Anonymous Network Concepts & Implementation

kevinkoo001@gmail.com

Overview

1. Overview & Background

2. Anonymous Network

   tor

   freenet

   Gnunet

   I2P

3. Circumvention Techniques against Censorships

   Obfsproxy

   flashproxy

Overview

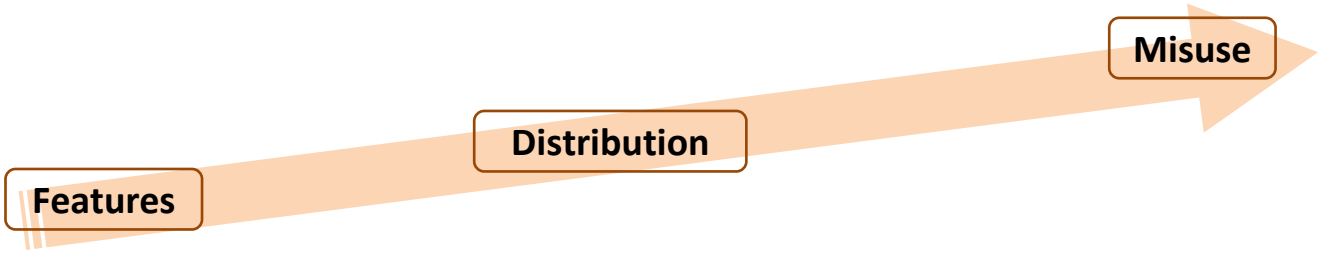
- Attack Trends Summary
  - Modern attack mostly involves malware, which
    - ✓ Attempts to conceal attack itself
    - ✓ Makes it hard to trace themselves down from network perspective
    - ✓ Makes it difficult to find artifacts by wiping out themselves from system perspective
    - ✓ Employs many techniques to be hard for analysis including:
      Anti-VM, Anti-disassembly, Anti-debugging and cryptography
    - ✓ Infects a target but do nothing harm until they achieve their goals
  - Imagine how future malware will evolve, which
    - ✓ Employs the combination of existing – even legitimate – tools/techniques in a malicious fashion
    - ✓ Emerges new variables targeting cloud computing
    - ✓ Focuses highly on target-oriented attack which does not affect others
    - ✓ Uses steganography technique in a wild more often
    - ✓ Forms private tor network with exploited zombie machines

Overview

- Malware/Crimeware

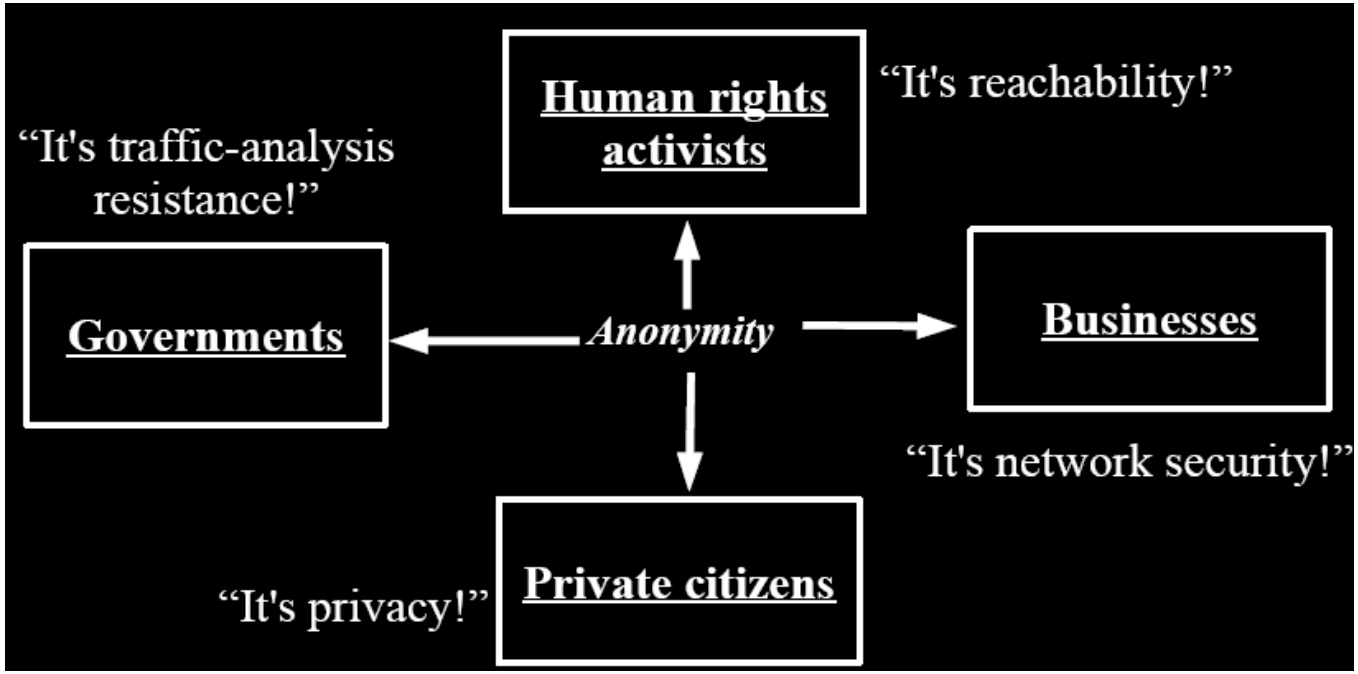
❖ Let's briefly take a look at what to have, how to spread and what to do.

✓ Key Loggers	✓ Attachment	✓ Information Compromise
✓ Screenscrapers	✓ Peer-to-Peer Networks	✓ Spam Transmission
✓ Email, IM Redirectors	✓ Piggybacking	✓ Denial-of-Service, DDoS
✓ Session Hijackers	✓ Internet Worms, Virus	✓ Click Fraud
✓ Web Trojans	✓ Web Browser Exploits	✓ Data Ransoming
✓ Transaction Generators	✓ Server Compromise	✓ Identity Stealing
✓ Data Theft	✓ Affiliate Marketing	✓ Credit Card Abuse
✓ Man-in-the-Middle	✓ Phishing	✓ Defamation
✓ Rootkits	✓ Pharming	✓ Embezzlement
		✓ Political Argument



Background

- Necessity / Motivation (1/2)
  - *"Anonymity serves different interests for different user groups."* by Roger Dingledine, the creator of the Tor



Background

- Necessity / Motivation (2/2)

❖ Regular citizens do not want to be watched and tracked.
❖ Businesses need to keep trade secrets.
❖ Law enforcement needs anonymity to get the job done.
❖ Government need anonymity for their security.
❖ Journalists and activists need anonymity for their personal safety.
❖ Hard to configure your own network though!!

But...

❖ Compromised botnets
❖ Stolen mobile phones
❖ Open wireless nets
❖ Malware spread (trojans, virus, worms)
❖ Spamming
❖ Phishing

