BTI 4202: Anonymity

Christian Grothoff

Berner Fachhochschule

21.5.2021

Learning Objectives

Part IV: Introduction to p≡p

Guest Speaker: Hernani Marques

- Executive Director of the p≡p foundation
- Speaker of CCC Switzerland
- Practices his own brand of applied ethics (aka non-parliamentary law-making):
  - Bundes-Ref. Biometrische Pässe
  - Kant. VI Bildungsinitiative Zürich (Abschaffung Schulgelder)
  - Bundes-Ref. Überwachungsgesetz BÜPF
  - Bundes-Ref. Geheimdienstgesetz NDG
  - Bundes-Ref. Geldspielgesetz
  - Bundes-VI E-Voting-Moratorium (vorzeitig abgebrochen)
  - Bundes-Ref. Versicherungsspione
  - Bundes-Ref. E-ID (**erfolgreich**)
  - Bundes-Ref. Polizeimassnahmengesetz PMT (13.6.2021)

Please join Big Blue Button

https://meet.pep.security/b/chr-8ym-6a5-zim

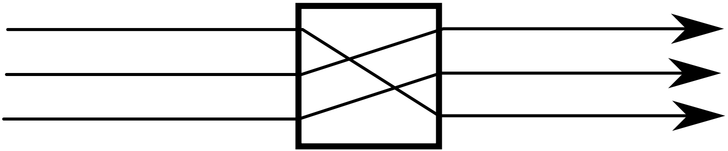
Part II: Anonymizing Systems

Anonymity: Dining Cryptographers

"Three cryptographers are sitting down to dinner. The waiter informs them that the bill will be paid anonymously. One of the cryptographers maybe paying for dinner, or it might be the NSA. The three cryptographers respect each other's right to make an anonymous payment, but they wonder if the NSA is paying." – David Chaum

Mixing

David Chaum's mix (1981) and cascades of mixes are the traditional basis for destroying linkability:

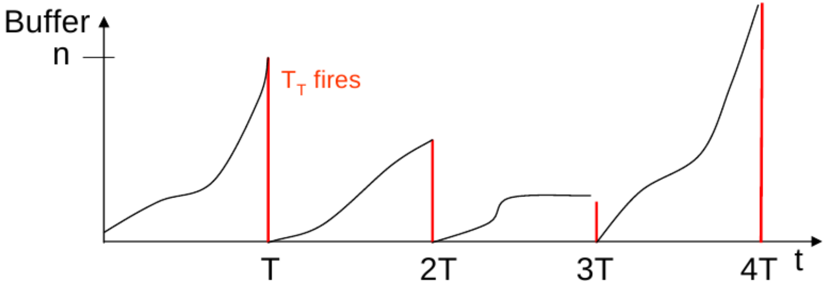


Mixing

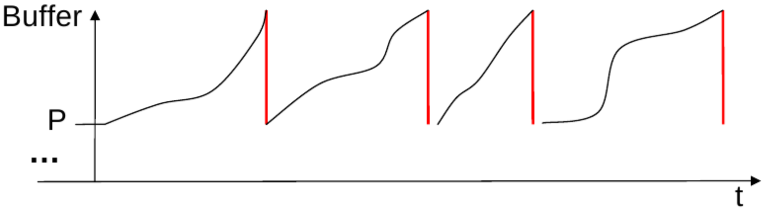
David Chaum's mix (1981) and cascades of mixes are the traditional basis for destroying linkability:

Threshold Mix

Timed Mix



Pool mix



Mixminion

G. Danezis, R. Dingledine, D. Hopwood and N. Mathewson describe Mixminion [1]:

- based on mixmailers (only application is E-mail)
- possibility to reply
- directory servers to evaluate participating remailers (reputation system)
- exit policies

Mixminion: key ideas

When a message traverses mixminion, each node must decrypt the message using its (ephemeral) private key.

The key idea behind the replies is splitting the path into two legs:

- the first half is chosen by the responder to hide the responder identity
- the second half was communicated by the receiver to hide the receiver identity
- a crossover-node in the middle is used to switch the headers specifying the path

Mixminion: replay?

Replay attacks were an issue in previous mixnet implementations.

