Chair for Network Architectures and Services
Department of Informatics
TU München – Prof. Carle

Peer-to-Peer Systems and Security

Chapter 3
3.3 Anonymity Systems

Dipl.-Inform. Heiko Niedermayer
Prof. Dr. Georg Carle

Vorlesung SS 2009

Overview

- Motivation
- Systems
  - Jondos (früher JAP) – mix cascade
  - Tor – onion routing network
- Conclusion

Motivation

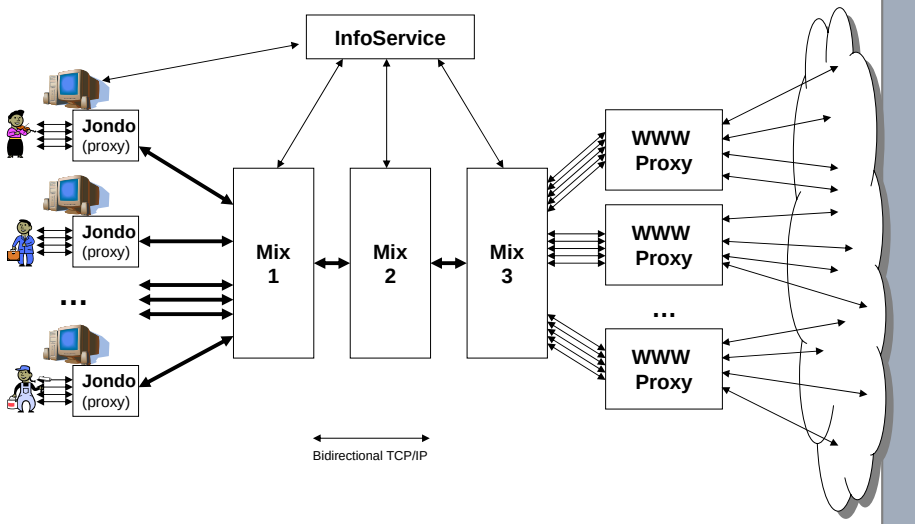
- … and what do the real systems do? …. a short introduction…

Jondonym

Jondonym (jondos.de)

- Until 2006 Java Anon Proxy (anon.inf.tu-dresden.de)
  - By Pfitzmann et. al, 2000.
- Jondonym provides sender anonymity for web surfing.
  - Support for cooperation with law enforcement and authorities (log when requested by court-order, e.g. all to one „bad“ site)
- Concept: Infrastructure with mix cascades
- Components
  - User: Jondo client software (→ Proxy)
  - Jondonym provider:
    - Mixes for the cascades
    - Info service to provide information about mixes and usage (→ size of anonymity set)
    - Web caches as exit points

Jondonym – Architecture (slide based on JAP)



Jondonym

Technology

- Chaumian mix with symmetric encryption channels
  - Two end-points communicate via mix channel.
  - A mix channel is a reliable connection-oriented fullduplex transport service.
  - Connection establishment
    - Initiated by sender by sending a packet which uses public key and symmetric cryptography.
  - Data transport and connection tear down
    - Sender and receiver send data packets using symmetric encryption.

Security

- Each mix owns a long-lived DSA signature key to prove its identiy.
- Layered encryption with AES-128 with replay protection.
- Trust bound to few mix providers, no real international diversity.

Jondonym design

- Developpers emphasize usablity.
  - Easy-to-use and good performance.
- Mix cascades profit from capacity effects.
  - As long as mix can handle the traffic, more traffic improves performance and anonymity.