Implemented Anonymous Network

(1) tor

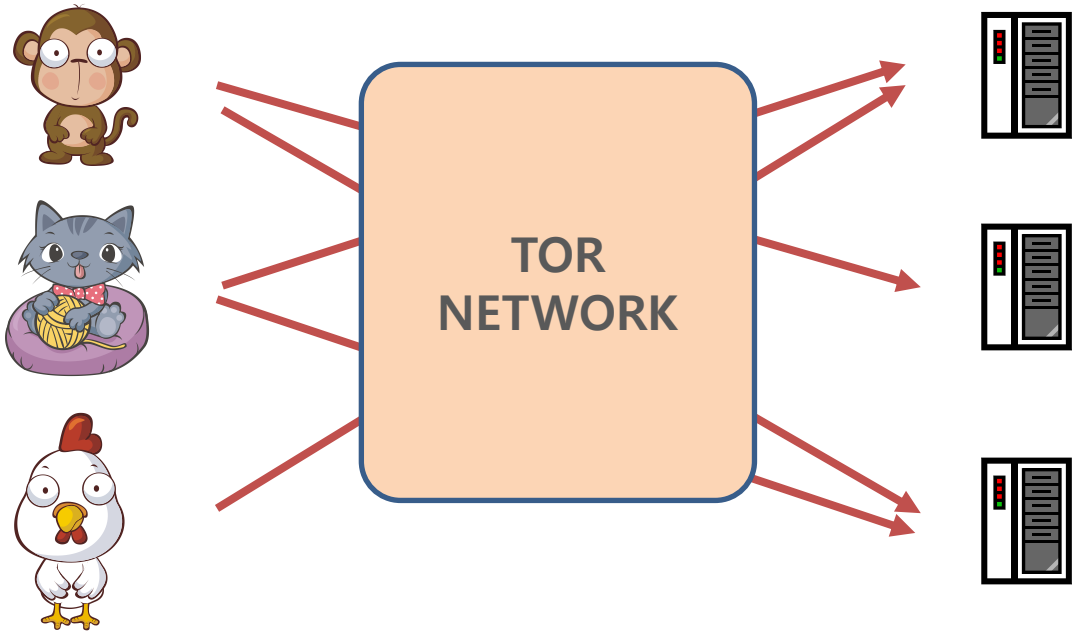
(2) freenet

(3) Gnunet

(4) I2P

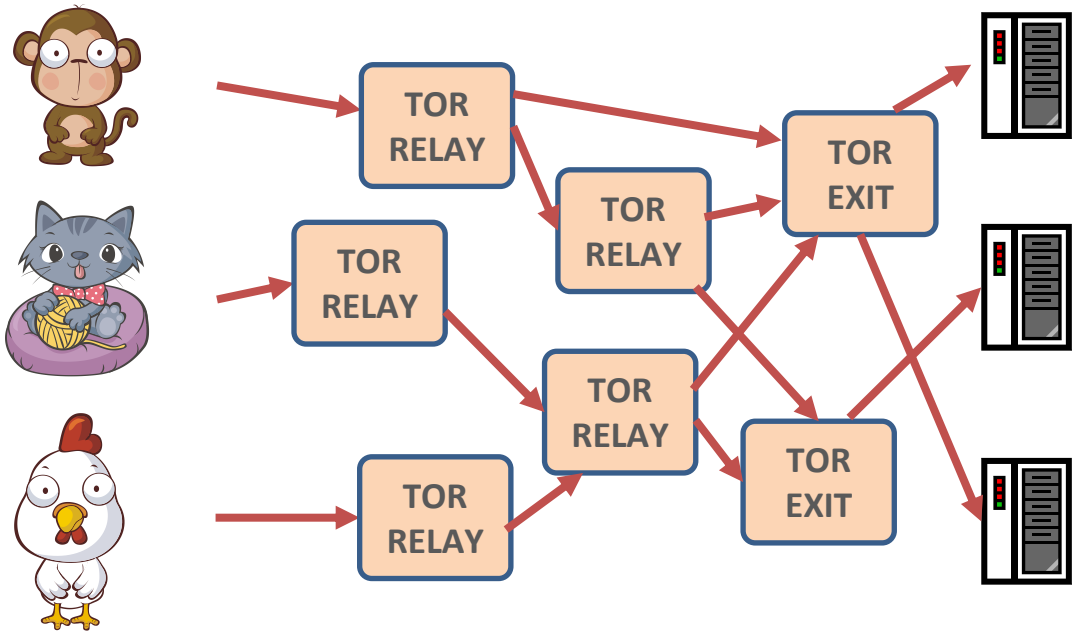
Implemented Anonymous Network - Tor

- The Tor (the Onion Routing) at a glance
  - When there is an evil user or server, then it could be blocked with ease.
  - Tor is designed for hiding where the communication comes from, and going to.



Implemented Anonymous Network - Tor

- The Tor (the Onion Routing) at a glance
  - Tor network consists of many relay and exit nodes.



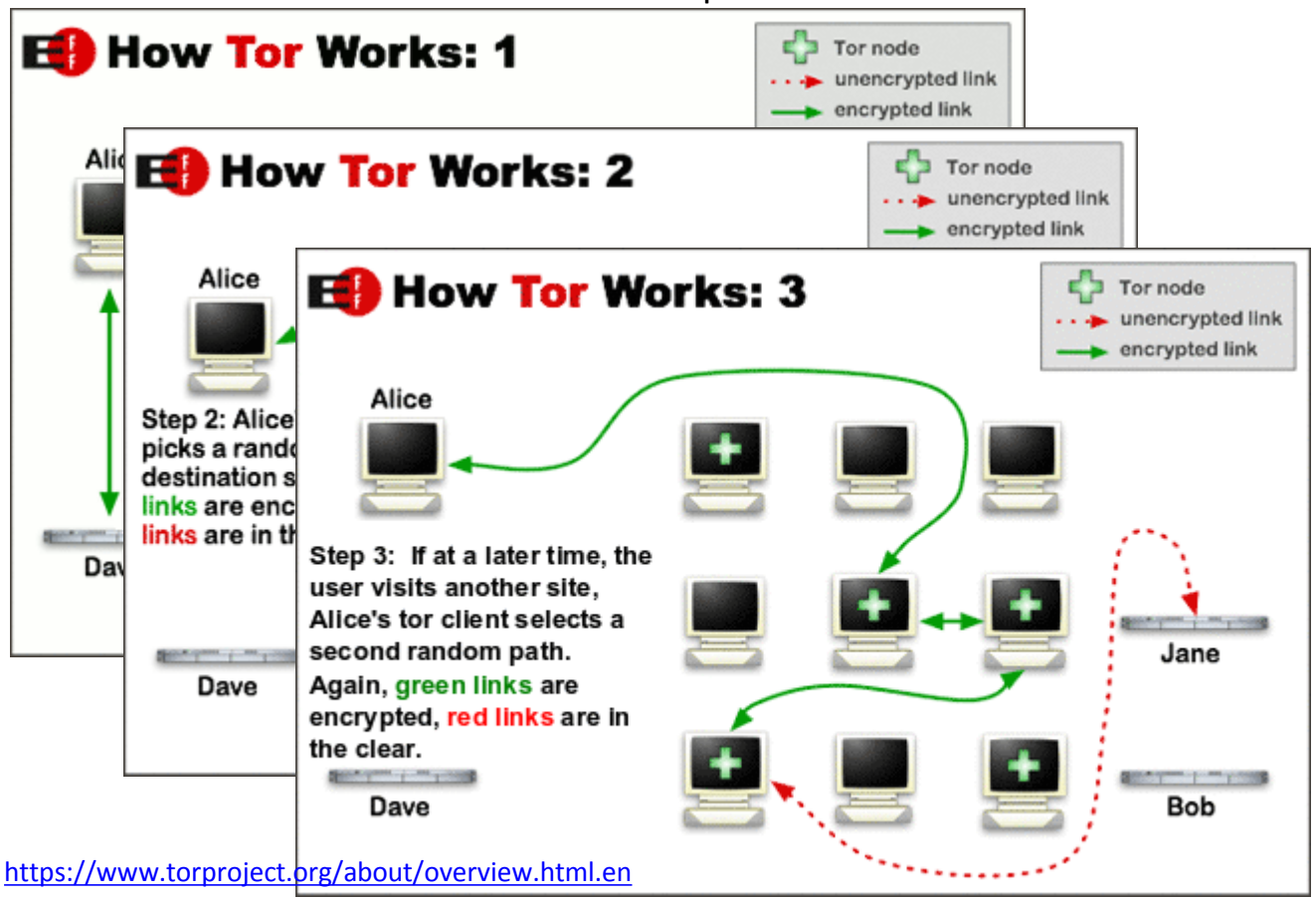
  - The idea comes from **Chaum's Mix-Net design** at first.
    Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms
    (Communications of the ACM February 1981 Volume 24 Number 2)

Implemented Anonymous Network - Tor

- The Tor (the Onion Routing) Concept
  - Open source software
    https://svn.torproject.org/cgi-bin/viewvc.cgi/Tor/
    http://sourceforge.net/projects/advtor/
  - A distributed, anonymous Network
  - A Protocol
  - Tor provides online anonymity

