Security Analysis of Instant Messenger TorChat

Master's thesis

Rain Viigipuu

Supervisor: Alexander Norta, PhD
External Supervisor: Arnis Paršovs, MSc

June 4, 2015

Challenge

Secure and private communication over the Internet

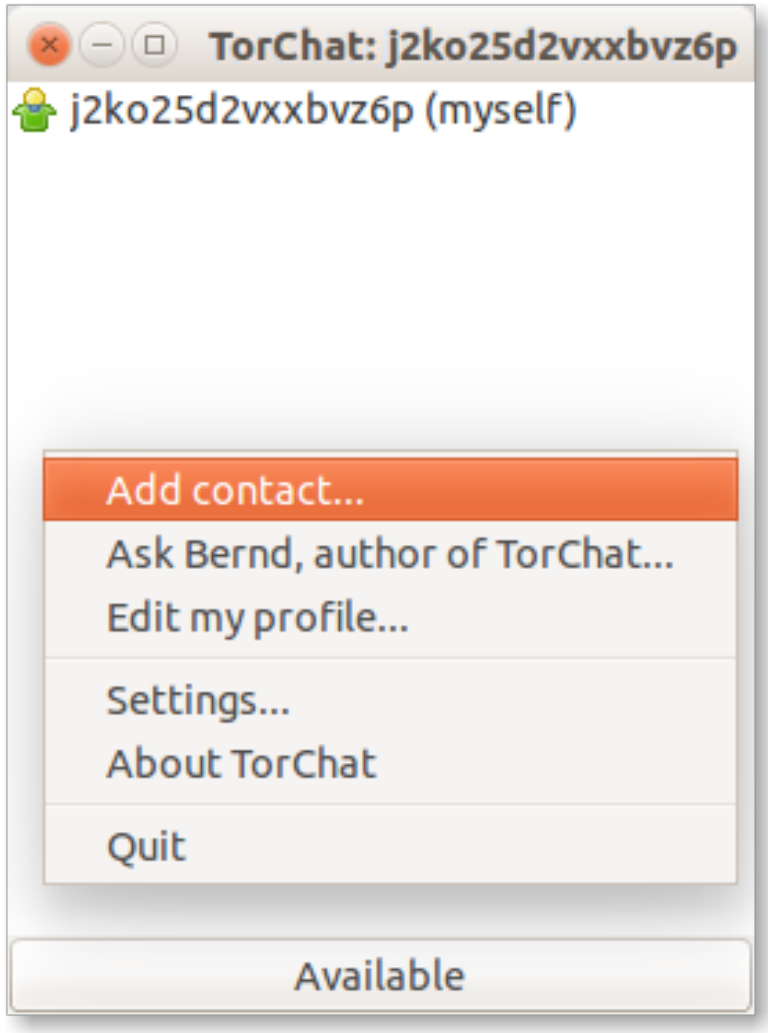
- Confidentiality
- Integrity
- Authenticity
- Metadata privacy

How to achieve that?