- Mixes are vulnerable to replay attacks
- Mixminion: servers keep hash of previously processed messages until the server key is rotated

$\Rightarrow$ Bounded amount of state in the server, no possibility for replay attack due to key rotation

Mixminion: Directory Servers

- Inform users about servers
- Probe servers for reliability
- Allow a partitioning attack unless the user always queries all directory servers for everything

Mixminion: Nymservers

- Nymservers keep list of use-once reply blocks for a user
- Vulnerable to DoS attacks (deplete reply blocks)
- Nymservers could also store mail (use one reply block for many messages).

Mixminion: obvious problems

- no benefits for running a mixmailer for the operator
- quite a bit of public key cryptography
- trustworthiness of directory servers questionable
- servers must keep significant (but bounded) amount of state
- limited to E-mail (high latency)

Mixminion: open problems

- exit nodes are fair game for legal actions
- no accounting to defend against abuse / DoS attacks
- statistical correlation of entities communicating over time possible (observe participation)

$\Rightarrow$ bridging between an anonymous network and a traditional protocol is difficult

Break

Part III: Tor

Tor

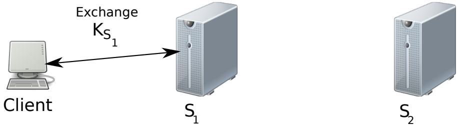
- Tor is a P2P network of **low-latency** mixes which are used to provide anonymous communication between parties on the Internet.
- Tor works for any TCP-based protocol
- TCP traffic enters the Tor network via a SOCKS proxy
- **Common usage:** client anonymity for web browsing

Onion Routing

- Multiple mix servers
- Path of mix servers chosen by initiator
- Chosen mix servers create "circuit"
  - Initiator contacts first server S_1, sets up symmetric key K_{S_1}
  - Then asks first server to connect to second server S_2; through this connection sets up symmetric key with second server K_{S_2}
  - ...
  - Repeat with server S_i until circuit of desired length n constructed

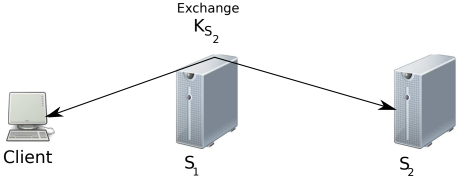
Onion Routing Example

- Client sets up symmetric key K_{S_1} with server S_1



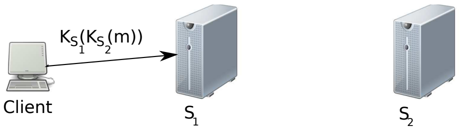
Onion Routing Example

- Via S_1 Client sets up symmetric key K_{S_2} with server S_2



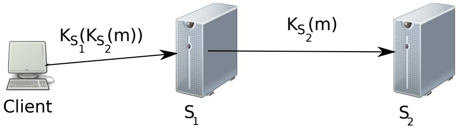
Onion Routing Example

- Client encrypts m as $K_{S_1}(K_{S_2}(m))$ and sends to S_1



Onion Routing Example

- S_1 decrypts, sends on to S_2, S_2 decrypts, revealing m

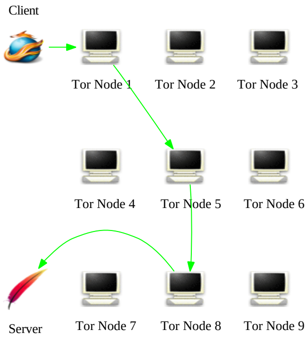


Tor - How it Works

- Low latency P2P Network of mix servers
- Designed for interactive traffic (https, ssh, etc.)
- "Directory Servers" store list of participating servers
  - Contact information, public keys, statistics
  - Directory servers are replicated for security
- Clients choose servers randomly with bias towards high BW/uptime
- Clients build long lived Onion routes "circuits" using these servers
- Circuits are bi-directional
- Circuits are of length three

