Universität Basel

Topic Defense PhD Martin Gwerder

Sending Unobservable Messages Across Public Networks

Martin Gwerder

8.6.2015

Table of contents

Universität Basel

Table of contents

Universität Basel

Main Goals are ...

- ... to have a common understanding of the PhD topic.
- ... to have an agreement on the focus of the thesis.
- ... to have an agreement on the expected outcome of thesis.

Universität Basel

Thesis Goal

Send messages unobserved through a public network.

Universität Basel

Definition of system

- Sends messages unobserved (not perceived) through public networks.
- Is easy to accept for users and node owners.
- Is reliable (in terms of message delivery and security).

Universität Basel

Attributes of user

- Does care about privacy.
- Does or does not have support from a mail server admin.
- Has no special computer knowhow.
- Has the ability to install a program or plugin on his personal computer.
- Has no cryptographic knowhow.
- Is using a device with enough calculation power to solve cryptographic tasks.

Intentions of user

- Send personal or confidential information securely to another user.

Expectations of user

- System should be easy to configure and maintain (in an ideal world: Zero touch).
- System should be fast.
- System should be reliable.
- System should work on any client he is already using.
- System should not be a legal problem to him or any of his peers.

Universität Basel

Attributes of observer

- Available founding is huge.
- Can have nodes infrastructure.
- Is able to read, write, modify or reroute network data freely at any point of the net.

Intentions of observer

- Discover message flows
- Discover message contents
- Identify users of the system
- Collect data of of users

Universität Basel

Definition of owner

- Does care about privacy.
- Has considerable computer know-how.
- Has the ability to install programs or plugins.
- Has possibly no cryptographic know-how.
- Does know his own infrastructure.
- Is using an Infrastructure with enough calculation power to solve cryptographic tasks.

Intentions of owner

- Support his users in sending personal or confidential information securely to another user

Expectations of owner

- System should be easy to configure and maintain (in an ideal world: Zero touch).
- System should be fast.
- System should be reliable.
- System should work on any client he is using.
- System should not be a legal problem for him or his company.
- System should still allow him to do regulatory tasks such as virus scanning or backup.

Universität Basel

Attributes of Node

- Is a publicly reachable Server.
- Participates in the whole system.
- Serves one or more defined purposes.
- Does have users participating in the unobservable system and other users.

Universität Basel

Protocol requirements

- Unidentifiable
- Untagable
- Unreplayable
- Monolithic messages

Universität Basel

Infrastructure requirements

- Unknown endpoints
- No relations between single hops
- Untrusted infrastructure
- No central infrastructure
- No direct communication between endpoints

Universität Basel

Acceptance requirements

- Easy
- Fast
- Reliable
- Not abuseable

Universität Basel

Building blocks

- Traffic/Chat generation
- Steganography, encryption, and hashing
- cryptopuzzles
- Discardable identities
- compression
- One time routing tokens (for sending or error replys)
- Routing
  - Split and reassembly of messages
  - possibly DC-Rings or XOr-trees
  - Onion routing

Universität Basel

Solution so far

- User sends a steganographicalli hidden message to a peer. This message contains:
  - Message (or parts of it) to be sent to the final recipient.
  - Decoy traffic.
  - OTRT (One Time Routing Token) for error messages.
  - Possible additional routing information.
- Node tries to decypt, uncompress, and disassemble received message into chunks.
- Node may reassemble chunks in the wait queue to a bigger chunk.
- Node may add routing information to chunk.
- Node passes message chunks on without knowing what is in it. It knows last and next hop (by IP).

Thesis Title

Messagevortex – Sending messages unobserved through a public network.

Universität Basel

Proposed thesis content is ...

- Create a generic approach to transport messages through public networks unobserved. (as defined previously)
- Create a generic implementation (traffic generator) of the approach.
- Generate large scale traffic samples with different parameters used by sender.
- Do traffic analysis against the approach to identify weaknesses and find optimal behaviour.

  Focus lies on:
  - Identifying endpoints of communication.
  - Identifying messages, message types or parts of them.
  - Identifying patterns of service usage.
  - Identifying weaknesses in robustness.
- Create a library/framework for creating messages.
- Create a working minimal prototype based on the library.

Discussion

Universität Basel