Implemented Anonymous Network - Tor

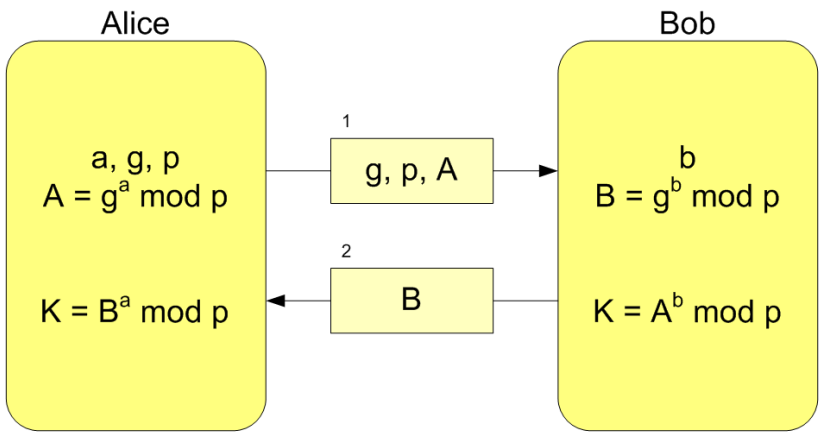
- The Tor (the Onion Routing): How it works
  - Alice's Tor client obtains a list of Tor nodes from a directory server, Dave.
  - Alice's Tor client picks a random destination server.
  - Alice's Tor client selects a second random path.



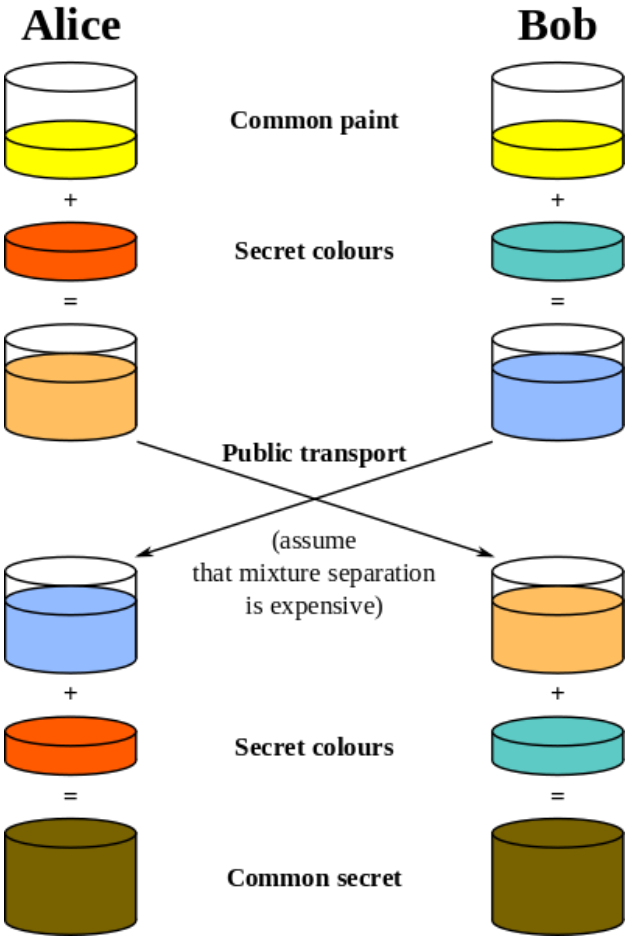
https://www.torproject.org/about/overview.html.en

- The Tor (the Onion Routing): Diffie-Hellman Key Exchange Algorithm in TLS (1/2)

  - ✓ DH establishes a shared secret that can be used for secret communications while exchanging data over a public network
  - ✓ (Step A) Alice and Bob have common information and secrets which belong to one's own.
  - ✓ (Step B) Each creates a value with a secret, and transmit it to the other.
  - ✓ (Step C) Using a value by the other, each creates common secret.



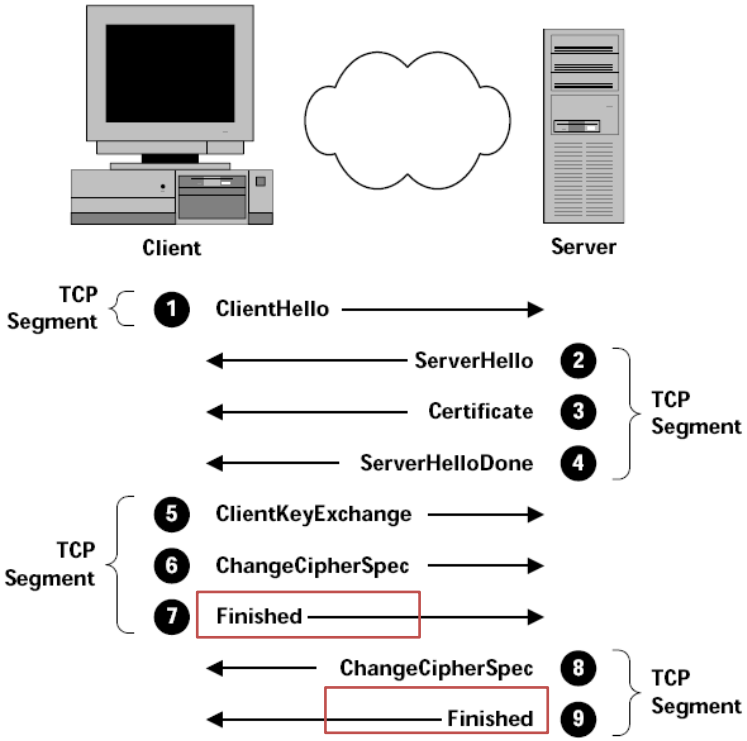
$K = A^b \bmod p = (g^a \bmod p)^b \bmod p = g^{ab} \bmod p = (g^b \bmod p)^a \bmod p = B^a \bmod p$



Implemented Anonymous Network - Tor

- The Tor (the Onion Routing): Diffie-Hellman Key Exchange Algorithm in TLS (2/2)

  - SSL / TLS (Secure Socket Layer / Transport Layer Security)

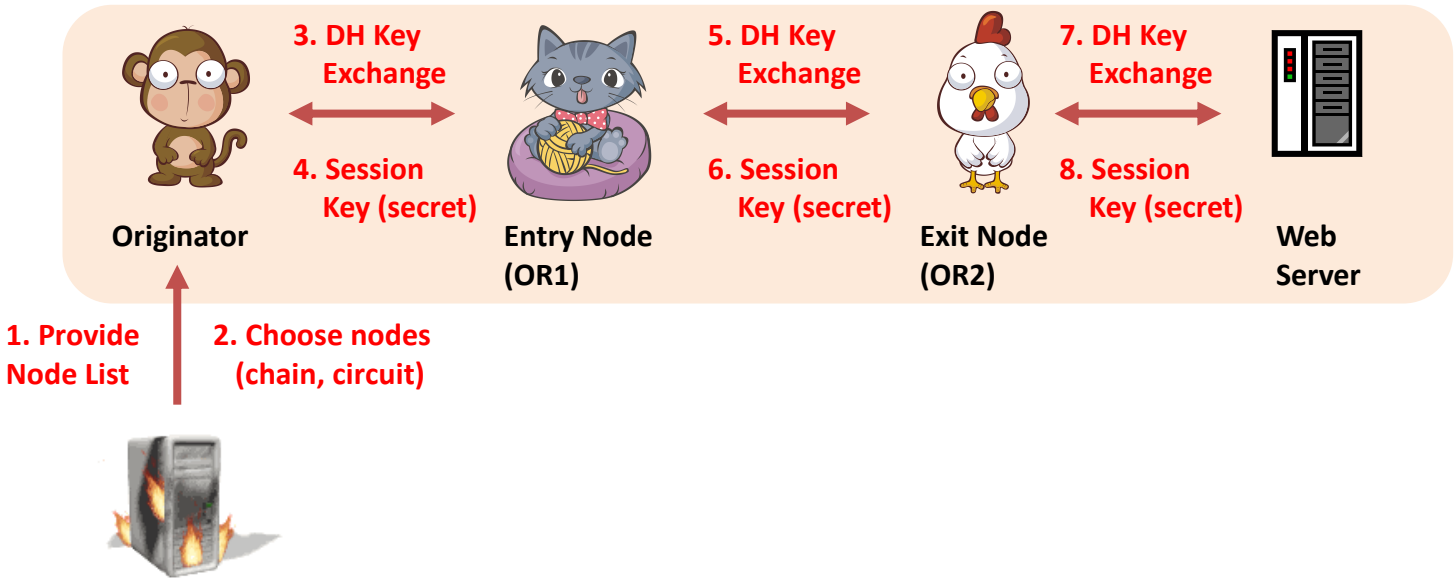


http://en.wikipedia.org/wiki/Secure_Sockets_Layer

Implemented Anonymous Network - Tor

- The Tor (the Onion Routing): Entire Mechanism (1/3)

