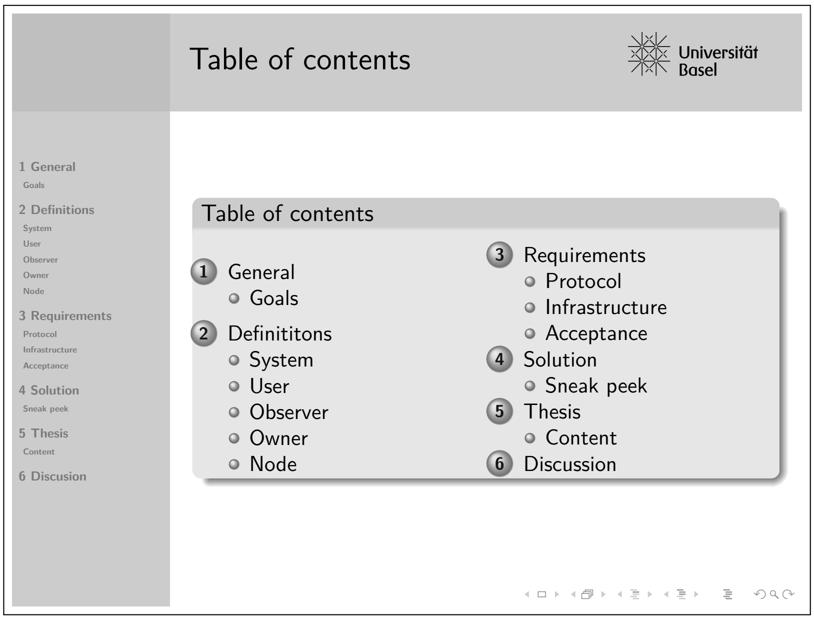


Table of contents

Universität Basel

1 General
Goals
2 Definitions
System
User
Observer
Owner
Node
3 Requirements
Protocol
Infrastructure
Acceptance
4 Solution
Sneak peek
5 Thesis
Content
6 Discusion

