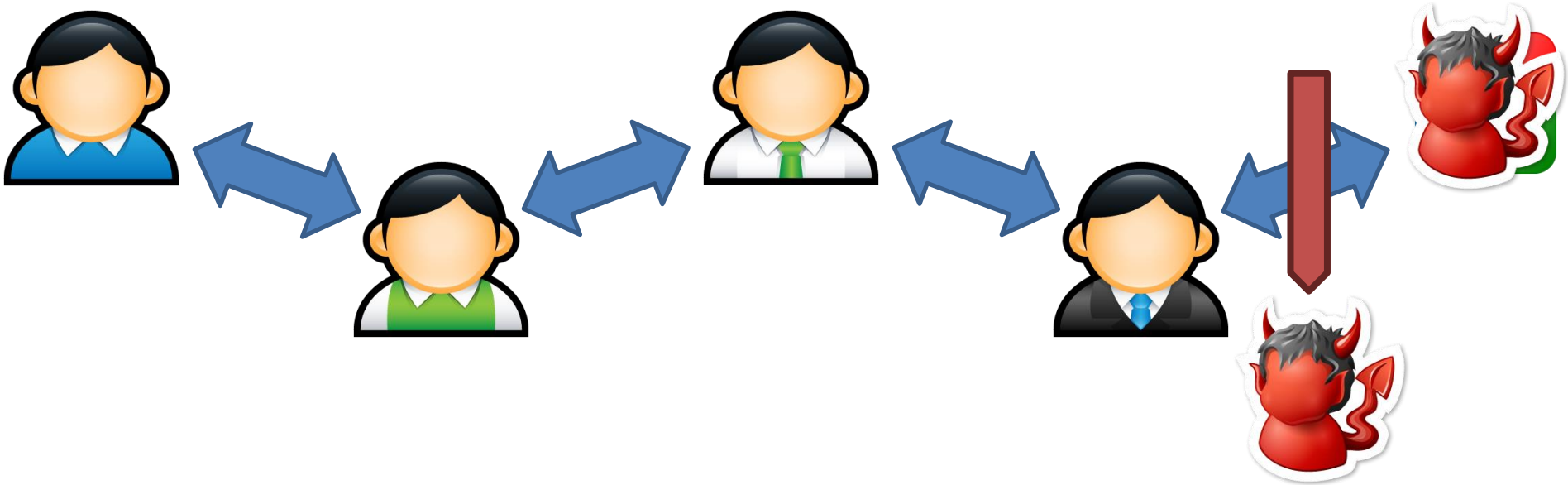
- No source anonymity
  - Target receives *m* incoming messages (*m* may = 0)
  - Target sends *m + 1* outgoing messages
  - Thus, the target is sending something
- Destination anonymity is maintained
  - If the source isn't sending directly to the receiver

Anonymity in Crowds



- Source and destination are anonymous
  - Source and destination are jondo proxies
  - Destination is hidden by encryption

Anonymity in Crowds



- Destination is known
  - Obviously
- Source is anonymous
  - O(n) possible sources, where n is the number of jondos

Other Implementation Details

- Crowds requires a central server called a Blender
  - Keep track of who is running jondos
    - Kind of like a BitTorrent tracker
  - Broadcasts new jondos to existing jondos
  - Facilitates exchanges of public keys

Summary of Crowds

- The good:
  - Crowds has excellent scalability
    - Each user helps forward messages and handle load
    - More users = better anonymity for everyone
- The bad:
  - Very weak destination anonymity
    - Evil jondos can always see the destination

