Anonymous IP-Services via Overlay Routing

Simon Rieche, Olaf Landsiedel, Heiko Niedermayer,
Klaus Wehrle, Georg Carle

Protocol Engineering and Distributed Systems
University of Tübingen
http://ps.ri.uni-tuebingen.de
Outline

- Motivation
- Related work
- Goals
- Anonymous communication
  - Path concatenation scheme
  - Service Directory
  - Name Service
  - Transparent Application Support
- Security analysis
- Example: anonymous web-browsing
- Conclusion
Motivation

Every man should know that his conversations, his correspondence, and his personal life are private.

Lyndon B. Johnson
President of the United States
1963 – 69

Today: Communication in the Internet is not private

Access and provide information without the threat of personal consequences

Need for anonymous communication schemes providing sender and receiver anonymity

SARA: Sender And Receiver Anonymity
# Related Work

<table>
<thead>
<tr>
<th></th>
<th>Web Mixes</th>
<th>Tor</th>
<th>Crowds</th>
<th>Tarzan</th>
<th>APFS</th>
<th>SARA</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Relay</strong></td>
<td>Server</td>
<td>Server</td>
<td>P2P</td>
<td>P2P</td>
<td>P2P</td>
<td>P2P</td>
</tr>
<tr>
<td><strong>Anonymity</strong></td>
<td>Sender</td>
<td>Sender, Receiver*</td>
<td>Sender</td>
<td>Sender, Receiver*</td>
<td>Sender, Receiver</td>
<td></td>
</tr>
<tr>
<td><strong>Protocol</strong></td>
<td>HTTP</td>
<td>TCP</td>
<td>HTTP</td>
<td>IP</td>
<td>Custom</td>
<td>IP</td>
</tr>
</tbody>
</table>

* Pre setup channels via rendezvous points
  - Do not depend on network load
  - Same for each everyone connecting to this server
Goals

- Sender and receiver anonymity
- Relationship anonymity
- Transparent application support
  - No changes to applications
  - IP level sanitizing
- Near real-time service
- Practical anonymity
  - No protection against global eavesdropper
Anonymous Communication: Onion Routing

- **Example:**

  1. **Sender selects an anonymous path**
  2. **Layered encryption**
     - One hop can only decrypt its successor
     - Each hop removes a layer of encryption
     - Intermediate nodes and receiver have no information about the sender

  

  Sender selects an anonymous path by encrypting messages with multiple layers of encryption, each layer encrypted with a public key of a different hop. This way, only the intended receiver can decrypt the message by removing each layer sequentially.
Anonymous Communication: Problem

- Sender has to know receiver’s IP address
  - Only sender and relationship anonymity
- To provide receiver anonymity
  - Hide receiver behind relaying nodes
  - Enables
    - Web server
    - File server
    - P2P
Anonymous Communication: Solution

- **Path selection**
  - Head by sender
  - Tail by receiver

- **Receiver publishes**
  - Path entry point
  - Path as layered encryption

- **Sender concatenates to anonymous path**
Service Discovery

- Retrieval of path sections
- The service discovery stores
  - Anonymous path sections
    - Signed with anonymous id against impersonation
  - All relaying nodes
- Path sections are encrypted
  - Does not reveal
    - Relaying nodes’ identities
    - Receiver’s identity
  - Implementation choice
    - Trusted servers
    - Peer-To-Peer based index (e.g. Chord)
Transparent Application Support

- **Sanitizing**
  - Clear payload from personal information

- **In-band signaling**
  - Node IP in payload
  - FTP, H.323, real-audio,…

- **Enhancement via proxy possible**
  - Very talkative protocols, like http

- **Other approaches only use proxies**
Transparent Application Support

- Virtual network interface (NIC)
- Private IP address
- Application independent
  - No changes to applications
  - Ftp, http, ssh, instant messaging, samba …
Threat Model

• Practical adversary
  ▶ Observe some part of the network
  ▶ Participate actively
    ▾ Relaying traffic of other nodes
    ▾ Offer service, e.g. web server
    ▾ Access content
  ▶ Compromise a limited number of nodes
  ▶ Influence communications
    ▾ Generating,
    ▾ Delaying,
    ▾ Modifying traffic content and patterns

• Do not protect against global adversary!
Security Analysis

- Source / destination observation
  - Traffic is relayed
  - Traffic relay for other nodes
  - Messages padding to constant length,

It is not possible to determine via observation whether a node is sender, relay or receiver of a message.
Example: Using a Web Browser

Sender

Host 1
Virtual IP: 10.20.4.77

Path through mix cascade

Host 2
Virtual IP: 10.2.3.79

Receiver
**Example: Using a Web Browser**

1. **GET http://www.freespeech.anon HTTP/1.1**
   - **Web browser**
   - **DNS resolve freespeech.anon**
   - **DNS reply 10.2.3.79**
   - **Virtual IP: 10.2.3.79**
   - **TCP data request to 10.2.3.79**
   - **Directory Service**
   - **Virtual IP and anonymous path sections**
   - **Path through mix cascade**
   - **TCP data request from 10.20.4.77**
   - **SARA**
   - **Host 2 Virtual IP: 10.2.3.79**
   - **www.freespeech.anon**
   - **TCP data reply to 10.20.4.77**
   - **Anonymous path sections**
   - **Path through mix cascade**
   - **GET path to freespeech.anon**
   - **TCP data reply from 10.2.3.79**
   - **Path through mix cascade**
   - **TCP data reply to 10.20.4.77**
   - **SARA**
   - **Directory Service**
   - **Get path to 10.20.4.77**
   - **TCP data reply to 10.20.4.77**
   - **Web server on Host 2**
Conclusion

• Need for
  ▶ Sender and receiver anonymity
  ▶ Transparent application support

• SARA provides
  ▶ Sender, receiver, and relationship anonymity
  ▶ Via path concatenation

• Transparent application support
  ▶ Communication stack, IP level support
  ▶ Address virtualization
  ▶ Seamless support for most protocols / applications

• Integration of existing web applications
  ▶ Web and fileservers
  ▶ Instant messaging, Audio streaming
Time for questions

http://ps.ri.uni-tuebingen.de
Ralf Steinmetz, Klaus Wehrle (Eds.)

Peer-to-Peer Systems & Applications
Springer Publishing, Sept. 2005

- **Compendium**
  - 10 Parts / 32 Chapters / 650 pages
  - Covers the wide spectrum of Peer-to-Peer Systems and Applications

- **Text Book for Teaching:**
  - Chapters designed for teaching classes and seminars
  - eLearning material available

- **Web Site:**
  - http://www.peer-to-peer.info