  - Circuit (Chain) establishment

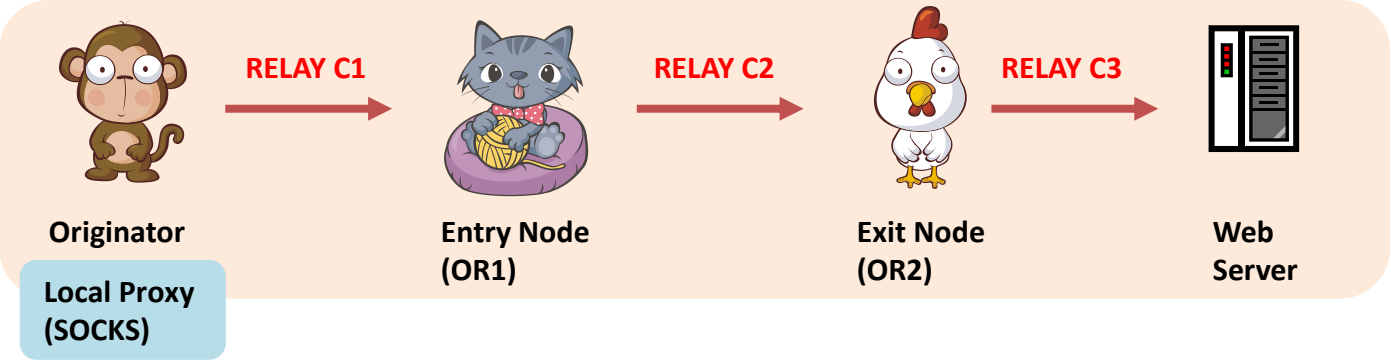


- ✓ All communication between nodes over TLSv1
- ✓ The originator and directory node actually involves with DH over TLS.

Implemented Anonymous Network - Tor

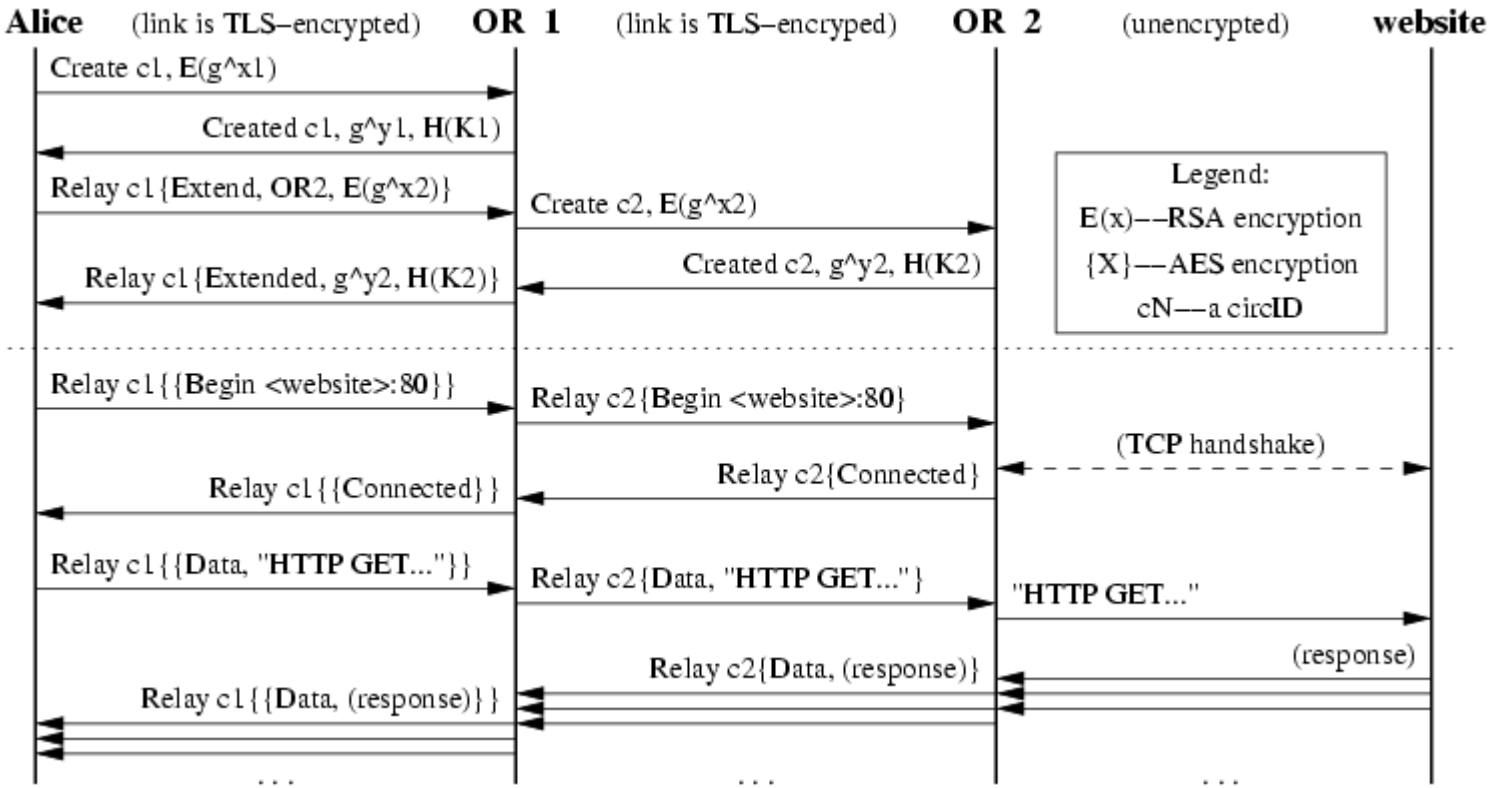
- The Tor (the Onion Routing): Entire Mechanism (2/3)

  - Sending HTTP data over the Internet anonymously



- ✓ C1 = {RELAY C1: [RELAY (Send HTTP request to Web-Server-IP)]}
- ✓ C2 = {RELAY C2: ENCRYPTED CONTENT}
- ✓ C3 = {Send HTTP request to Web-Server-IP}
- ✓ OR1 (Entry Node) knows the origin which the packets come from.
- ✓ OR2 (Exit Node) knows the destination which the incoming packets go to.
- ✓ If any, all OR nodes between entry node and exit node only know the adjacent nodes.