Tor - How it Works - Example

- Example of Tor client circuit



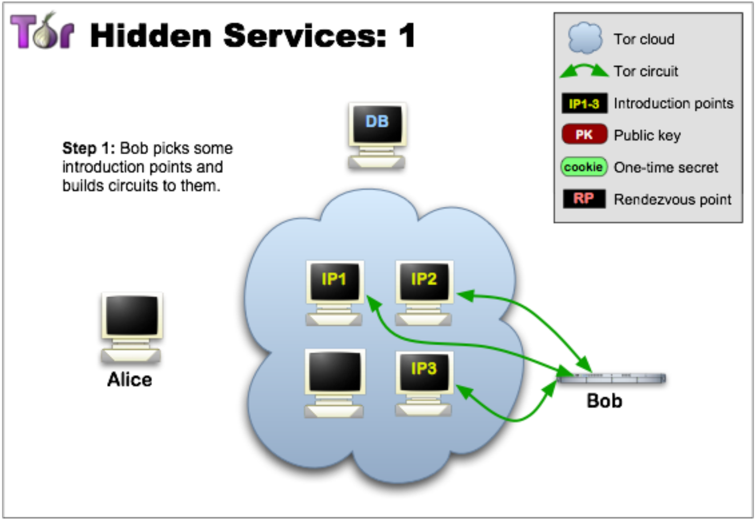
Tor - How it Works - Servers

- Servers are classified into three categories for usability, security and operator preference
- Entry nodes (aka guards) - chosen for first hop in circuit
  - Generally long lived "good" nodes
  - Small set chosen by client which are used for client lifetime (security)
- Middle nodes - chosen for second hop in circuit, least restricted set
- Exit nodes - last hop in circuit
  - Visible to outside destination
  - Support filtering of outgoing traffic
  - Most vulerable position of nodes

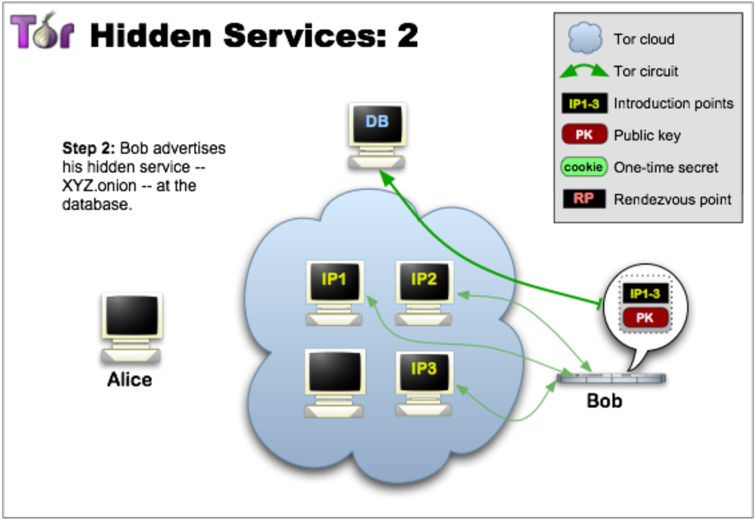
Hidden Services in Tor

- Hidden services allow Tor servers to receive incoming connections anonymously
- Can provide access to services available *only* via Tor
  - Web, IRC, etc.
  - For example, host a website without your ISP knowing