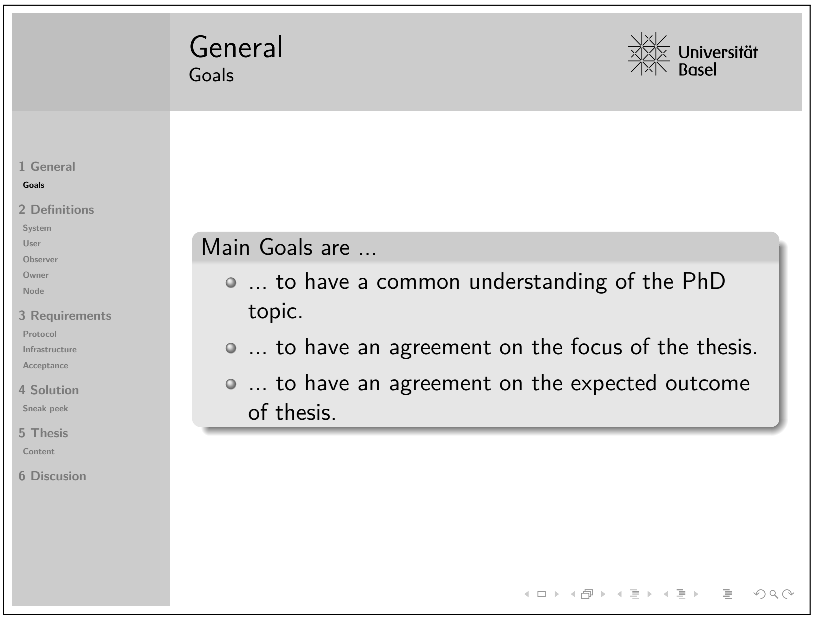
Table of contents

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

Inhaltsverzeichnis

1 General

1.1 Goals



General
Goals

Universität Basel

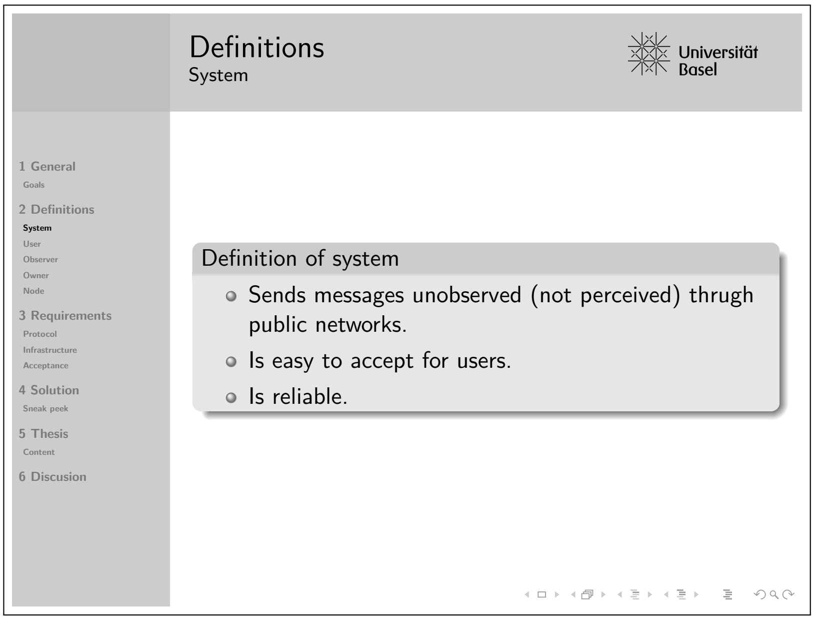
1 General
Goals
2 Definitions
System
User
Observer
Owner
Node
3 Requirements
Protocol
Infrastructure
Acceptance
4 Solution
Sneak peek
5 Thesis
Content
6 Discussion

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.

2 Defininititons

2.1 System



Definitions
System

Universität Basel

1 General
- Goals

2 Definitions
- System
- User
- Observer
- Owner
- Node

3 Requirements
- Protocol
- Infrastructure
- Acceptance

4 Solution
- Sneak peek

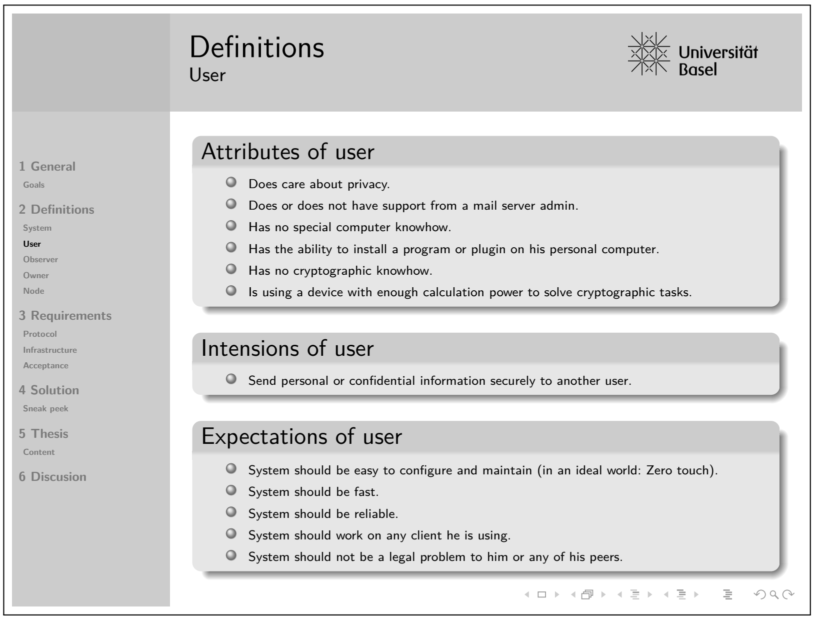
5 Thesis
- Content

6 Discusion

Definition of system

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

2.2 User



Definitions

User

Universität Basel

1 General
Goals

2 Definitions
System
User
Observer
Owner
Node

3 Requirements
Protocol
Infrastructure
Acceptance

4 Solution
Sneak peek

5 Thesis
Content

6 Discusion

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.