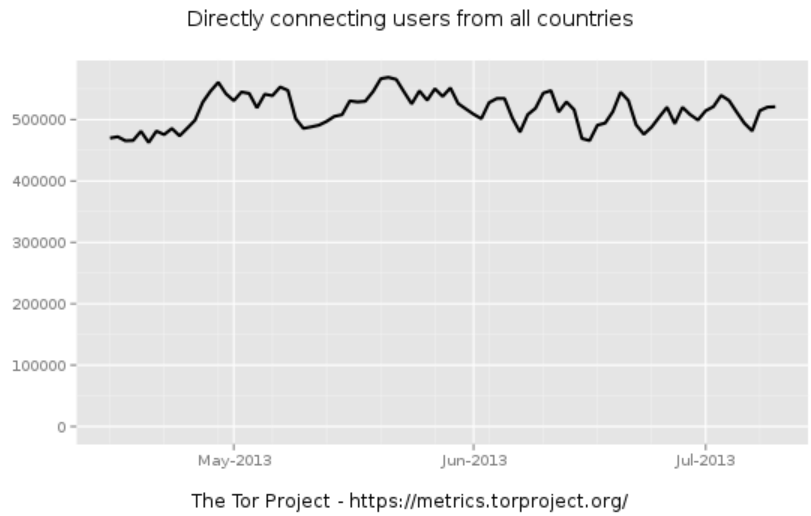
- The Tor (the Onion Routing): Entire Mechanism (3/3)
  - Diagram about tor operation in details



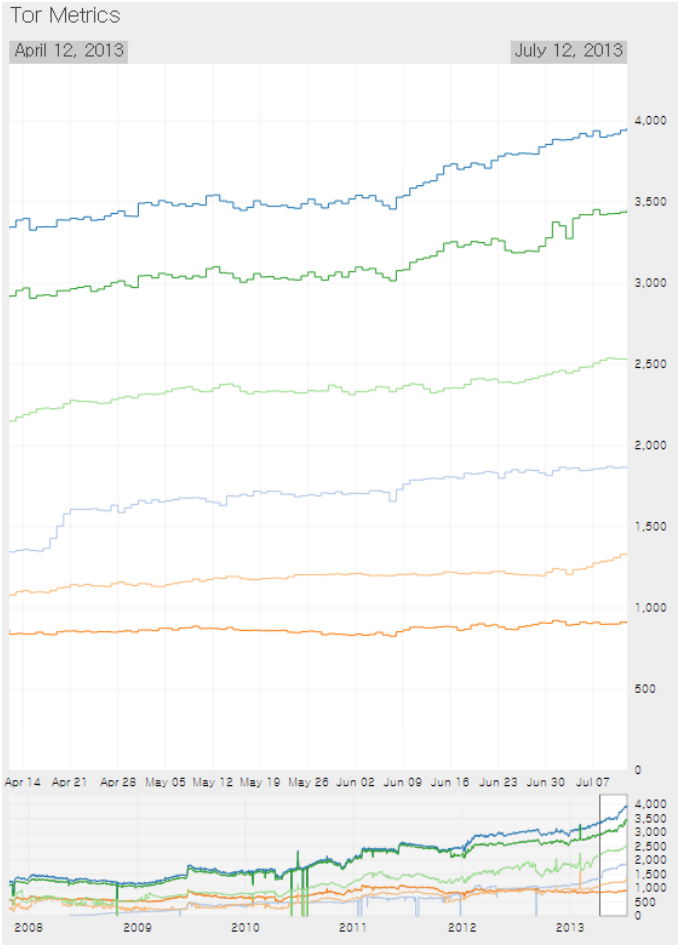
https://svn.torproject.org/svn/projects/design-paper/tor-design.html

Implemented Anonymous Network - Tor

- The Tor (the Onion Routing): Statistics as of July, 2013 (1/2)
  - One of the largest deployed network
  - Almost 4,000 relays
  - Almost 2,000 bridges
  - Around 500,000 users per each day



http://tigerpa.ws/tor_metrics/



Implemented Anonymous Network - Tor

- The Tor (the Onion Routing): Statistics as of July, 2013 (2/2)
  - Some countries(ISPs) have a censorship to prevent users from getting access to certain sites.
  - Bridge Relays (almost 25,000)
    Helps censored users access the Tor network
    Are not listed in the same public directories

Top-10 countries by possible censorship events (BETA):

Start date (yyyy-mm-dd): 2013-01-25 End date (yyyy-mm-dd): 2013-04-25

Update table

Country	Downturns	Upturns
Iran	31	14
Syrian Arab Republic	13	16
China	13	8
United Republic of Tanzania	9	15
India	5	6
Vietnam	4	5
Republic of Korea	3	3
Gibraltar	3	2
Taiwan	3	0
Dominica	2	2

Implemented Anonymous Network - Tor

- The Tor (the Onion Routing): Official Record
  - Tor Relay IP Address in the Past
  - https://metrics.torproject.org/exonerator.html

Was there a Tor relay running on this IP address?

IP address in question: *(Ex.: 86.59.21.38 or 2001:858:2:2:aabb:0:563b:1526)*

Date or timestamp, in UTC: *(Ex.: 2010-01-01 or 2010-01-01 12:00)*

제출 재설정

  - Tor Relay IP Search
  - https://metrics.torproject.org/relay-search.html

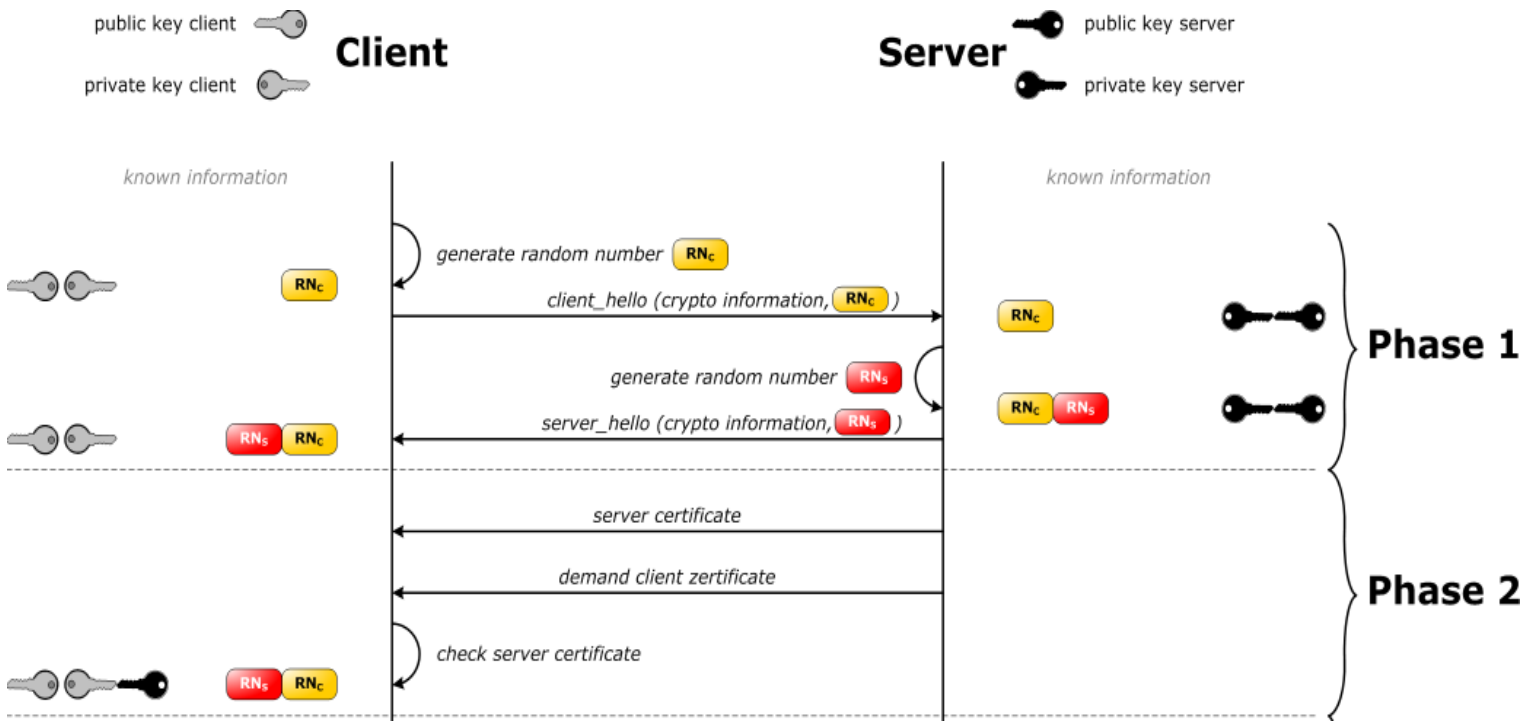
Tor Metrics Portal: Relay Search

Search for a relay in the relay descriptor archive by typing (part of) a **nickname**, **$-prefixed fingerprint**, or **IP address** and optionally a **month (yyyy-mm)** or up to three **days (yyyy-mm-dd)** in the following search field and clicking Search. The search will stop after 30 hits or, unless you provide a month or a day, after parsing the last 30 days of relay lists.