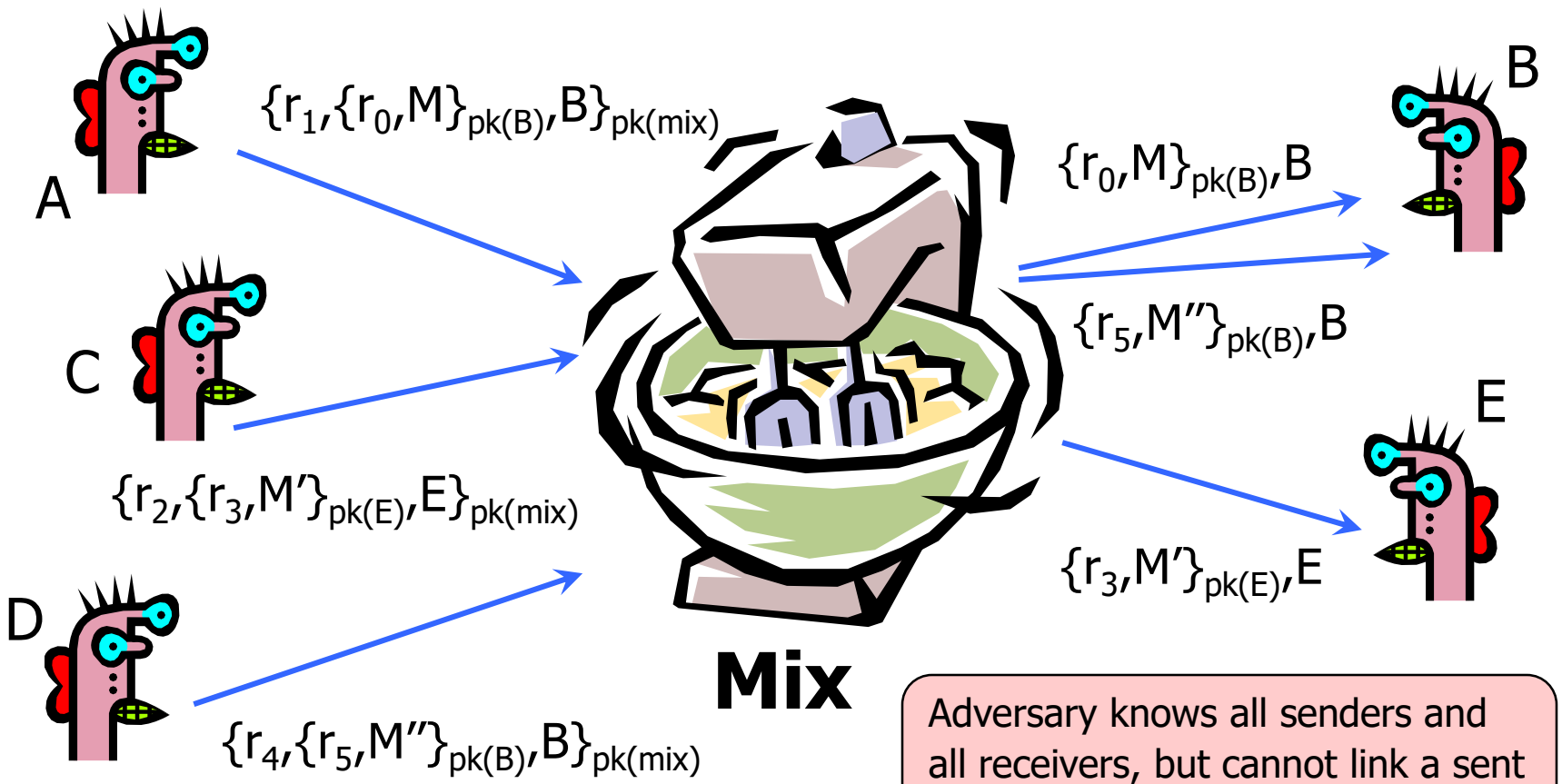
OUTLINE

- ❑ Definitions and Examples
- ❑ Crowds
- ❑ Chaum Mix / Mix Networks
- ❑ Tor

Chaum's Mix

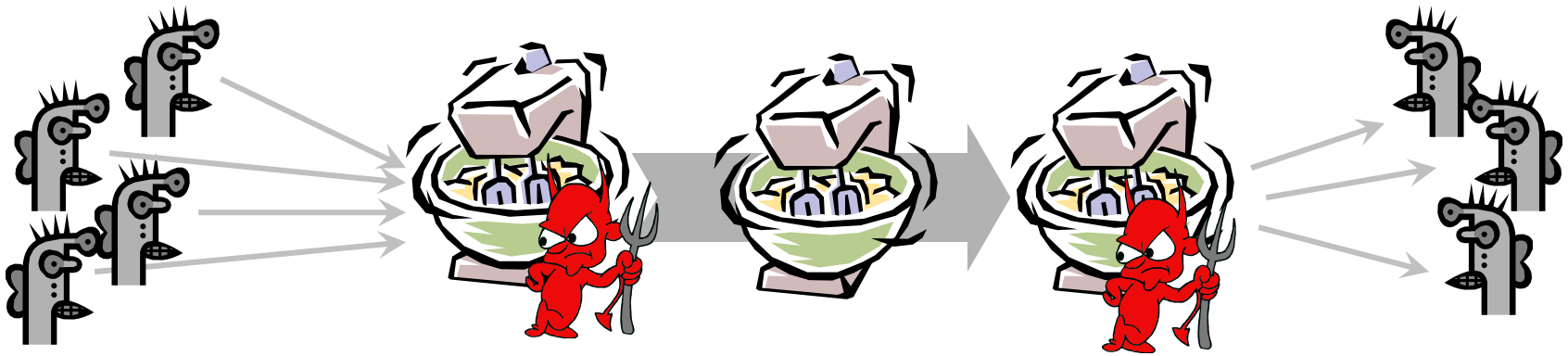
- Early proposal for anonymous email
  - David Chaum. "Untraceable electronic mail, return addresses, and digital pseudonyms". Communications of the ACM, February 1981.
- Public key crypto + trusted re-mailer (Mix)
  - Untrusted communication medium
  - Public keys used as persistent pseudonyms
- Many modern anonymity systems use Mix as the basic building block

Basic Mix Design



Adversary knows all senders and all receivers, but cannot link a sent message with a received message

Mix Cascade



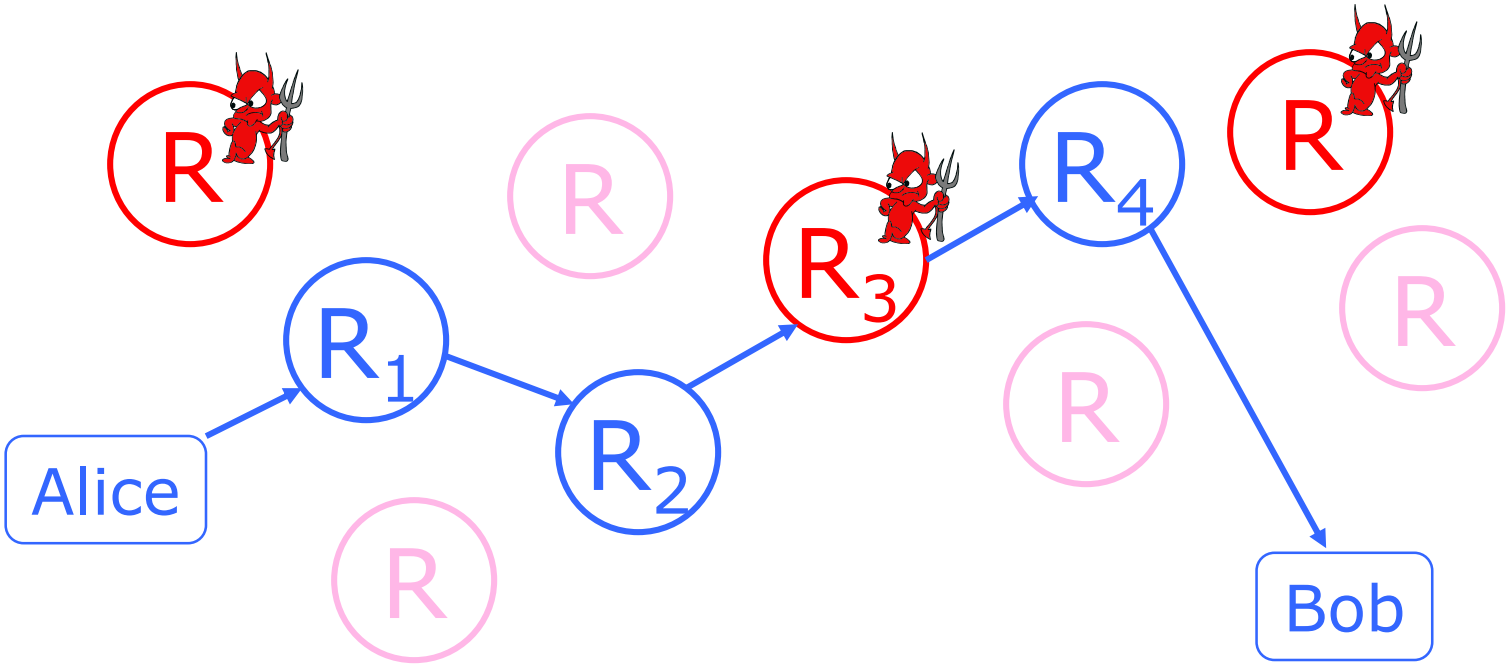
- Messages are sent through a sequence of mixes
  - Can also form an arbitrary network of mixes (mixnet)
- Some of the mixes may be controlled by attacker, but even a single good mix guarantees anonymity
- Pad and buffer traffic to foil correlation attacks

Disadvantages of Basic Mixnets

- Public-key encryption and decryption at each mix are computationally expensive
- Basic mixnets have high latency
  - Ok for email, not Ok for anonymous Web browsing
- Challenge: low-latency anonymity network
  - Use public-key cryptography to establish a "circuit" with pairwise symmetric keys between hops on the circuit
  - Then use symmetric decryption and re-encryption to move data messages along the established circuits
  - Each node behaves like a mix; anonymity is preserved even if some nodes are compromised