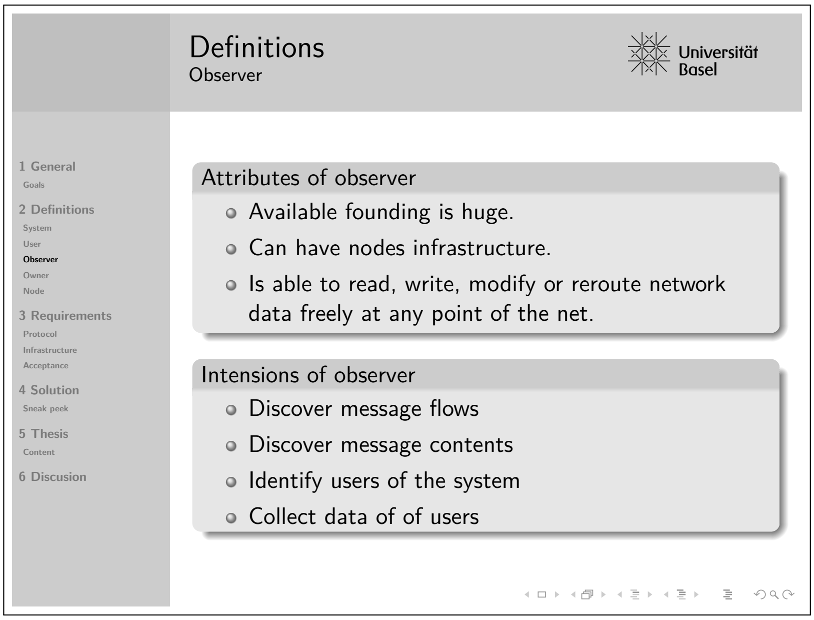
Intensions of user

- 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.

2.3 Observer



Definitions

Observer

Universität Basel

1 General
- Goals

2 Definitions
- System
- User
- **Observer**
- Owner
- Node

3 Requirements
- Protocol
- Infrastructure
- Acceptance

4 Solution
- Sneak peek

5 Thesis
- Content

6 Discusion

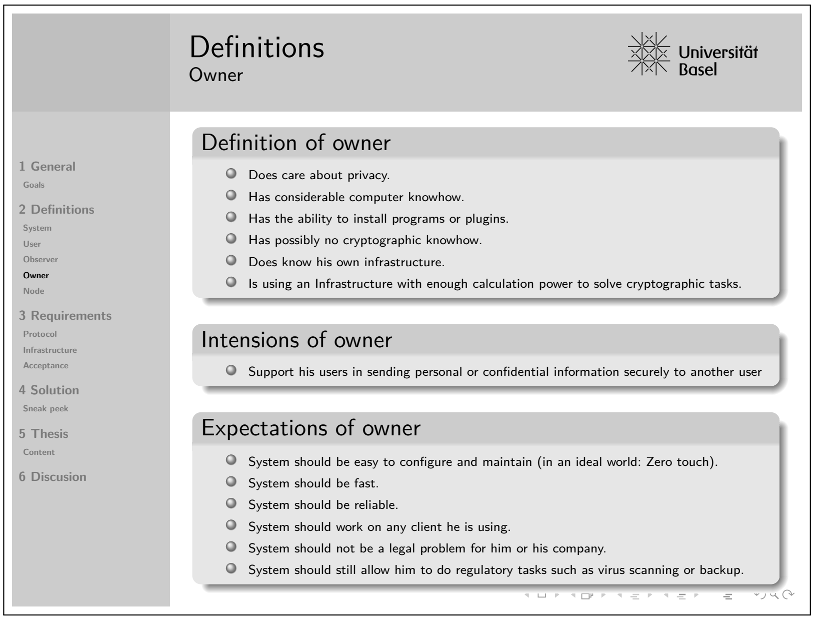
Attributes of observer

- 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.