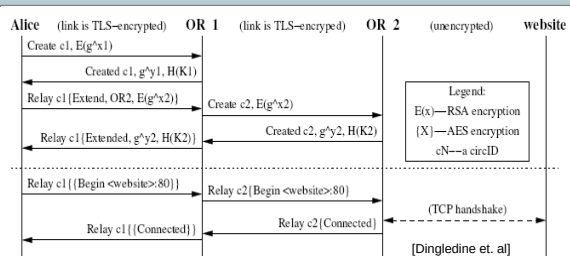
Tor

Tor (The second generation Onion Router)

tor.eff.org

- Mix network
  - Based on Onion Routing.
  - No mixing, but round robin flow processing at re-routers.
  - Uses SSL/TLS connections.
  - Circuit = fixed route selected by sender.
- Infrastructure approach
  - Distributed, by volunteers, over 1700 Tor re-routers all over the world, most in USA and Germany.
- Protocol Cleaning
  - Not part of Tor, Tor comes with Privoxy, a privacy enhancing local proxy.
- Servers
  - Currently 8 authority servers (3 at US universities, 2 in Germany and Netherlands, 1 in Austria).
  - Many re-routers work as directory servers.
  - Guard servers to protect first hop (a reply to recent attacks).

Tor – Circuits



[Dingledine et. al]

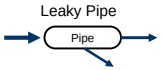
Telescoping circuits

- Initiator negotiates symmetric session keys with each hop.
  - Uses public key of node and Diffie-Hellman exchange.
  - Information obtained from a service directory.
- Client can signal each hop to either relay the packet, create, or extend a circuit.
  - Telescoping = client can signal the last hop anytime to extend or cut the circuit
- Congestion control via end-to-end ACKs along the circuits.

Tor – Security

Some security aspects

- Forward Secrecy
  - Forward Secrecy = breaking the longterm key for a node does not enable the attacker to read recorded communication with the node.
  - Achieved through Diffie-Hellman exchange and short-lived session keys.
- Several TCP streams share a circuit
  - Good for efficiency and anonymity.
- Leaky pipe topology
  - Using inband signalling the traffic can exit the network also in the middle of a circuit (against pattern and traffic volume attacks)
- Distributed authority and directory server concept good for trust.
- Self-protection of routers
  - Exit routers and intermediate routers.
  - Exit routers specify exit policies using IP and port range.



Tor - Hidden Services

Hidden Services

(0.)

- Bob creates Public/Private Key-Pair for his hidden service.
- Bob selects a set of Introduction Points (IP) and signs this information and send it to the Service-Directory
- Bob builds circuits to the Introduction Points and tells them to wait for traffic.

(1.)

- Alice knows Bob's hidden service (out-of-band). She asks the Service Directory (SD) for a set of Introduction Points.

(2.)

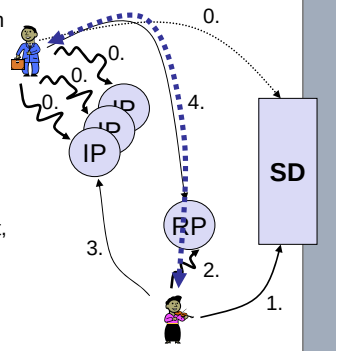
- Alice selects a Rendezvous-Point (RP) and tells them a specific RP-Cookie for the connection to Bob.

(3.)

- Alice opens circuit to an IP of Bob with the service request, her RP, the RP-Cookie and a Diffie-Hellman number.

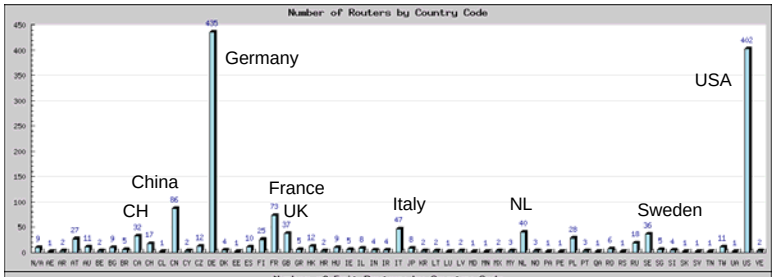
(4.)

- Bob builds a circuit to the RP using the RP-Cookie, his Diffie-Hellman number and a hash of the session key.
- RP interconnects the circuits of Alice and Bob.
- Alice sends a relay begin message to Bob and now the applications are connected.



Tor nodes - Geographic Diversity

Routers



Exit Routers

[torstatus.kgprog.com, 2007]

Conclusion

Conclusion

- Mix cascade: JAP
- Mix network (not mixing!) / Onion Routing network: Tor