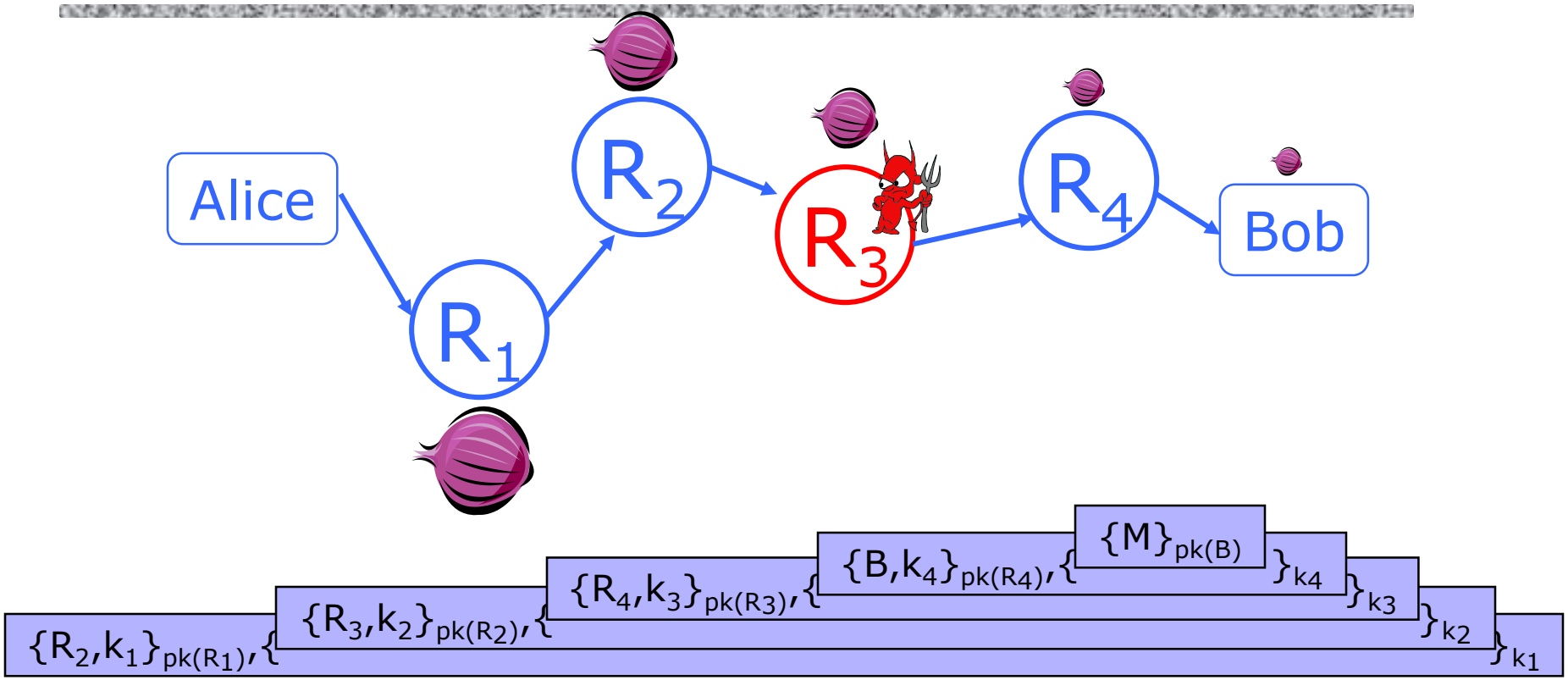
Onion Routing

[Reed, Syverson, Goldschlag 1997]



- Sender chooses a sequence of routers
  - Some may be honest, some controlled by attacker
  - Sender controls the length of the path

Route Establishment



- Routing info for each link encrypted with router's public key
- Each router learns only the identity of the next router

R. Dingledine, N. Mathewson, P. Syverson

Tor:
The Second-Generation Onion Router

(USENIX Security 2004)

Tor: The 2nd Generation Onion Router

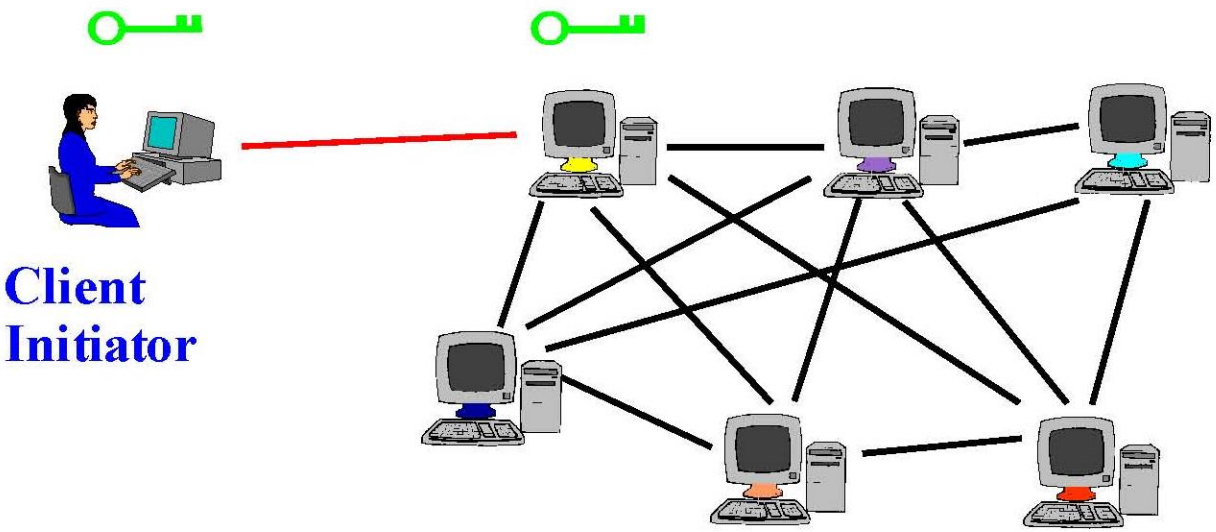
- Basic design: a mix network with improvements
  - Forward secrecy
  - Introduces guards to improve source anonymity
  - Takes bandwidth into account when selecting relays
    - Mixes in Tor are called relays
  - Introduces hidden services
    - Servers that are only accessible via the Tor overlay

Deployment and Statistics

- Largest, most well deployed anonymity preserving service on the Internet
  - Publicly available since 2002
  - Continues to be developed and improved
- Currently, ~5000 Tor relays around the world
  - All relays are run by volunteers
  - It is suspected that some are controlled by intelligence agencies
- 500K – 900K daily users
  - Numbers are likely larger now, thanks to Snowden

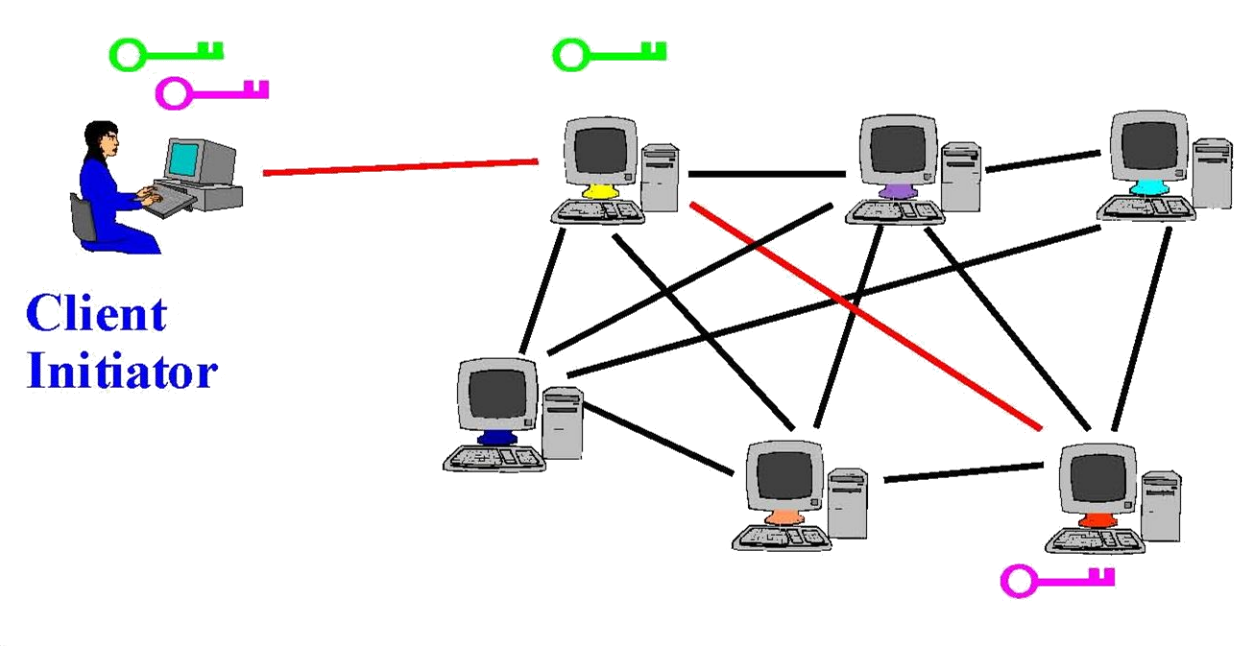
Tor Circuit Setup (1)