Intensions of observer

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

2.4 Owner



Definitions

Owner

Universität Basel

1 General

Goals

2 Definitions

System

User

Observer

Owner

Node

3 Requirements

Protocol

Infrastructure

Acceptance

4 Solution

Sneak peek

5 Thesis

Content

6 Discusion

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.

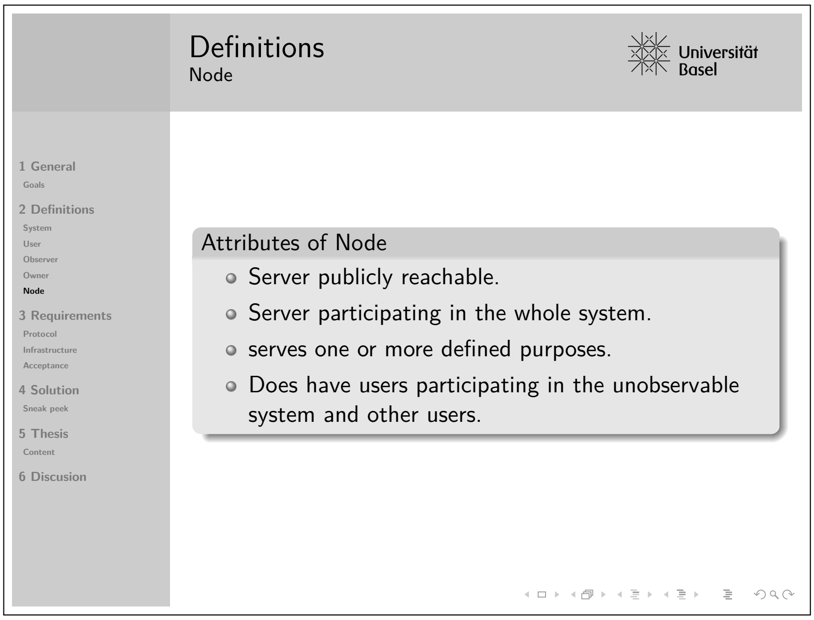
Intensions of owner

- 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.

2.5 Node



Definitions

Node

Universität Basel

1 General
- Goals

2 Definitions
- System
- User
- Observer
- Owner
- Node

3 Requirements
- Protocol
- Infrastructure
- Acceptance

4 Solution
- Sneak peek

5 Thesis
- Content

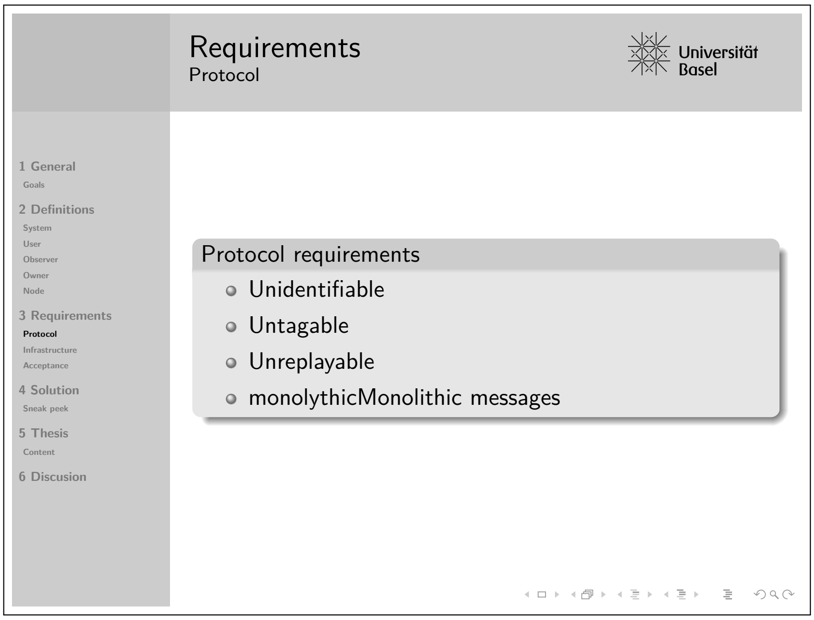
6 Discusion

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.