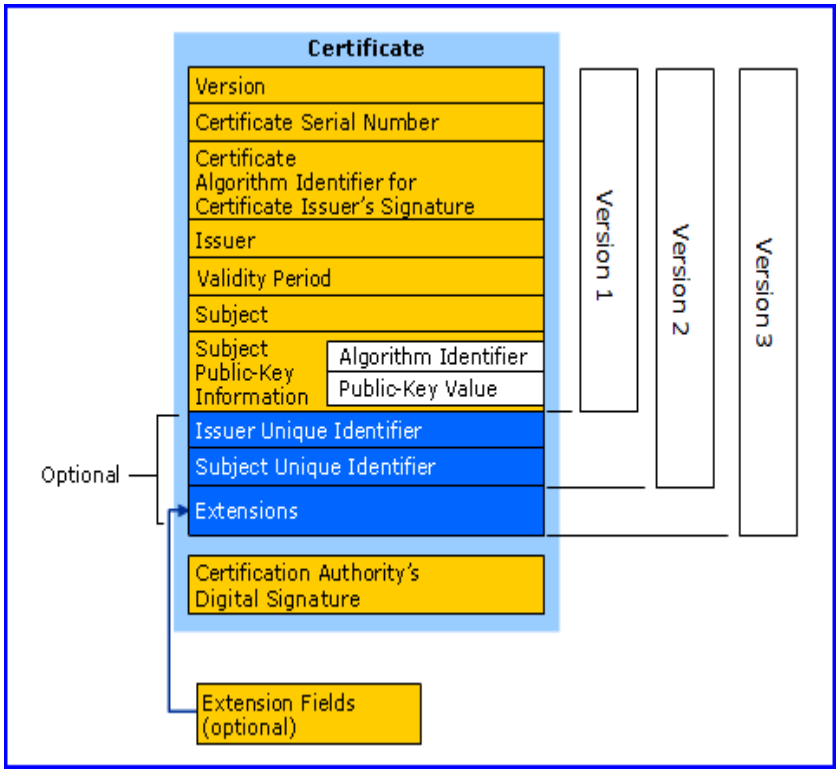
Search

Implemented Anonymous Network - Tor

- The Tor (the Onion Routing): Detection Technique Example (1/2)
  - Someone should talk to directory server (public) to join the tor network.
  - A series of unauthorized certificates in SSL/TLS communication <u>before encryption.</u>
  - Other than IP/Port (Layer 3), all TLS traffic are encrypted.



- The Tor (the Onion Routing): Detection Technique Example (2/2)
  - ❖ X.509 Certificate has an issuer/subject field.
  - ❖ Tor initiates a series of SSL/TLS connections with 3~5 hosts at the same time.
    → This requires behavior-based analysis if bridges are used for censorship bypass.

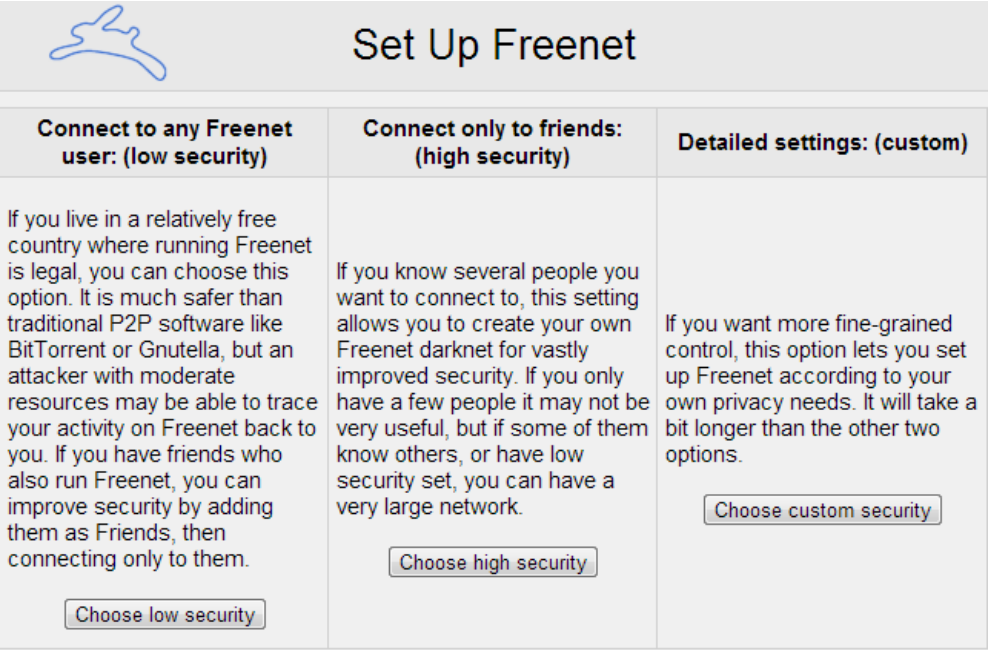



```
Certificate:
    Data:
        Version: 1 (0x0)
        Serial Number: 7829 (0x1e95)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
                OU=Certification Services Division,
                CN=Thawte Server CA/emailAddress=server-certs@thawte.com
        Validity
            Not Before: Jul  9 16:04:02 1998 GMT
            Not After : Jul  9 16:04:02 1999 GMT
        Subject: C=US, ST=Maryland, L=Pasadena, O=Brent Baccala,
                 OU=FreeSoft, CN=www.freesoft.org/emailAddress=baccala@freesoft.org
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:b4:31:98:0a:c4:bc:62:c1:88:aa:dc:b0:c8:bb:
                    33:35:19:d5:0c:64:b9:3d:41:b2:96:fc:f3:31:e1:
                    66:36:d0:8e:56:12:44:ba:75:eb:e8:1c:9c:5b:66:
                    70:33:52:14:c9:ec:4f:91:51:70:39:de:53:85:17:
                    16:94:6e:ee:f4:d5:6f:d5:ca:b3:47:5e:1b:0c:7b:
                    c5:cc:2b:6b:c1:90:c3:16:31:0d:bf:7a:c7:47:77:
                    8f:a0:21:c7:4c:d0:16:65:00:c1:0f:d7:b8:80:e3:
                    d2:75:6b:c1:ea:9e:5c:5c:ea:7d:c1:a1:10:bc:b8:
                    e8:35:1c:9e:27:52:7e:41:8f
                Exponent: 65537 (0x10001)
    Signature Algorithm: md5WithRSAEncryption
        93:5f:8f:5f:c5:af:bf:0a:ab:a5:6d:fb:24:5f:b6:59:5d:9d:
        92:2e:4a:1b:8b:ac:7d:99:17:5d:cd:19:f6:ad:ef:63:2f:92:
        ab:2f:4b:cf:0a:13:90:ee:2c:0e:43:03:be:f6:ea:8e:9c:67:
        d0:a2:40:03:f7:ef:6a:15:09:79:a9:46:ed:b7:16:1b:41:72:
        0d:19:aa:ad:dd:9a:df:ab:97:50:65:f5:5e:85:a6:ef:19:d1:
        5a:de:9d:ea:63:cd:cb:cc:6d:5d:01:85:b5:6d:c8:f3:d9:f7:
        8f:0e:fc:ba:1f:34:e9:96:6e:6c:cf:f2:ef:9b:bf:de:b5:22:
        68:9f
```

http://en.wikipedia.org/wiki/X.509
http://helpforsure.wordpress.com/tag/x-509-version-3-digital-certificates/

Implemented Anonymous Network - *Freenet*

- What is *Freenet*?
  - A separate network that runs over the internet
  - Only access *Freenet* content through *Freenet* including:
    Freesites (websites on *Freenet*),
    in-Freenet chat forums (FMS, Sone, etc),
    files shared within *Freenet*,
    in-Freenet email
  - Distributed Database
  - The more popular a file or page, the more widely it will be cached, the faster it will download.