- Client proxy establish a symmetric session key and circuit with relay node #1



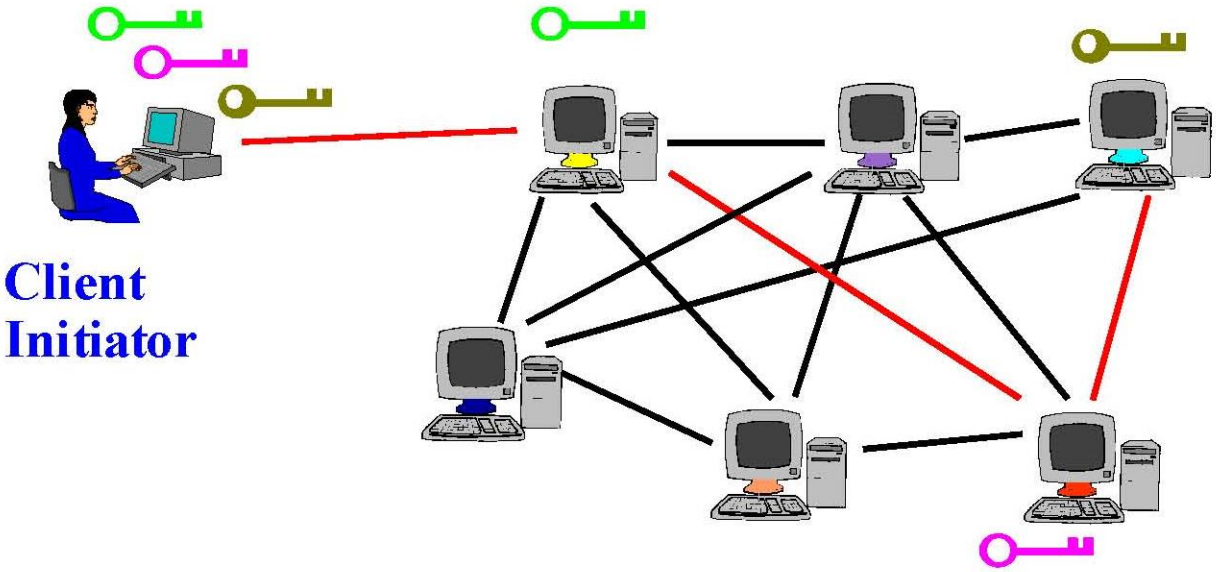
Tor Circuit Setup (2)

- Client proxy extends the circuit by establishing a symmetric session key with relay node #2
  - Tunnel through relay node #1 - don't need !



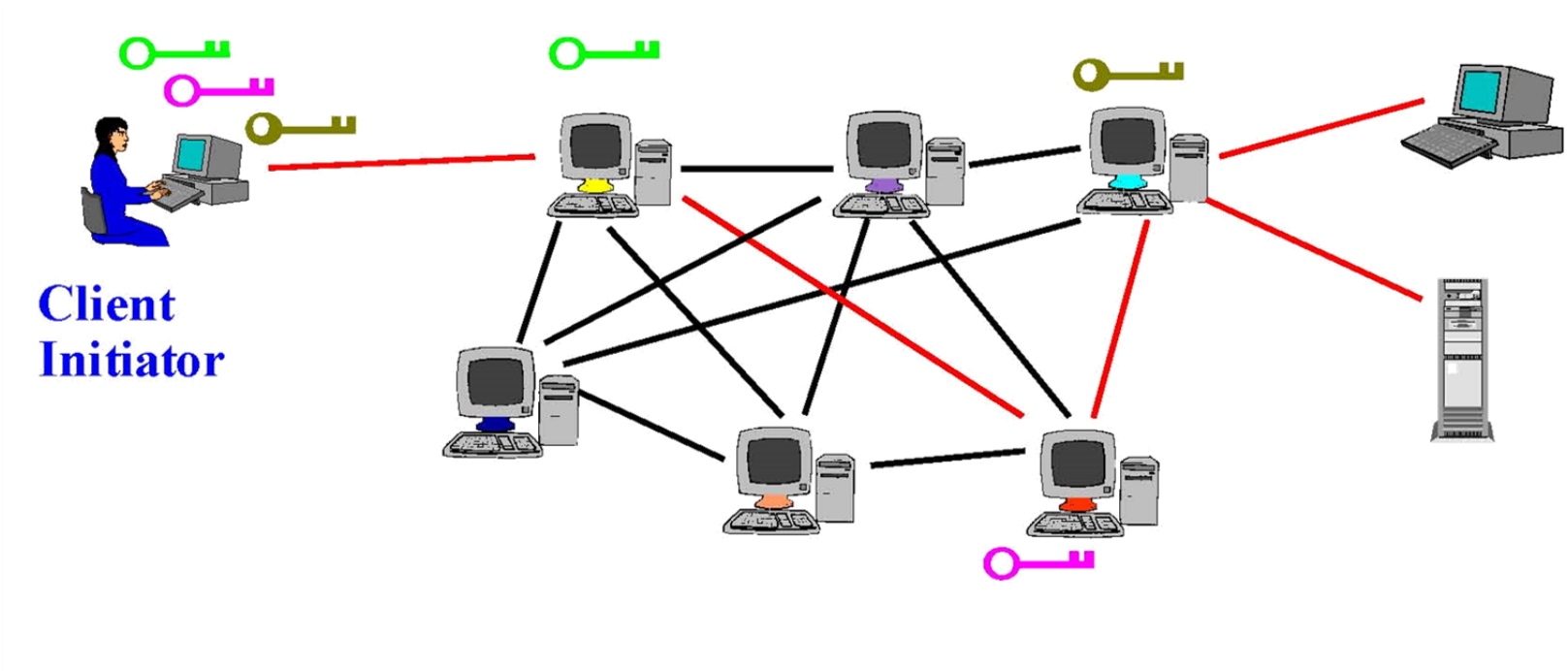
Tor Circuit Setup (3)

- Client proxy extends the circuit by establishing a symmetric session key with relay node #3
  - Tunnel through relay nodes #1 and #2



Using a Tor Circuit

- Client applications connect and communicate over the established Tor circuit
  - Datagrams decrypted and re-encrypted at each link



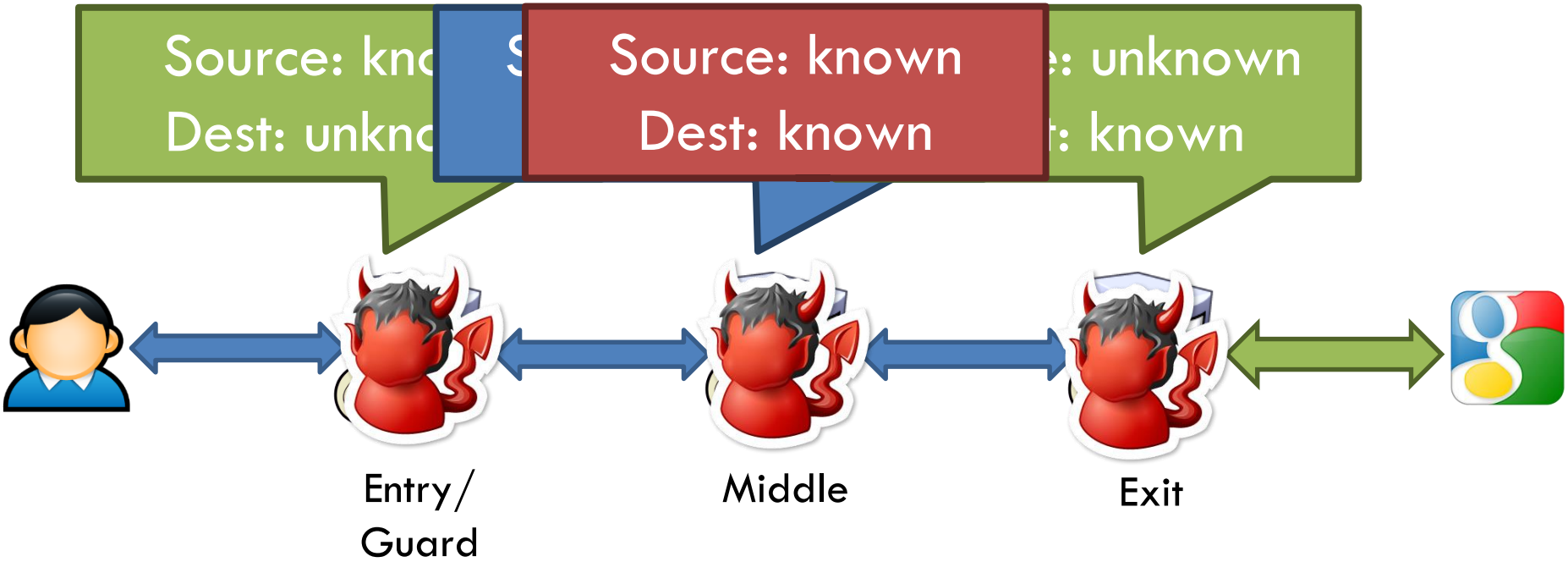
How Do You Use Tor?