3 Requirements

3.1 Protocol



Requirements
Protocol

Universität
Basel

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

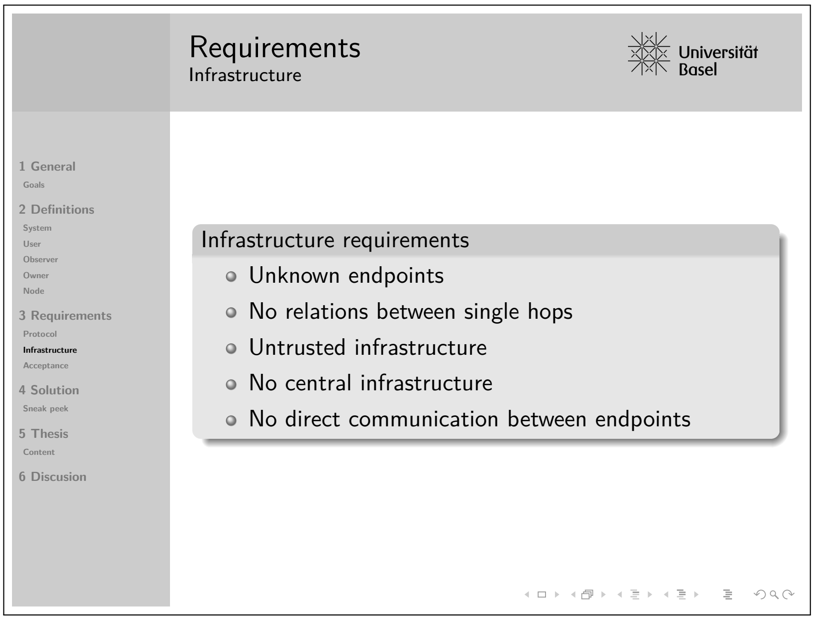
- Unidentifiable
  If a message or a participating node is identifiable then it is easy for an observer to block some or all parts of the system. This makes the system unreliable and may force users to use specific nodes (such as nodes which are under the control of the observer) and therefore compromise the overall security. Only a service that is able to hide its messages in legitimate network traffic is not subject to selective blocking.

- Untagable
  If messages going through the system are tagable by any of the participants (nodes) then an observer might tag messages and then follow them while they are propagating the network. If information is appended to a message it must be cloaked with the same reliability as the original message itself.

- Unreplayable
  If an observer can replay any part of the message (send it multiple times), he can identify the traffic generated by those messages by statistical means. This would enable him to identify traffic which is caused by a specific message and thus narrow down the possible final recipients.

- Monolithic messages
  Messages should not depend on external content (such as images). If a message is not self-contained then "bugging" is an easy way to identify the message on its way up until they reach the recipient or the recipient itself.

3.2 Infrastructure



Requirements
Infrastructure

Universität Basel

1 General
Goals

2 Definitions
System
User
Observer
Owner
Node

3 Requirements
Protocol
Infrastructure
Acceptance

4 Solution
Sneak peek

5 Thesis
Content

6 Discusion

Infrastructure requirements

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

- Unknown endpoints
  Every endpoint should behave the same as an intermediate routing point. They should receive and send messages so that they are not identifiable as endpoints. Identifiable endpoints simplify analysis.