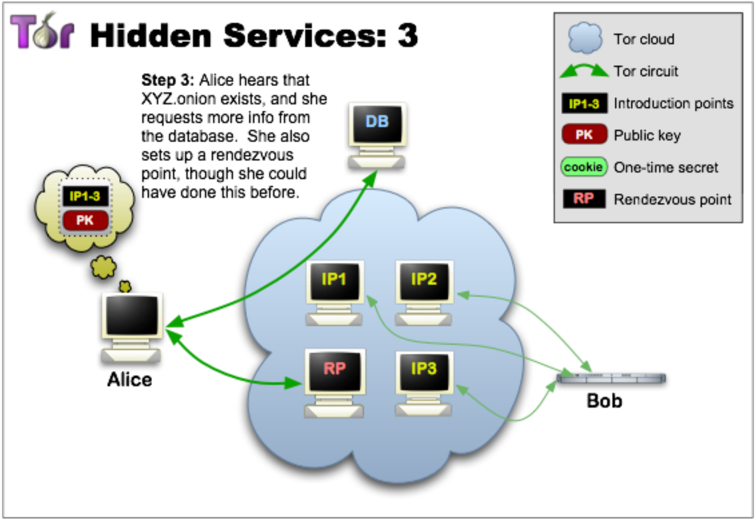
Hidden Services Example 1



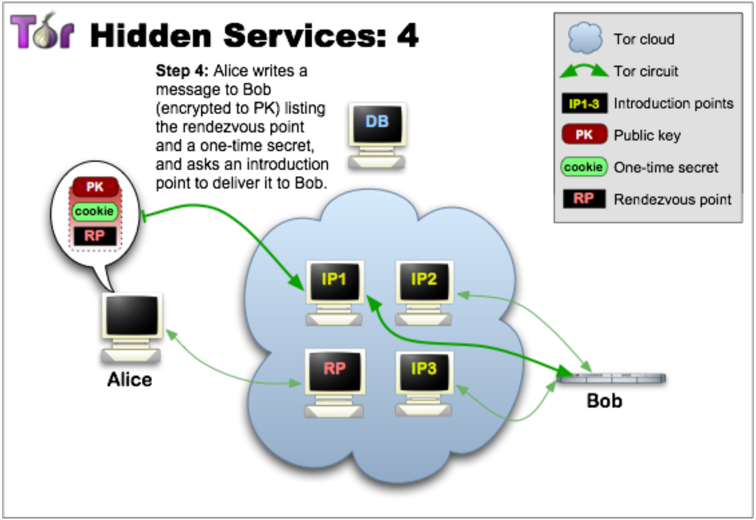
Hidden Services Example 2



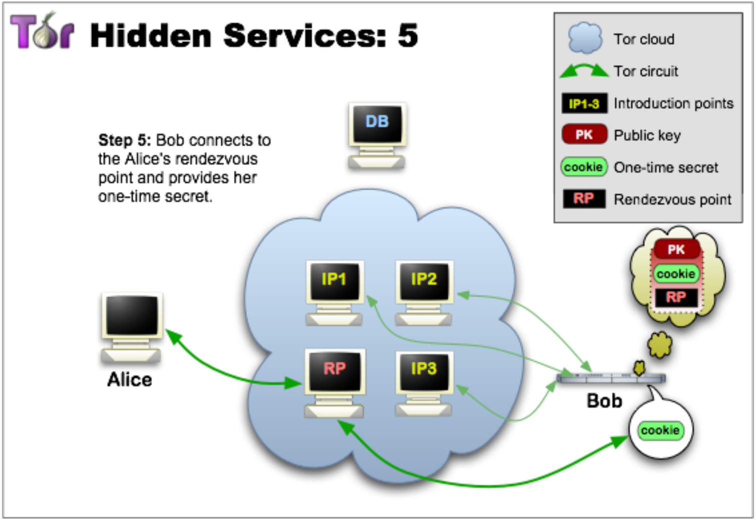
Hidden Services Example 3



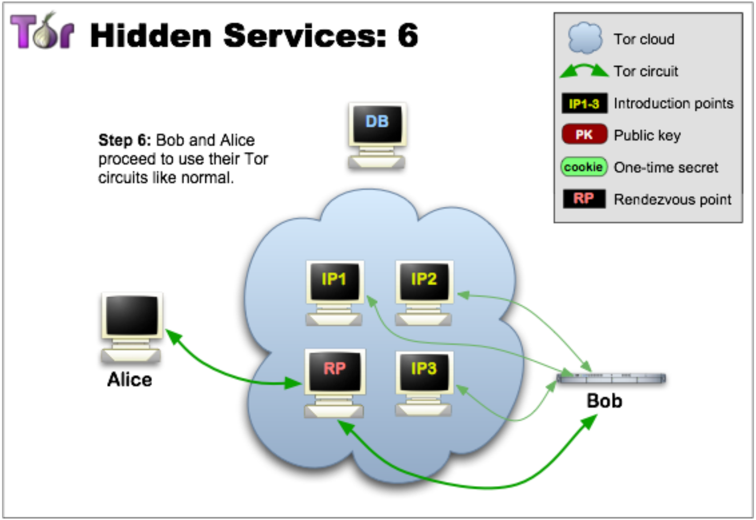
Hidden Services Example 4



Hidden Services Example 5



Hidden Services Example 6



Types of Attacks on Tor

- Exit Relay Snooping
- Website fingerprinting
- Traffic Analysis
- Intersection Attack
- DoS

Exercise

- Install Tor
- Configure Tor relay
- Setup hidden service
- Perform risk analysis for deanonymization

References

George Danezis, Roger Dingledine, and Nick Mathewson.
Mixminion: Design of a type iii anonymous remailer protocol.
In *Proceedings of the 2003 IEEE Symposium on Security and Privacy*, SP '03, 2003.

Brad Miller, Ling Huang, A.D. Joseph, and J.D. Tygar.
I know why you went to the clinic: Risks and realization of https traffic analysis.
http://arxiv.org/abs/1403.0297, 2014.