1. Download, install, and execute the Tor client
   - The client acts as a SOCKS proxy
   - The client builds and maintains circuits of relays
2. Configure your browser to use the Tor client as a proxy
   - Any app that supports SOCKS proxies will work with Tor
3. All traffic from the browser will now be routed through the Tor overlay

Selecting Relays

- How do clients locate the Tor relays?
- Tor Consensus File
  - Hosted by trusted directory servers
  - Lists all known relays
    - IP address, uptime, measured bandwidth, etc.
- Not all relays are created equal
  - Entry/guard and exit relays are specially labelled
  - Why?
- Tor does not select relays randomly
  - Chance of selection is proportional to bandwidth

Attacks Against Tor Circuits



- Tor users can choose any number of relays
  - Default configuration is 3

Predecessor Attack

- Assumptions:

  - This is the predecessor attack
  - Attacker controls the first and last relay
  - Probability of being in the right positions increases over time

- A

  – (M-1)/(N-1) chance for the last relay

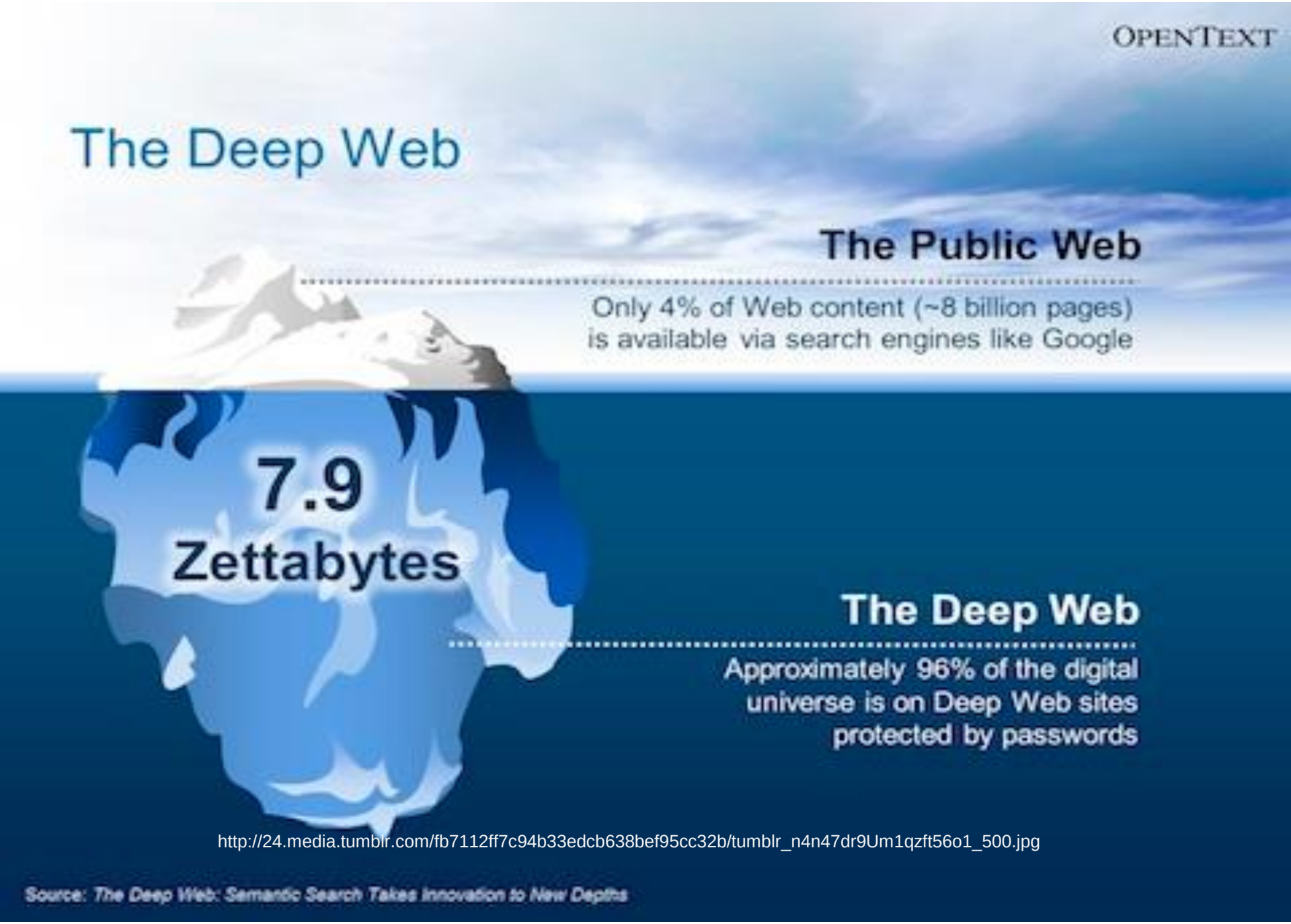
  – Roughly $(M/N)^2$ chance overall, for a single circuit

- However, client periodically builds new circuits

  – Over time, the chances for the attacker to be in the correct positions improves!

Guard Relays

- Guard relays help prevent attackers from becoming the first relay
  - Tor selects 3 guard relays and uses them for 3 months
  - After 3 months, 3 new guards are selected
- Only relays that:
  - Have long and consistent uptimes…
  - Have high bandwidth…
  - And are manually vetted may become guards
- Problem: what happens if you choose an evil guard?
  - M/N chance of full compromise



http://24.media.tumblr.com/fb7112ff7c94b33edcb638bef95cc32b/tumblr_n4n47dr9Um1qzft56o1_500.jpg

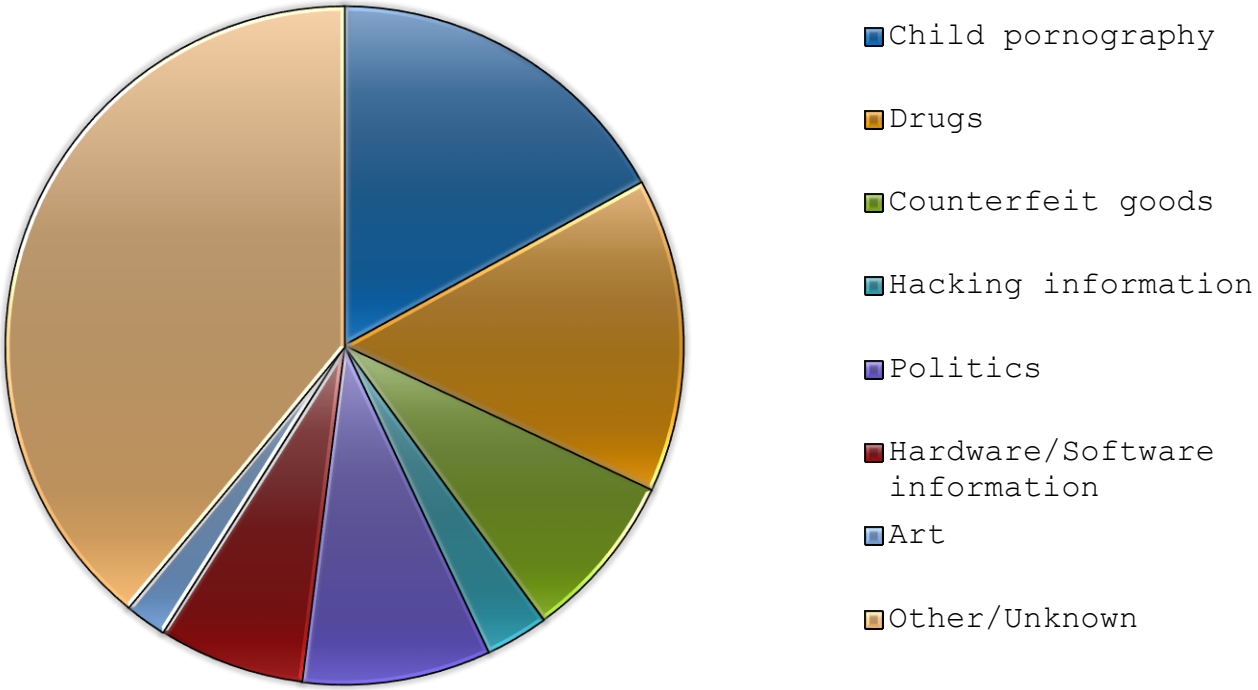
What is this invisible web ?