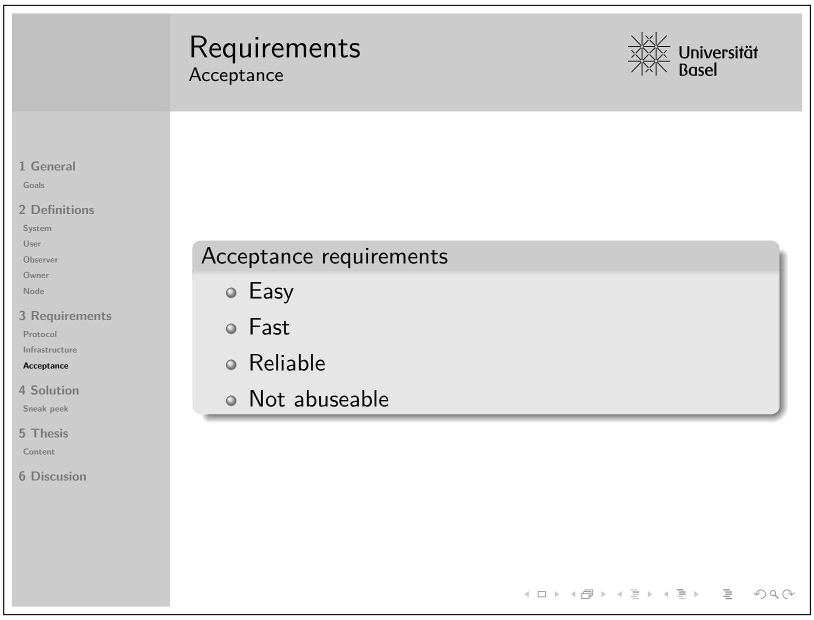
- No relations between single hops
  Messages transferred from server to server must be unrelated. Server identifiable to send messages due to received messages are potential targets for analysis.

- Untrusted infrastructure
  Unlike in a company owned net, in a public network trusting an infrastructure is not sensible. It is very often not clear who owns a server and who else does have access to it. The motivation of an infrastructure owner is often not clear and his intentions may or may not be sincere. So an unobservable system may not build its unobservability based on behaviour of the transporting infrastructure.

- No central infrastructure
  Central infrastructure may be attacked or shut down. They are easier to monitor than an unknown number of participants. Furthermore a central infrastructure may be used to compromise security of messages or nodes. It enables an observer to identify nodes by monitoring the traffic of a central infrastructure.

- No direct communication between endpoints
  If sender and receiver communicate directly then they are easily identified. So – all communications between endpoints should normally be done via intermediate nodes.

3.3 Acceptance



Requirements
Acceptance

Universität Basel

1 General
Goals

2 Definitions
System
User
Observer
Owner
Node

3 Requirements
Protocol
Infrastructure
Acceptance

4 Solution
Sneak peek

5 Thesis
Content

6 Discusion

Acceptance requirements

- Easy
- Fast
- Reliable
- Not abuseable

- Easy
  A system must be easy to use. The possibilities should be similar to common elaborated systems and the usage should be alike or the same. This offers a steep learning curve to the user.

  If ignored, only the users heavily concerned about their privacy would be willing to use the system. All others would ignore it as they are not ready to invest efforts into a system that offers them not sufficient benefits but new limitations.

- Fast
  In today's world we already adapted to fast moving messages. It is quite common that people talk to each other and send at the same time additional informations by chat or mail. They do expect that this information propagates fast through public networks. For some messages even an almost instant reply of the recipient is expected by the sender. Therefore any system must allow a fast transport of messages from the sender to the recipient.

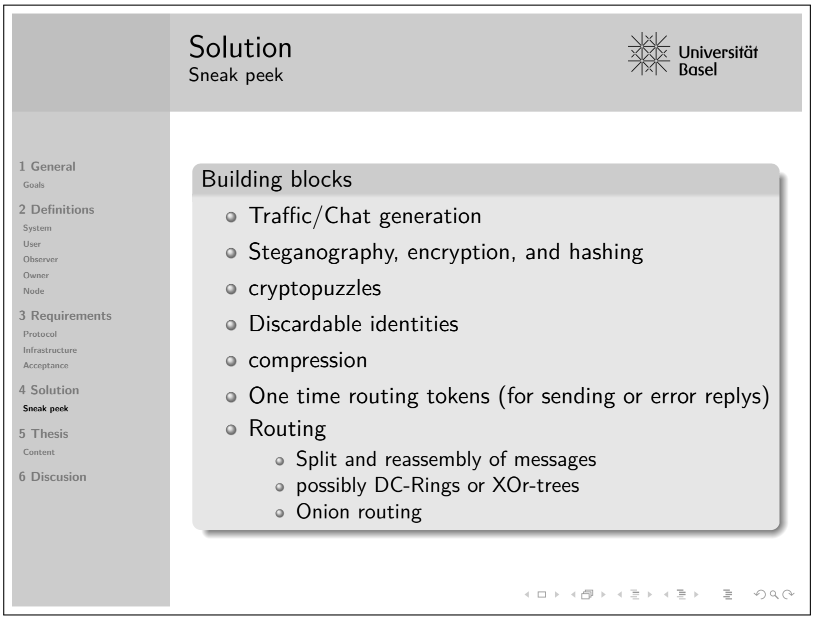
- Reliable
  Messages are expected to arrive at the recipient's device. Today there are numerous common systems such as email, chat, sms and mms offering reliable transfers. Any system not sending reliably will not be used due to the limitations given by an unreliable system.

