

1 General

Goals

Thesis Goa

2 Definitions

System

User

Observe

Owner

Node

3 Requirements

Protocol

Acceptance

4 Solution

Sneak pe

5 Thesis

. . .

6 Discusion

Topic Defense PhD Martin Gwerder

Sending Unobservable Messages Across Public Networks

Martin Gwerder

8.6.2015

Table of contents



1 General

2 Definitions

3 Requirements

4 Solution

5 Thesis

6 Discusion

Table of contents

- General
 - Goals
 - Thesis Goal
- Definititons
 - System
 - User
 - Observer
 - Owner
 - Node

- Requirements
 - Protocol
 - Infrastructure
 - Acceptance
- Solution
 - Sneak peek
- 5 Thesis
 - Thesis Title
 - Content
- Discussion

General Goals



1 General

Goals

Thesis Goal

2 Definitions

Systen

User

01

Owne

Node

3 Requirements

Protocol

Infrastructur Acceptance

4 Solution

5 Thoric

Title

6 Discusion

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.

General Thesis Goal



1 General

Thesis Goal

2 Definitions

Heor

Observer

Owne

Node

3 Requirements

Protocol

Acceptance

4 Solution
Sneak peek

5 Thesis

I ITIE

6 Discusion

Thesis Goal

Send messages unobserved through a public network.

Definitions System



1 General

1 Genera

Thesis Goa

2 Definitions

System

Heor

Owner

....

3 Requirements

Protocol

Infrastructui

4 Solution

5 Thesis

Litle

6 Discusion

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).

Definitions User



1 Genera

1 Genera

Thesis Go

2 Definitions

2 Delillition

System

User

Obser

Owne

Node

3 Requirements

Protoco

Intrastructu

4 Solution

- ---

Title

6 Disausias

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.

Definitions Observer



1 Genera

1 Genera

Thesis Go

2 Definitions

C.....

User

Observer

Owner

None

3 Requirements

Infrastructu

Acceptance

4 Solution

5 Thesi

Title

6 Discusion

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

Definitions

Owner



1 Conoral

1 Genera

Thesis Go

2 Definitions

2 Definition

System

User

Ubserv

Owner

3 Requirements

Protocol

Infrastructui

4 Solution

Sneak pee

5 Thesis

- I ILIE

6 Discusion

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.
- O System should still allow him to do regulatory tasks such as virus scanning or backup.



Definitions Node



1 General

1 General

Thesis Goal

2 Definitions

..

Ubserve

Node

3 Requirements

Protocol

Intrastructur

4 Solution

5 Thesis

Title

6 Discusion

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.

Requirements Protocol



1 General

1 Oction

Thesis Goal

2 Definitions

C.....

Heor

01-----

0.....

Node

3 Requirements

Protocol

Acceptance

Ассерение

4 Solution

Sneak p

5 Thesis

. . .

6 Discusion

Protocol requirements

- Unidentifiable
- Untagable
- Unreplayable
- Monolithic messages

Requirements Infrastructure



1 General

2 Definitions

3 Requirements

Infrastructure

4 Solution

6 Discusion

Infrastructure requirements

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

Requirements Acceptance



1 General

2 0011014

Thesis Goa

2 Definitions

...

Observer

Observ

Node

3 Requirements

Infrastruc

Acceptance

4 Solution

Sneak peek

5 Thesis

. . .

6 Discusion

Acceptance requirements

- Easy
- Fast
- Reliable
- Not abuseable

Solution Sneak peek



1 General

1 Genera

Thesis Goa

2 Definitions

2 Deminition

...

Owner

Node

3 Requirements

Protocol

Acceptance

4 Solution Sneak peek

5 Thoris

Litle

6 Discusion

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

Solution Sneak peek (2)



1 Genera

Thesis G

0 0 0 ...

2 Definition

System

0.....

D1 - -1 -

3 Requirements

Protocol Infrastructuu

Acceptance

4 Solution Sneak peek

5 Thesi

Title

6 Discusion

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 Proposed Title



1 General

2 0011014

Thesis Goal

2 Definitions

Dystem

Observer

ODJCIV

Node

3 Requirements

Infrastructur

4 Solution

5 Thesis

- Itile

6 Discusion

Thesis Title

Messagevortex – Sending messages unobserved through a public network.

Thesis



1 General

_ ____

Thesis Goal

2 Definitions

System

User

Observe

Owne

Node

3 Requirements

Frotocoi

Acceptance

4 Solution

Sneak peek

5 Thesis

Title Content

Discusion

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



1 General

Goals

Thesis Goal

2 Definitions

System

Observer

ODJUIT

Node

3 Requirements

Protoc

Infrastructure

Acceptance

4 Solution

Sneak peek

5 Thesis

· . .

6 Discusion