- All information that cannot be indexed using general web search engines
- Also known as the deep web, deep internet, deepnet, or the hidden web
  - Webpages with no links on them, called disconnected pages
  - Webpages generated from databases
  - Dynamically generated webpages
  - Webpages that require a registration form to access/Password protected webpages

Accessing some of the deep web content

- .onion: is a domain host suffix designating an anonymous hidden service reachable via the Tor network.
- The purpose of using such a system is to make both the information provider and the person accessing the information more difficult to trace, whether by one another, by an intermediate network host, or by an outsider.
- .onion adresses are 16-character non-mneumonic hashes, compromised of alphabetic and numeric strings.
- The "onion" name refers to onion routing, the technique used by Tor to achieve a degree of anonymity.

Darknet Usage



telegraph.co.uk, 22 April 2014

Hidden Services

- Tor is very good at hiding the source of traffic
  - But the destination is often an exposed website
- What if we want to run an anonymous service?
  - i.e. a website, where nobody knows the IP address?
- Tor supports Hidden Services
  - Allows you to run a server and have people connect
  - … without disclosing the IP or DNS name
- Many hidden services
  - Tor Mail, Tor Chat
  - DuckDuckGo
  - Wikileaks
  - The Pirate Bay
  - Silk Road (2.0)

Firefox | Services | Sil... | Hello there. | http://...ST.txt | Sea Kitten P... | http:/...rchiv/ | Welcome to... | TORDIR - Li... | TORDIR - Li... | TORDIR - Li... | Against Ser... | Circle... | BlackMarke... | - Guns - Ha... | Buttery
7jguhsfwruviatqe.onion/index.php/Main_Page
typed in user-password
Log in / create account

The Hidden Wiki

page | discussion | view source | history

navigation
- Main page
- All pages
- Recent changes
- Random page

search
Go Search

toolbox
- What links here
- Related changes
- Special pages
- Printable version
- Permanent link

Main Page

About this Wiki

News / History

- Entries over 30 days old are moved to the Site News Archive.
- See this index for articles regarding anonymity, stenography, marketplaces, software, and other topics.

Comms

- ion@torpm - SiteOp - not checked very often
- OnionNet #hiddenwiki - IRC
- Talk:Main Page - Community notepad for discussion, questions, complaints and suggestions.
- Special:RecentChanges - Discussion, questions, complaints and suggestions

Editor's picks

Bored? Pick a random page from the article index and replace one of the five slots with it.

1. TORCH - Tor Search Engine. Claims to index around 600k pages.
2. List of Anonymous Networks - Try these out and learn from them.
3. Silk Road - Private marketplace with escrow. (Bitcoin)
4. Needed Hidden Services - Ideas for hidden services to benefit the Tor community.
5. Eradic - Quality Deepnet Supplier of Weed, LSD, and Ecstasy (BTC/Dwolla/LR) (Host: FH)

Browsing / Mirroring

These links may be used to browse or mirror all the pages in this wiki:

- Special:AllPages, Admin Dumps, The Hidden Wiki:Back up

Volunteer TODO

Bored? Here are five random things to help out with.

1. Plunder other hidden service lists for links and place them here.
2. File the SnapBBSIndex links wherever they go.
3. Set external links to HTTPS where available, good certificate, and same content.
4. Care to start recording onionland's history? Check out Onionland's Museum.
5. Check the list of dead hidden services for services that have returned.

Hidden services - HTTP/HTTPS

Volunteers last verified all services in this section as up, or marked as DOWN, on: 2011-06-12

Introduction Points

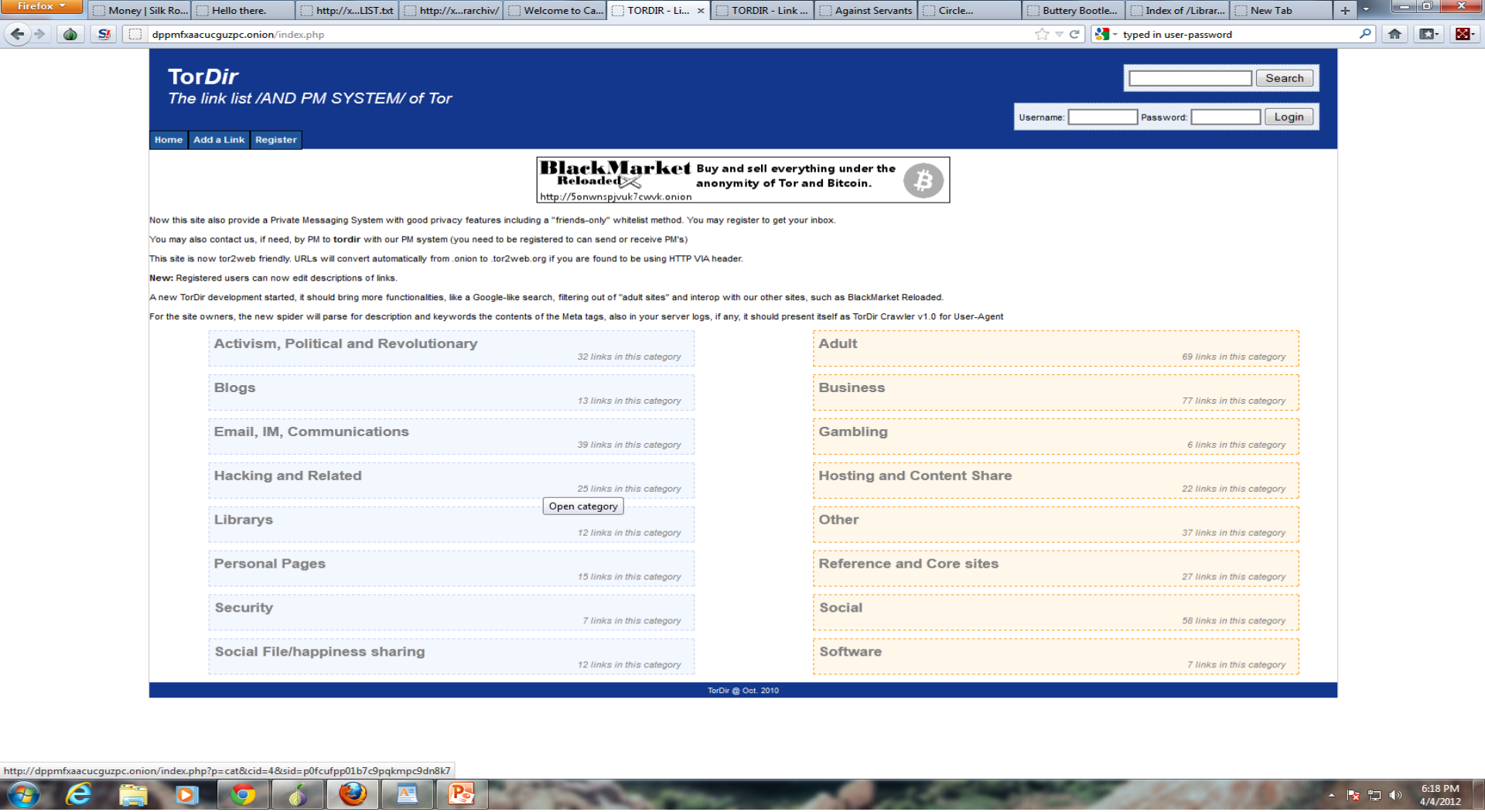
OnionLand link indexes and search engines.