  Another part of reliability is the protection. The message protection must be unbreakable (within reasonable bounds). If the system can be attacked easily then it offers ”no value”for ädditional effort”. For most users this would be a reason to discard such a solution.

- Not abuseable
  Any system may be abused. The willingness of using a system if it is to easily abusable is very limited. A user will not be using a system which increases UBM (unsolicited bulk messages) or enables someone to blackmail him easily.

4 Solution

4.1 Sneak peek



Solution
Sneak peek

Universität
Basel

1 General
Goals

2 Definitions
System
User
Observer
Owner
Node

3 Requirements
Protocol
Infrastructure
Acceptance

4 Solution
Sneak peek

5 Thesis
Content

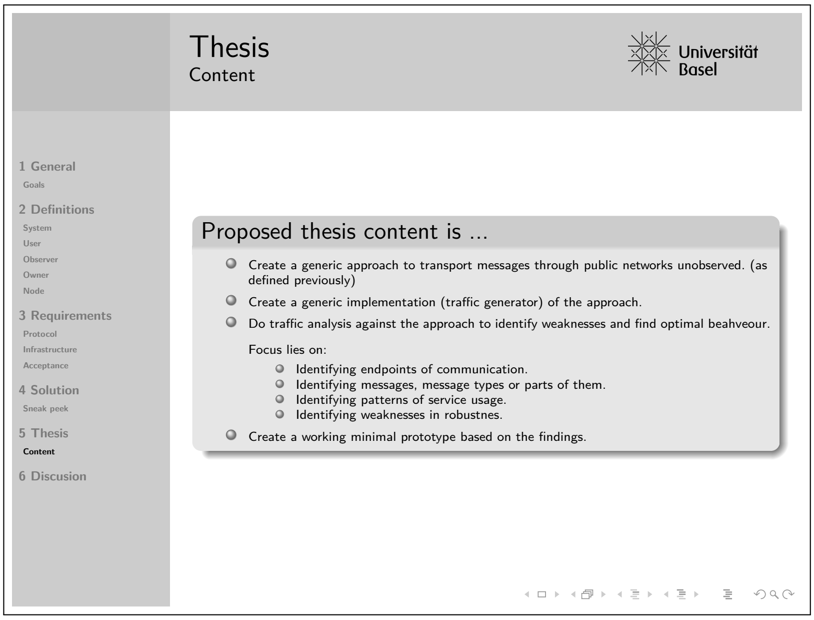
6 Discusion

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

5 Thesis

5.1 Content



Thesis
Content

Universität Basel

1 General
Goals
2 Definitions
System
User
Observer
Owner
Node
3 Requirements
Protocol
Infrastructure
Acceptance
4 Solution
Sneak peek
5 Thesis
Content
6 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.
- Do traffic analysis against the approach to identify weaknesses and find optimal beahveour.

  Focus lies on:
  - Identifying endpoints of communication.
  - Identifying messages, message types or parts of them.
  - Identifying patterns of service usage.
  - Identifying weaknesses in robustnes.
- Create a working minimal prototype based on the findings.

6 Discussion

Discussion

1 General
Goals
2 Definitions
System
User
Observer
Owner
Node
3 Requirements
Protocol
Infrastructure
Acceptance
4 Solution
Sneak peek
5 Thesis
Content
6 Discusion