Set Up Freenet

Connect to any Freenet user: (low security)	Connect only to friends: (high security)	Detailed settings: (custom)
If you live in a relatively free country where running Freenet is legal, you can choose this option. It is much safer than traditional P2P software like BitTorrent or Gnutella, but an attacker with moderate resources may be able to trace your activity on Freenet back to you. If you have friends who also run Freenet, you can improve security by adding them as Friends, then connecting only to them. Choose low security	If you know several people you want to connect to, this setting allows you to create your own Freenet darknet for vastly improved security. If you only have a few people it may not be very useful, but if some of them know others, or have low security set, you can have a very large network. Choose high security	If you want more fine-grained control, this option lets you set up Freenet according to your own privacy needs. It will take a bit longer than the other two options. Choose custom security

https://freenetproject.org/faq.html

Implemented Anonymous Network - *Freenet*

- Properties

  - A large distributed storage device
  - When storing a file, you receive a key to retrieve the file.
  - With a key, *Freenet* returns the appropriate file.

  - Data Management
    Location to store data: *C:\Users\[UserID]\AppData\Local\Freenet\datastore*
    Little or no control over what is stored in your datastore
    Kept or deleted depending on how popular they are.

  - Routing
    Initially, each node has no information about the performance of the other nodes. (Random Routing)
    More documents → same node; begin to cluster with data items (Cuz the same routing rules are used)
    As a result, the network will self-organize into a distributed, clustered structure.

Implemented Anonymous Network - *Freenet*

- Properties

  - Keys
    Each file that exists on Freenet has a key associated with it.
    Fproxy → *http://localhost:8888/[Freenet Key]*

  - CHK - Content Hash Keys
    The decryption key is stored encrypted within the file.

CHK	@	file hash	,	decryption key	,	crypto settings

  - SSK - Signed Subspace Keys
    Usually for sites that are going to change over time

SSK	@	public key hash	,	decryption key	,	crypto settings	/	user selected name	-	version

  - USK - Updateable Subspace Keys
    Linking to the latest version of a Signed Subspace Key (SSK) site

USK	@	public key hash	,	decryption key	,	crypto settings	/	user selected name	-	version

  - KSK - Keyword Signed Keys
    Allowing to save named pages in Freenet

KSK	@	myfile.txt

Implemented Anonymous Network - *Gnunet*

- What is *Gnunet*?

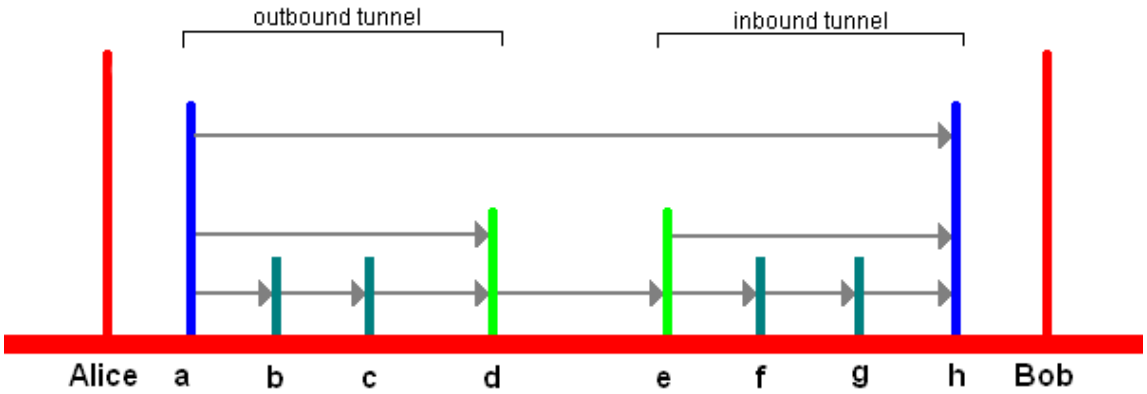
  - Started in late 2001
  - Implemented for secure peer-to-peer networking
  - Improved content encoding: **ECRS, the encoding for censorship resistant sharing**

  - A framework for secure peer-to-peer networking that does not use any centralized
  - Focus on anonymous censorship-resistant file-sharing
  - Provides anonymity by
    . making messages originating from a peer indistinguishable from messages that the peer is routing
    . acting as routers and use link-encrypted connections with stable bandwidth utilization
  - Similar to tor, but limited to share files anonymously, searching, swarming, and caching.

http://en.wikipedia.org/wiki/GNUnet
https://gnunet.org/

Implemented Anonymous Network – *I2P*

- What is *I2P*? (1/2)
  - Began in 2003
  - An anonymizing network, a low latency mix network
  - Goal:
    producing a low latency, fully distributed, autonomous,
    scalable, anonymous, resilient, and secure network
  - All data is wrapped with several layers of encryption. (End-to-End)
  - The network is both distributed and dynamic, with no trusted parties and no centralized resources.

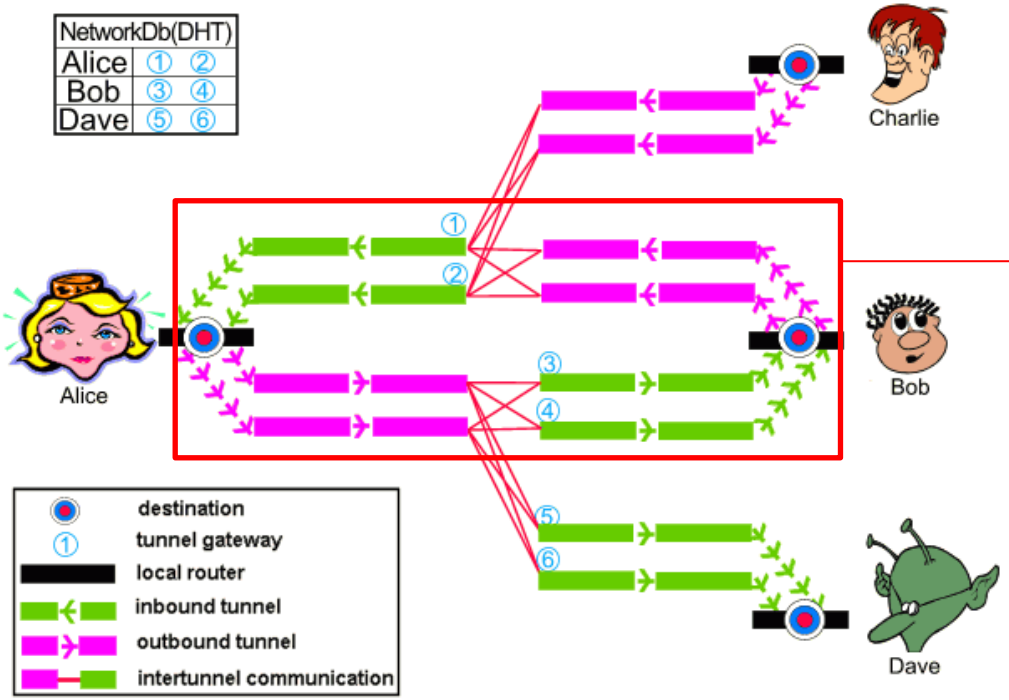


		tunnel encryption (private key AES)	a to d, e to h
garlic encryption (ElGamal/SessionTag+AES)	a to h	transport encryption (DH/STS+AES, etc)	a to b, b to c, c to d, d to e, e to f, f to g, g to h

http://www.i2p2.de/

Implemented Anonymous Network – *I2P*

- What is *I2P*? (2/2)
  - Made up of a set of nodes ("routers") with a number of unidirectional inbound and outbound virtual paths (“tunnels”)
  - Has its own internal network database (using a modification of the *Kademlia* algorithm) for distributing routing and contact information securely



http://www.i2p2.de/how_intro

Garlic Wrapped:
(Garlic Routing)
1. Layered Encryption
2. Bundling multiple messages together
3. ElGamal/AES Encryption