- TorMarks - The fastest-loading TOR directory around. (Host: FH)

Contents [hide]

1 About this Wiki
1.1 News / History
1.2 Comms
1.3 Editor's picks
1.4 Browsing / Mirroring
1.5 Volunteer TODO
2 Hidden services - HTTP/HTTPS
2.1 Introduction Points
2.2 Tor Network
2.3 Marketplace
2.3.1 Financial Services
2.3.2 Commercial Services
2.4 Hosting - Web / File / Image
2.4.1 Webhost comparison
2.5 Blogs
2.6 Forums / Boards / Chans
2.7 Email / Messaging
2.8 Political Advocacy
2.9 Wikis
2.10 Whistleblowing
2.10.1 WikiLeaks
2.10.2 Operation AntiSec
2.10.3 Other
2.11 H/P/A/W/V/C
2.11.1 Phishing Sites
2.12 Audio - Music / Streams
2.13 Video - Movies / TV
2.14 Books
2.15 Drugs
2.15.1 Noncommercial (D)
2.15.2 Commercial (D)
2.16 Erotica
2.16.1 Above Age
2.16.1.1 Noncommercial (E)
2.16.1.2 Commercial (E)
2.16.2 Under Age
2.17 Uncategorized
2.18 Non-English
2.18.1 Czech / Čeština
2.18.2 Danish / Dansk
2.18.3 Dutch / Nederlands
2.18.4 Finnish / Suomi
2.18.5 French / Français

5:09 PM
4/4/2012



One of the other “main pages” of the Deep Web is TorDir. TorDir is a site that uses a special crawler for the Deep Web, so that it may act similar to Google in that it categorizes web sites, and allows you to view many different and obscure .onion sites that fall into each category.

Currency of the Deep Web

- Bitcoins:
  - An electronic cash system using peer-to-peer networking, digital signatures and cryptographic proof to enable irreversible payments between parties without relying on trust. Payments are issued and transferred by the Bitcoin network.
  - Participants begin using Bitcoin by first acquiring a Bitcoin wallet and one or more Bitcoin addresses. Bitcoin addresses are used for receiving Bitcoins, similar to how e-mail addresses are used for receiving e-mail.

Tor Bridges

- Anyone can look up the IP addresses of Tor relays
  - Public information in the consensus file
- Many countries block traffic to these IPs
  - Essentially a denial-of-service against Tor
- Solution: Tor Bridges
  - Essentially, Tor proxies that are not publicly known
  - Used to connect clients in censored areas to the rest of the Tor network
- Tor maintains bridges in many countries

Obfuscating Tor Traffic

- Bridges alone may be insufficient to get around all types of censorship
  - DPI can be used to locate and drop Tor frames
  - Some countries blocked all encrypted packets for some time
- Tor adopts a pluggable transport design
  - Tor traffic is forwarded to an obfuscation program
  - Obfuscator transforms the Tor traffic to look like some other protocol
    - BitTorrent, HTTP, streaming audio, etc.
  - Deobfuscator on the receiver side extracts the Tor data from the encoding

Summary

- Presented a brief overview of popular anonymity systems
  - How do they work?
  - What are the anonymity guarantees?
- Introduced Tor
- Lots more work in anonymous communications
  - Dozens of other proposed systems
    - Tarzan, Bluemoon, etc.
  - Many offer much stronger anonymity than Tor
  - … however, performance is often a problem

How “Bad” People Got Caught

Case 0:
Harvard Bomb Threat

- All Tor nodes are publicly known (except bridges): http://torstatus.blutmagie.de
- Easy to correlate who was attached to Harvard network and using Tor at the same time the email was sent (unless you use a bridge).
- Eldo Kim was connected to the Tor network around that time.
- Suspect Eldo Kim wanted to get out of a final and admitted he made the bomb threat when interviewed.

The Harvard Case

Case 0: Harvard Bomb Threat

Lessons Learned:

- Don't be the only person using Tor on a monitored network at a given time
- Use a bridge?
- Don't admit anything
- Correlation attacks

More importantly:
Do NOT get involved in any illegal activities

The Silk Road

Firefox | Money | Silk R... | Hello there. | http://xs...KLIST.txt | http://xq...rarchiv/ | Welcome to Card... | TORDIR - Link List | TORDIR - Link List | Against Servants | Circle... | Buttery Bootleggi... | Index of /Library/...

silkroadvb5piz3r.onion/silkroad/category/98

typed in user-password

Silk Road
anonymous marketplace

Welcome **43567rssdfgh**!
messages(1) | orders(0) | account(฿0.00) | settings | log out

search | (0)

- *Money(78)*
  - Bullion(1)
  - Digital currencies(12)
  - Loans(2)
- Apparel(25)
- Books(259)
- Computer equipment(4)
- Digital goods(119)
- Drug paraphernalia(15)
- Drugs(1371)
- Electronics(5)
- Fireworks(1)
- Forgeries(30)
- Hardware(1)
- Lab Supplies(5)
- Medical(3)
- Musical instruments(2)
- Services(31)
- XXX(119)

sort by bestselling | Domestic only | update

title	price	seller	ship from	
Your USD for MY BTC= NO FEES!	฿0.02	BTC Buddy	undeclared	add to cart
Need bitcoins? Bitcoins for your moneypak.	฿0.00	Sugar Mama	undeclared	add to cart
BTC4M.P. DON'T GET SUCKERED IN SECONDS!!! BTC4M.P.	฿0.02	BTC Buddy	undeclared	add to cart
Need bitcoins? Bitcoins for your moneypak.	฿0.00	Sugar Mama	undeclared	add to cart
VENDORS. I WANT YOUR BTC	฿0.20	BTC Buddy	undeclared	add to cart
Your USD for MY BTC= NO FEE!	฿0.02	BTC Buddy	undeclared	add to cart
30 Day Loan Pool Program	฿0.00	badboy97(100)	undeclared	add to cart
Lottery to Benefit WikiLeaks (Win $100!!!)	฿0.41	RickyRango(98)	United States of America	add to cart
Bitcoin exchange to paypal 100€	฿31.86	ExchangeService(97)	undeclared	add to cart
0% comission BitCoin for Westernunion or Moneygram	฿0.00	googleyed(99)	undeclared	add to cart
LIMITED BTC AVAILABLE NOW	฿0.02	BTC Buddy	undeclared	add to cart
Bitcoin for your UKash *Low commision guarantee*	฿0.00	googleyed(99)	undeclared	add to cart
Selling bitcoins? Moneypaks for your bitcoins!	฿0.00	Sugar Mama	undeclared	add to cart
bitcoin to paypal exchange 100$	฿24.77	ExchangeService(97)	undeclared	add to cart
$100 U.S. Federal Reserve Note	฿23.61	uglysurfer(99)	undeclared	add to cart
LIMITED BTC AVAILABLE NOW	฿0.02	BTC Buddy	undeclared	add to cart
Barcode Manipulation scam keeping your store safe	฿0.59	warweed(98)	undeclared	add to cart
Need bitcoins? Bitcoins for moneygram!	฿0.00	Sugar Mama	undeclared	add to cart

- One of the many online black markets.
- Did not require a paid membership for buyers.
- 1.2B $ in revenue and $80M in commission (70% of online Drug market)
  - It is interesting to think on how to cash this $80M worth of Bitcoins
  - Involved 145,000 Byers and 2500 vendors. A total of 1M transactions
  - If a legitimate startup, it would have been valued $2.4B
  - Arrest through (Marco Polo) operation that involved FBI, IRS, DHS, DEA, US secret, service, US postal inspection, etc

6:03 PM

The Silk Road case

- The earliest they could find was from “altoid” on the Shroomery.org forums on 01/27/11. http://www.shroomery.org/forums/showflat.php/Number/13860995

Ignore

GLBSE.com

ShadowOfHarbringer
Hero Member

Activity: 1260

Bringing Har® to you since 1952

Ignore

Re: A Heroin Store
January 30, 2011, 08:09:37 PM

#71

Quote from: Nefario on January 30, 2011, 06:30:07 AM

(probably berried in the desert or in a forest)

Somehow, I'm seeing tremendous increase of popularity of forest sightseeing ☺

Quote from: altoid on January 29, 2011, 07:44:51 PM

What an awesome thread! You guys have a ton of great ideas. Has anyone seen Silk Road yet? It's kind of like an anonymous amazon.com. I don't think they have heroin on there, but they are selling other stuff. They basically use bitcoin and tor to broker anonymous transactions. It's at http://tydgccykixpbu6uz.onion. Those not familiar with Tor can go to silkroad420.wordpress.com for instructions on how to access the .onion site.