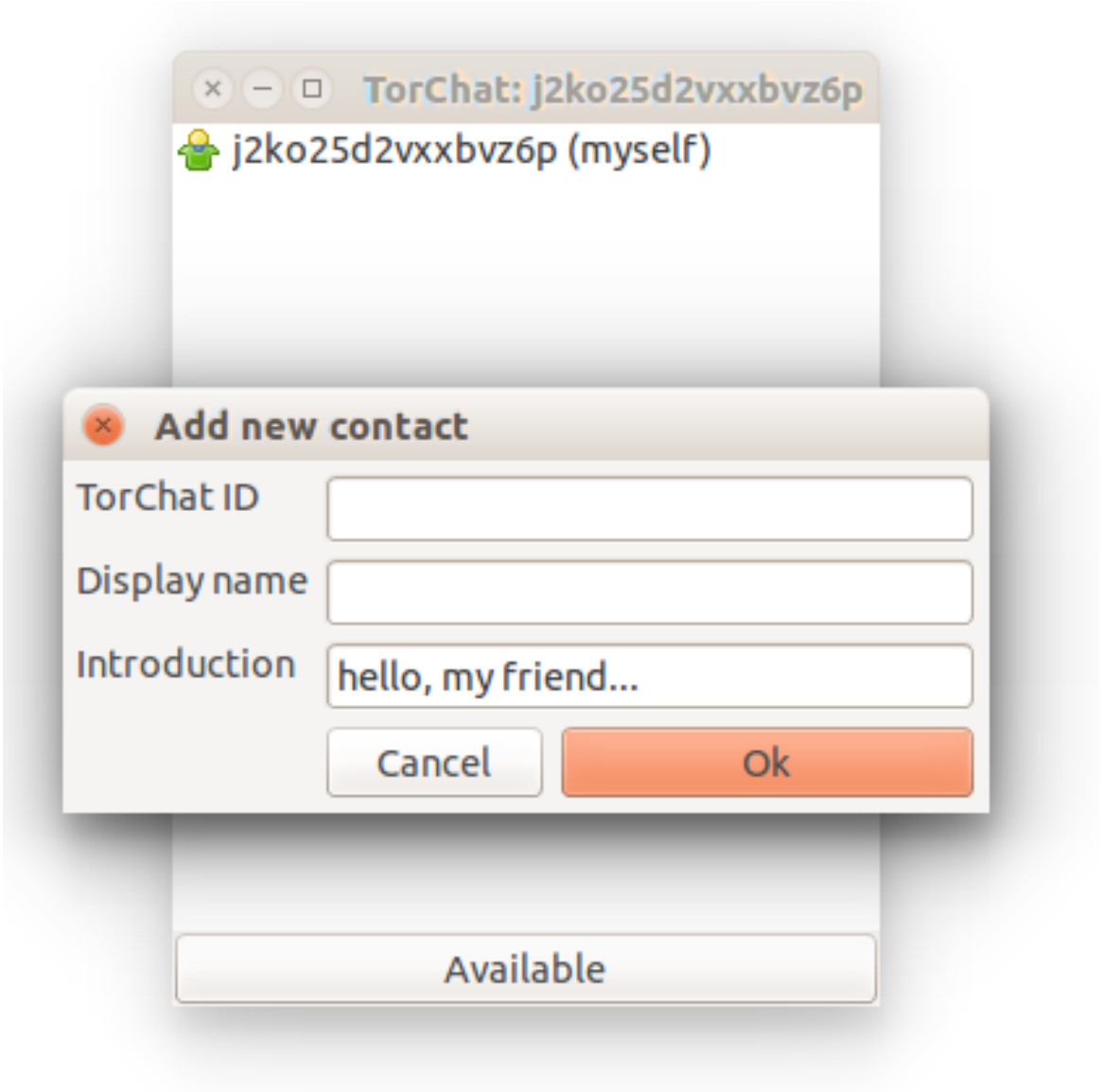
TorChat


TorChat: j2ko25d2vxxbvz6p
j2ko25d2vxxbvz6p (myself)
Available

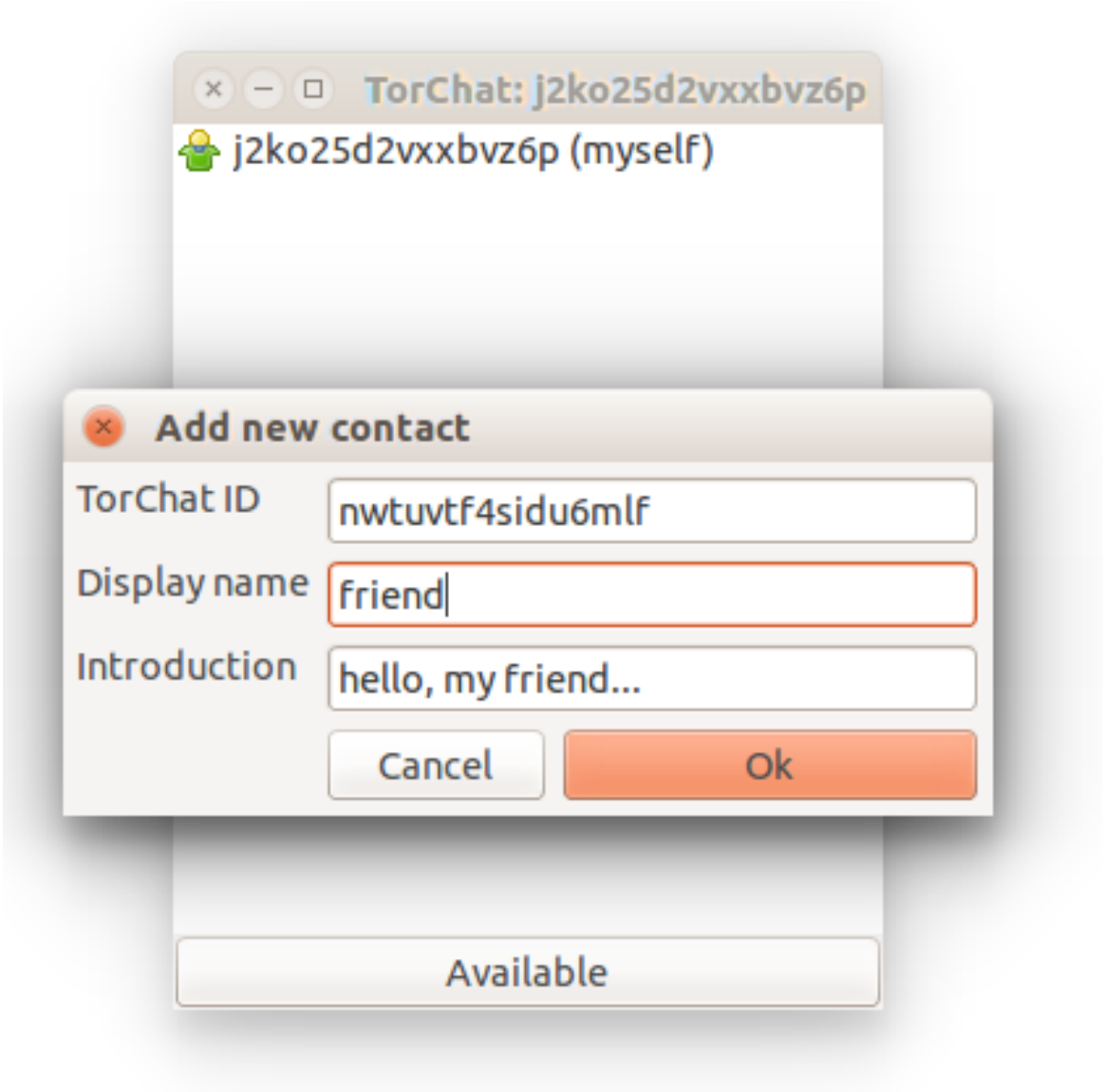
TorChat


TorChat: j2ko25d2vxxbvz6p
j2ko25d2vxxbvz6p (myself)
Add contact...
Ask Bernd, author of TorChat...
Edit my profile...
Settings...
About TorChat
Quit
Available

