

1 General

Goals

2 Definitions

System

User

Observer

Owner

Node

3 Requirements

Protocol

Infrastructure

Acceptance

4 Solution

Sneak peek

5 Thesis

Content

6 Discussion

Topic Defense PhD Martin Gwerder

Sending Unobservable Messages Across Public Networks

Martin Gwerder

8.6.2015

1 General

Goals

2 Definitions

System

User

Observer

Owner

Node

3 Requirements

Protocol

Infrastructure

Acceptance

4 Solution

Sneak peek

5 Thesis

Content

6 Discussion

Table of contents

- | | |
|----------------|------------------|
| 1 General | 3 Requirements |
| • Goals | • Protocol |
| | • Infrastructure |
| 2 Definititons | • Acceptance |
| • System | 4 Solution |
| • User | • Sneak peek |
| • Observer | 5 Thesis |
| • Owner | • Content |
| • Node | 6 Discussion |

1 General

Goals

2 Definitions

System

User

Observer

Owner

Node

3 Requirements

Protocol

Infrastructure

Acceptance

4 Solution

Sneak peek

5 Thesis

Content

6 Discussion

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.

1 General

Goals

2 Definitions

System

User

Observer

Owner

Node

3 Requirements

Protocol

Infrastructure

Acceptance

4 Solution

Sneak peek

5 Thesis

Content

6 Discussion

Definition of system

- Sends messages unobserved (not perceived) through public networks.
- Is easy to accept for users.
- Is reliable.

1 General

Goals

2 Definitions

System

User

Observer

Owner

Node

3 Requirements

Protocol

Infrastructure

Acceptance

4 Solution

Sneak peek

5 Thesis

Content

6 Discussion

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.

Intensions 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 using.
- System should not be a legal problem to him or any of his peers.

1 General

Goals

2 Definitions

System

User

Observer

Owner

Node

3 Requirements

Protocol

Infrastructure

Acceptance

4 Solution

Sneak peek

5 Thesis

Content

6 Discussion

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.

Intensions of observer

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

1 General

Goals

2 Definitions

System

User

Observer

Owner

Node

3 Requirements

Protocol

Infrastructure

Acceptance

4 Solution

Sneak peek

5 Thesis

Content

6 Discussion

Definition of owner

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

Intensions 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.

1 General

Goals

2 Definitions

System

User

Observer

Owner

Node

3 Requirements

Protocol

Infrastructure

Acceptance

4 Solution

Sneak peek

5 Thesis

Content

6 Discussion

Attributes of Node

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

1 General

Goals

2 Definitions

System

User

Observer

Owner

Node

3 Requirements

Protocol

Infrastructure

Acceptance

4 Solution

Sneak peek

5 Thesis

Content

6 Discussion

Protocol requirements

- Unidentifiable
- Untagable
- Unreplayable
- monolythicMonolithic messages

1 General

Goals

2 Definitions

System

User

Observer

Owner

Node

3 Requirements

Protocol

Infrastructure

Acceptance

4 Solution

Sneak peek

5 Thesis

Content

6 Discussion

Infrastructure requirements

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

1 General

Goals

2 Definitions

System

User

Observer

Owner

Node

3 Requirements

Protocol

Infrastructure

Acceptance

4 Solution

Sneak peek

5 Thesis

Content

6 Discussion

Acceptance requirements

- Easy
- Fast
- Reliable
- Not abuseable

1 General

Goals

2 Definitions

System

User

Observer

Owner

Node

3 Requirements

Protocol

Infrastructure

Acceptance

4 Solution

Sneak peek

5 Thesis

Content

6 Discussion

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

1 General

Goals

2 Definitions

System

User

Observer

Owner

Node

3 Requirements

Protocol

Infrastructure

Acceptance

4 Solution

Sneak peek

5 Thesis

Content

6 Discussion

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.
- 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 working minimal prototype based on the findings.

1 General

Goals

2 Definitions

System

User

Observer

Owner

Node

3 Requirements

Protocol

Infrastructure

Acceptance

4 Solution

Sneak peek

5 Thesis

Content

6 Discussion