Let me know what you guys think

So here we go, first Bitcoin drug store.
We're going into deep water faster than i thought then.

I wonder how long will it take for govs to start investigating Bitcoin.

{{ Bitcoin.pl Elite Member, Bitcointalk Hero Member [1176] }}
1NLWBAD7ZD82fJDDawKfp5RAKSR8YWWYd3 | GPG/PGP Keys [3072D/F92EDBA4]
Hate forced fees ? Use "No Forced TX Fee" Bitcoin Client fork. **Now updated to v0.8.6 !** (use carefully !)

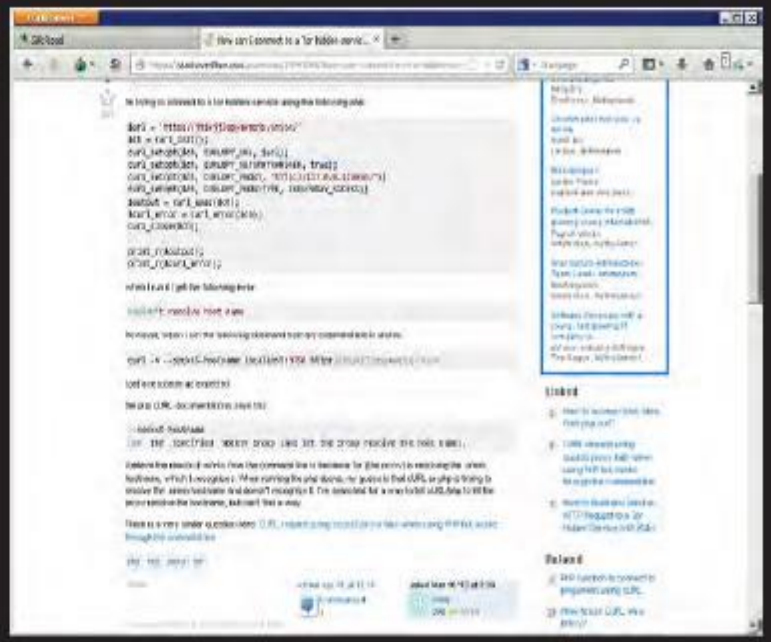
grondilu
Hero Member

Re: A Heroin Store
January 30, 2011, 08:45:31 PM

#72

The Silk Road case

- "Ross Ulbricht." account also posted on StackOverflow asking for help with PHP code to connect to a Tor hidden service. The username was quickly changed to "frosty" (03/16/12). http://stackoverflow.com/questions/15445285/how-can-i-connect-to-a-tor-hidden-service-using-curl-in-php



- Guess who is now a suspect for being "Dread Pirate Roberts"? Ross William Ulbricht.

The Silk Road case

- Someone was connecting to a server that hosts the Silk Road from an Internet café near where Ross lived in San Francisco. Private messages on Silk Road make it seem Dread Pirate Roberts lived in the Pacific time zone.
- IP of a Silk Road server was attached to via a VPN server that was connected to by an IP belonging to an Internet cafe on Laguna Street in San Francisco from which Ulbricht had also connected to his Gmail account with (both on June 3, 2013).
- PM to Dread Pirate Roberts from a user said the site was leaking "some sort of external IP address" belonging to the VPN.
- FBI starts taking down SilkRoad servers, though I'm are not sure how they were found. Could have been money trail to aliases, or as Nicholas Weaver conjectured, they hacked SilkRoad and made it contact an outsides server without using Tor so it revealed it's real IP. Once located, FBI was able to get a copy of one of the servers.

- On 07/10/13 US Customs intercepted 9 IDs with different names, but all having a picture of Ulbricht. Homeland Security interviewed Ulbricht, but he denied having ordered them.

- Smart: “ULBRICHT generally refused to answer any questions pertaining to the purchase of this or other counterfeit identity documents.”
- Stupid: “However, ULBRICHT volunteered that "hypothetically" anyone could go onto a website named "Silk Road" on "Tor" and purchase any drugs or fake identity documents the person wanted. “
- Roommates knew him as “Josh”. PMs show DPR was interested in getting fake IDs.

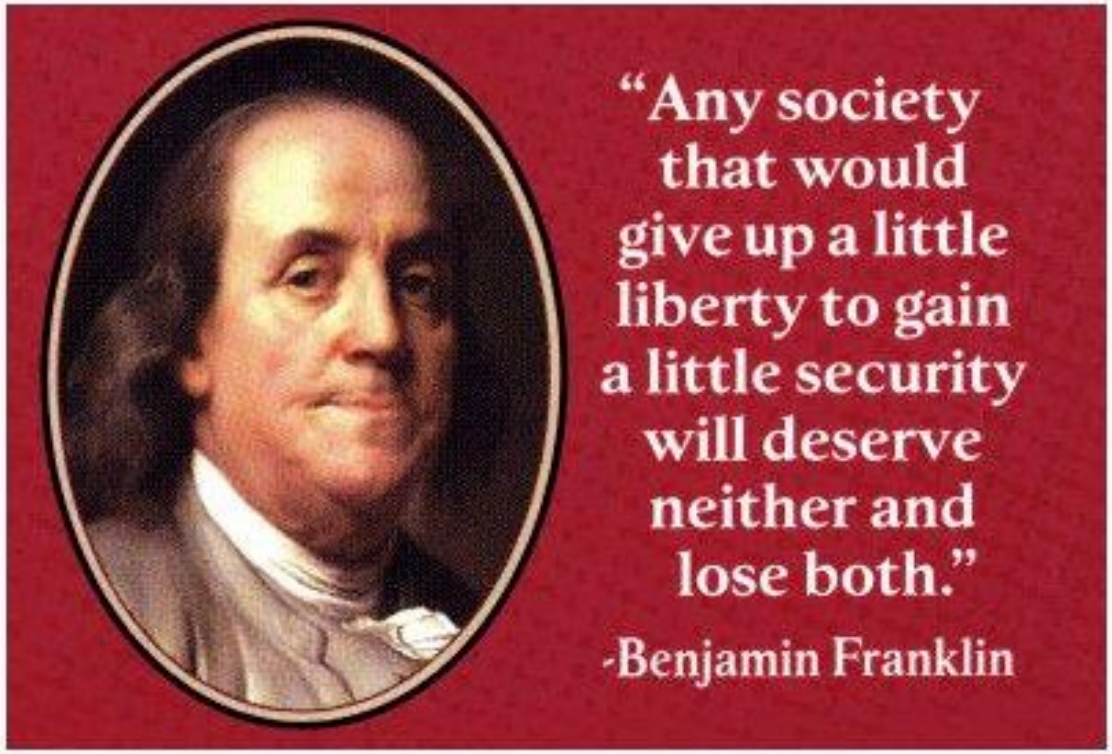
- Server used SSH and a public key that ended in frosty@frosty. Server also had some of the same code posted on StackOverflow.
- Eventually, on 10/01/2013 the FBI Landed on him in a Library right after he entered the password for his laptop. More evidence was found on his laptop.

Lessons Learned:

- Keep online identities separate
  - Keep different usernames
  - From different locations
- Have a consistent story
- Don’t talk about interests
- Don’t volunteer information!

Once More:

The real lesson is that you should never get involved in any illegal activities



Interesting projects:
Evaluate the privacy of a whistleblower submission system:
https://securedrop.org/
Used by Canadian news agenesis such as CBC:
https://securedrop.cbc.ca/