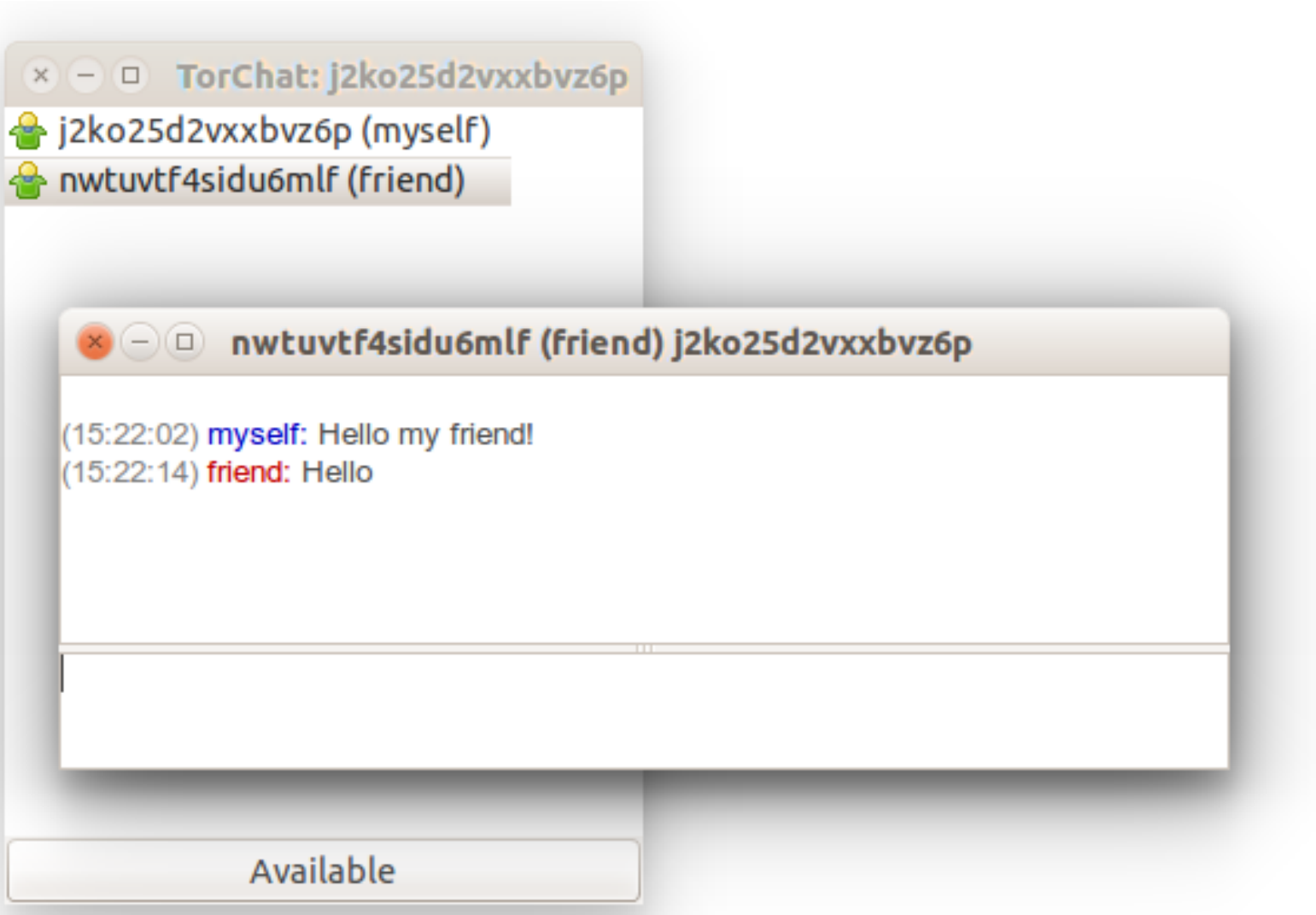
TorChat


TorChat: j2ko25d2vxxbvz6p
j2ko25d2vxxbvz6p (myself)
Add new contact
TorChat ID
Display name
Introduction
hello, my friend...
Cancel
Ok
Available

TorChat


TorChat: j2ko25d2vxxbvz6p
j2ko25d2vxxbvz6p (myself)
Add new contact
TorChat ID
nwtuvtf4sidu6mlf
Display name
friend
Introduction
hello, my friend...
Cancel
Ok
Available