Peer Profiling (Peer Collection)
Peer Selection (Peer Choosing)

Circumvention Techniques against Censorships

(1) DPI (Deep Packet Inspection)

(2) Obfsproxy

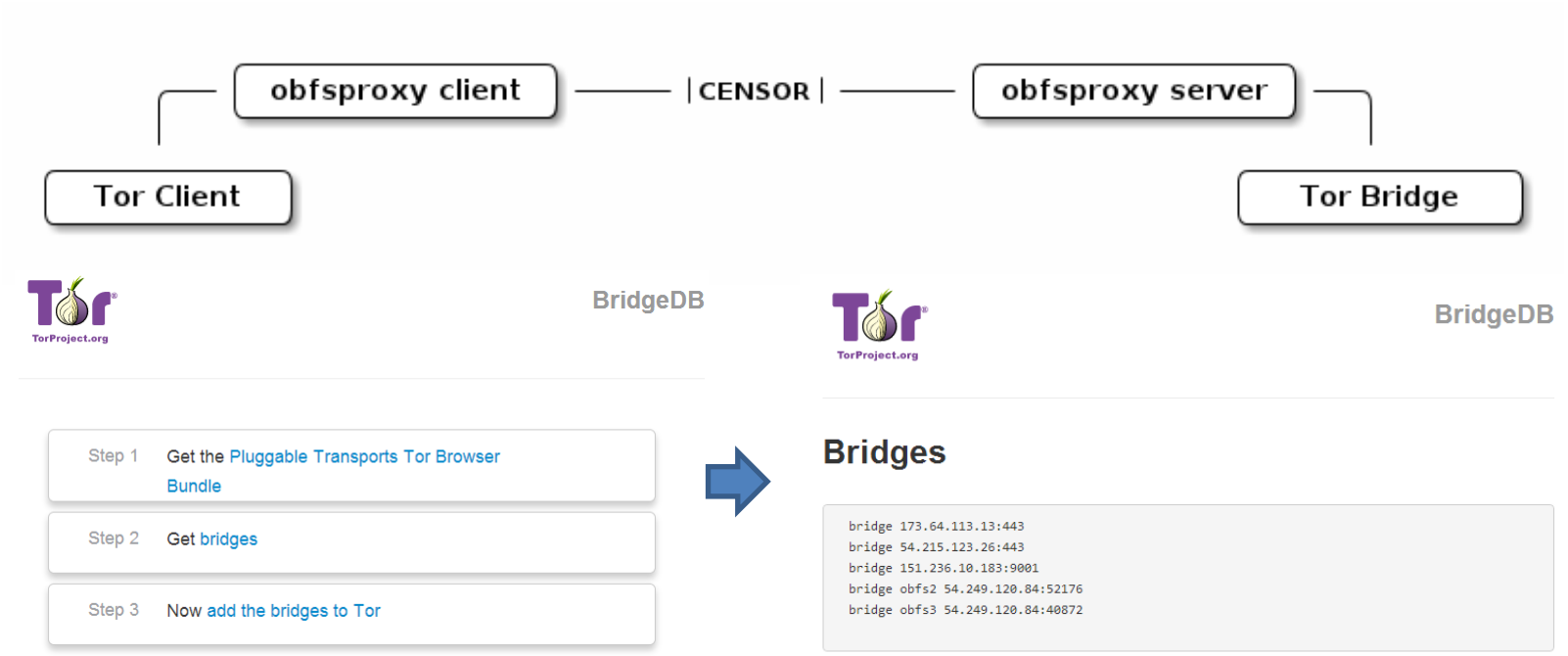
(3) Flashproxy

Circumvention Techniques against Censorships

- How to circumvent censorships by DPI (deep packet inspections)
  - Even bridges could be blocked by DPI.
  - New techniques have been introduced to circumvent such censorships.
  - Core technology: **pluggable transport transformation**
    - ✓ **Obfsproxy** is a Python framework for implementing new pluggable transports. It uses Twisted for its networking needs, and pyptlib for some pluggable transport-related features. It supports the obfs2 and obfs3 pluggable transports. (by George Kadianakis)
    - ✓ **Flashproxy** turns ordinary web browsers into bridges using websockets, and has a little python stub to hook Tor clients to the websocket connection. (by David Fifield)
    - ✓ **ScrambleSuit** is a pluggable transport that protects against follow-up probing attacks and is also capable of changing its network fingerprint (packet length distribution, inter-arrival times, etc.). It's part of the Obfsproxy framework. (by Philipp Winter)
    - ✓ **StegoTorus** is an Obfsproxy fork that extends it to a) split Tor streams across multiple connections to avoid packet size signatures, and b) embed the traffic flows in traces that look like html, javascript, or pdf. (by Zack Weinberg)
    - ✓ **SkypeMorph** transforms Tor traffic flows so they look like Skype Video. (by Ian Goldberg)
    - ✓ **Dust** aims to provide a packet-based (rather than connection-based) DPI-resistant protocol. (by Brandon Wiley)

https://www.torproject.org/docs/pluggable-transports.html.en

- How to circumvent censorships by DPI - ***Obfsproxy***
  - Transforms the Tor traffic between the client and the bridge.
  - Supports multiple protocols, **pluggable transports**.
  - Get bridges in Bridge DB and then add them to tor



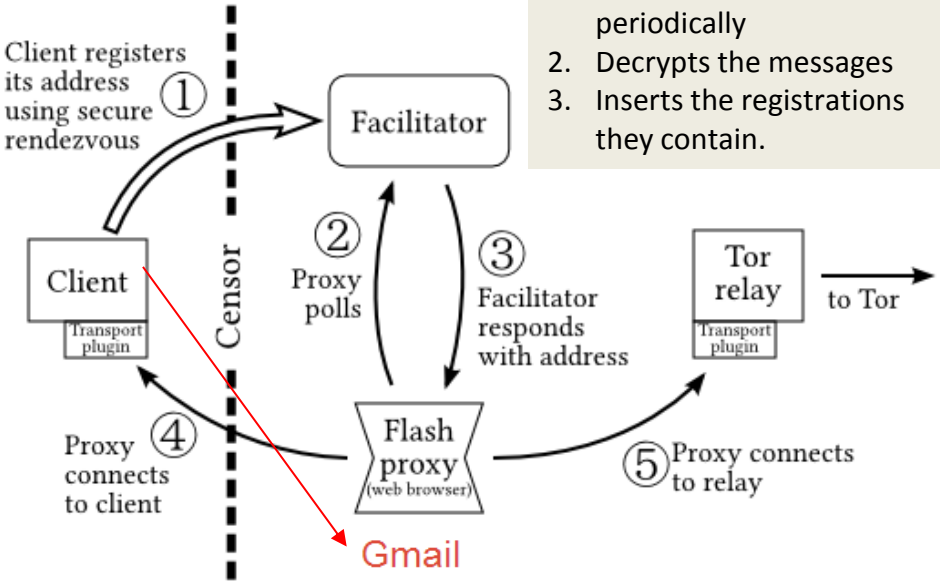
https://www.torproject.org/projects/obfsproxy.html.en
https://bridges.torproject.org/?transport=obfs2

- How to circumvent censorships by DPI - ***flashproxy***

  - Began as a project in Stanford's class in spring 2011
  - Works at tor version 0.2.3.2-alpha or later
  - This model have supposed that facilitator outside have been already blocked.
    : Client does not communicate directly to facilitator, designed to be covert and very hard to block.

1. Checks this mailbox periodically
2. Decrypts the messages
3. Inserts the registrations they contain.

1. Makes TLS Connection
2. Sends encrypted email from anonymous address to a special facilitator addr.



https://crypto.stanford.edu/flashproxy/
https://crypto.stanford.edu/flashproxy/flashproxy.pdf

Question and Answer