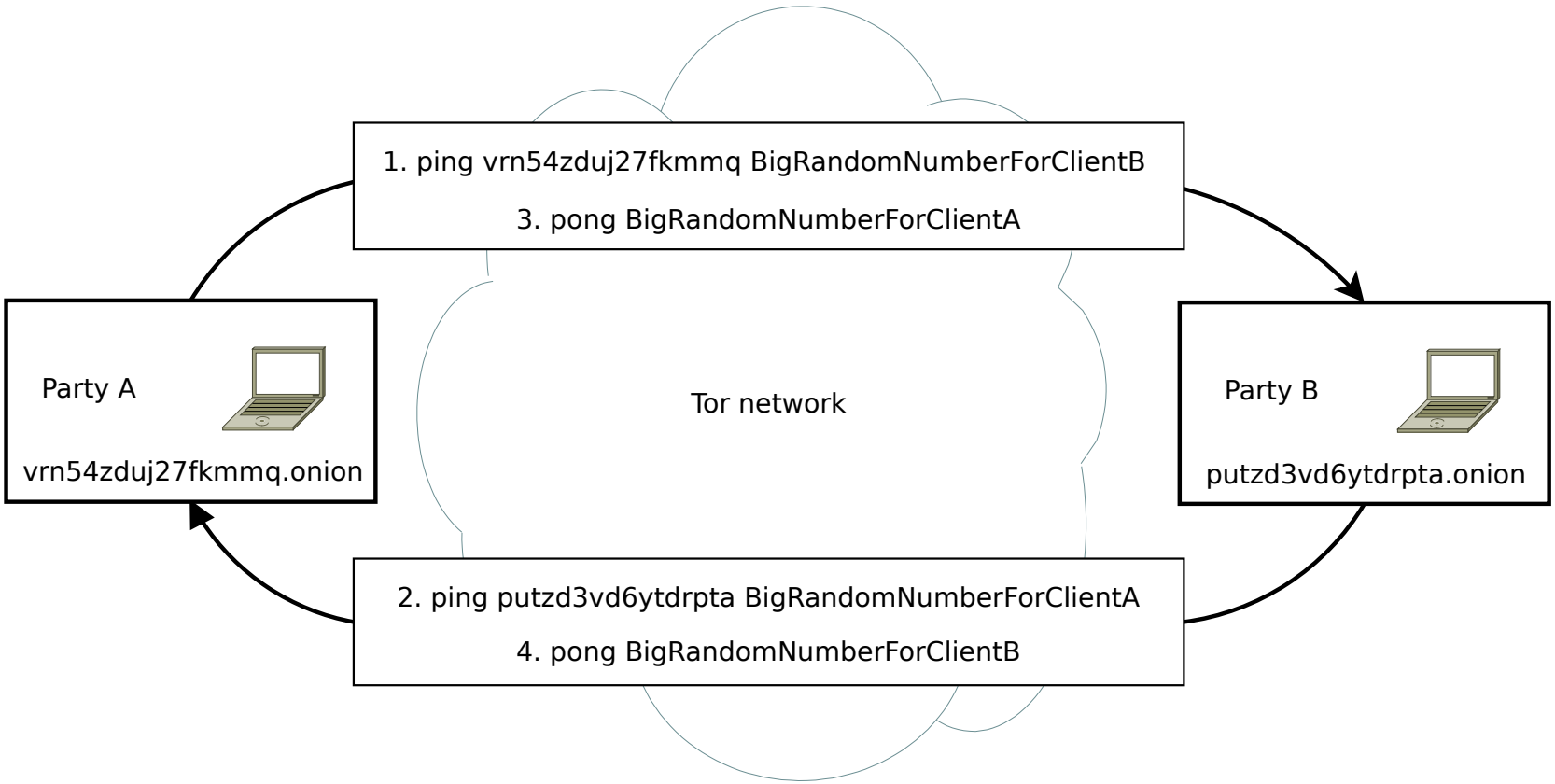
TorChat


TorChat: j2ko25d2vxxbvz6p
j2ko25d2vxxbvz6p (myself)
nwtuvtf4sidu6mlf (friend)
nwtuvtf4sidu6mlf (friend) j2ko25d2vxxbvz6p
(15:22:02) myself: Hello my friend!
(15:22:14) friend: Hello
Available

Objectives

1. Document TorChat protocol
2. Analyze security of the protocol
3. Audit reference implementation

TorChat protocol



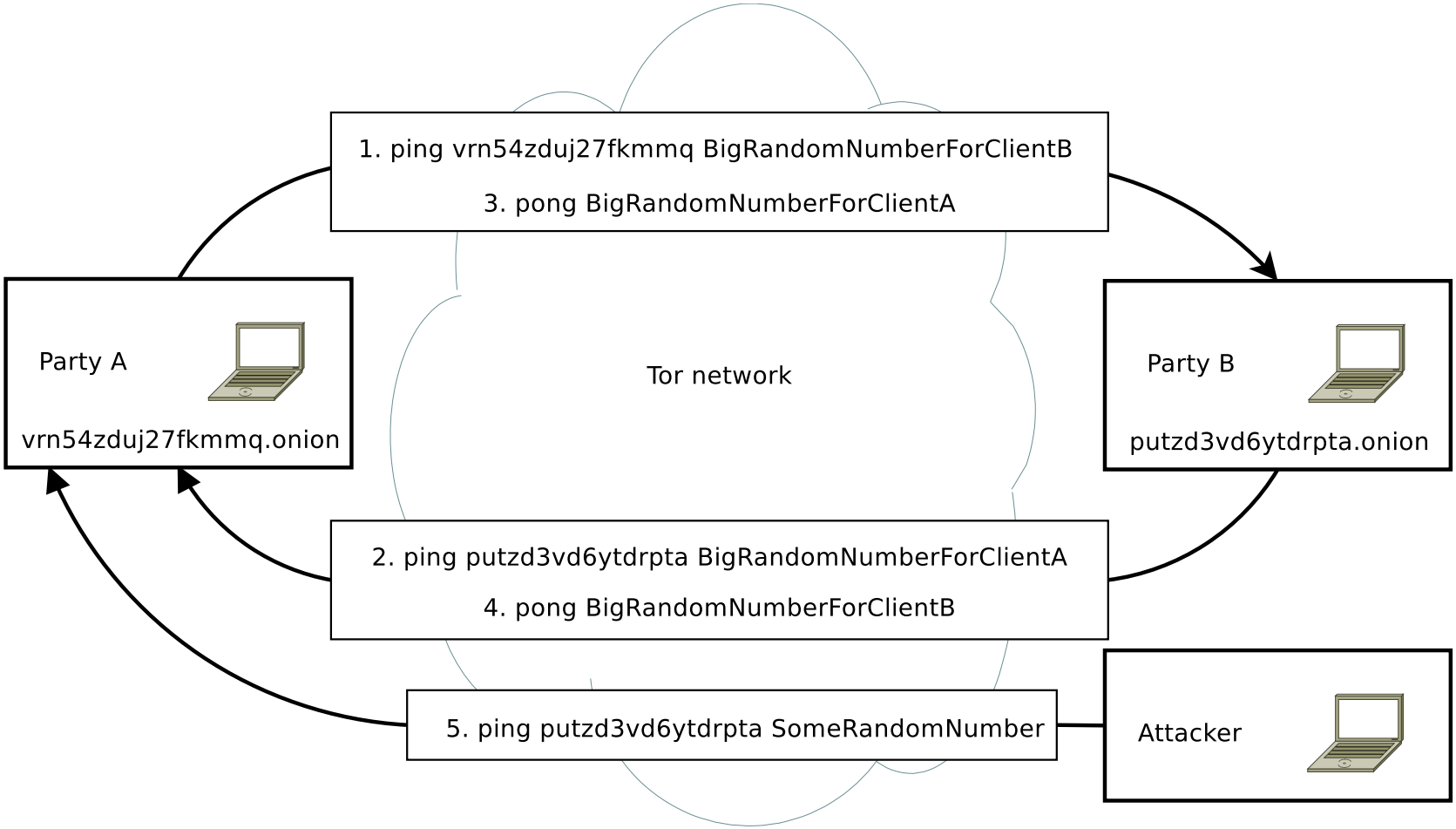
Methodology

Based on EFF's "Secure Messaging Scorecard".

1. How is the communication protected in transit?
2. Can the service be used anonymously?
3. Who can learn about communication taking place?
4. How user's profile information is protected?
5. What forensic evidence is left on the user's device?
6. Is the source code available, is software available from trusted source?

Findings (1)

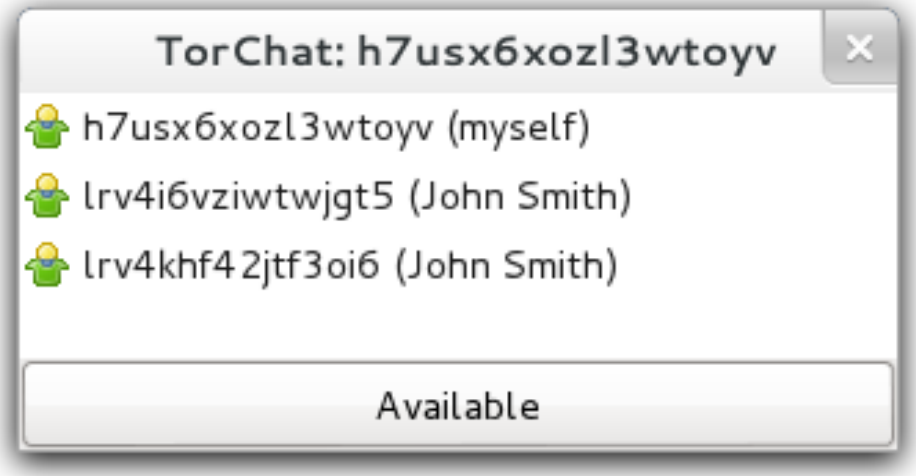
Communication confirmation attack:



Findings (2)

Contact list manipulation:

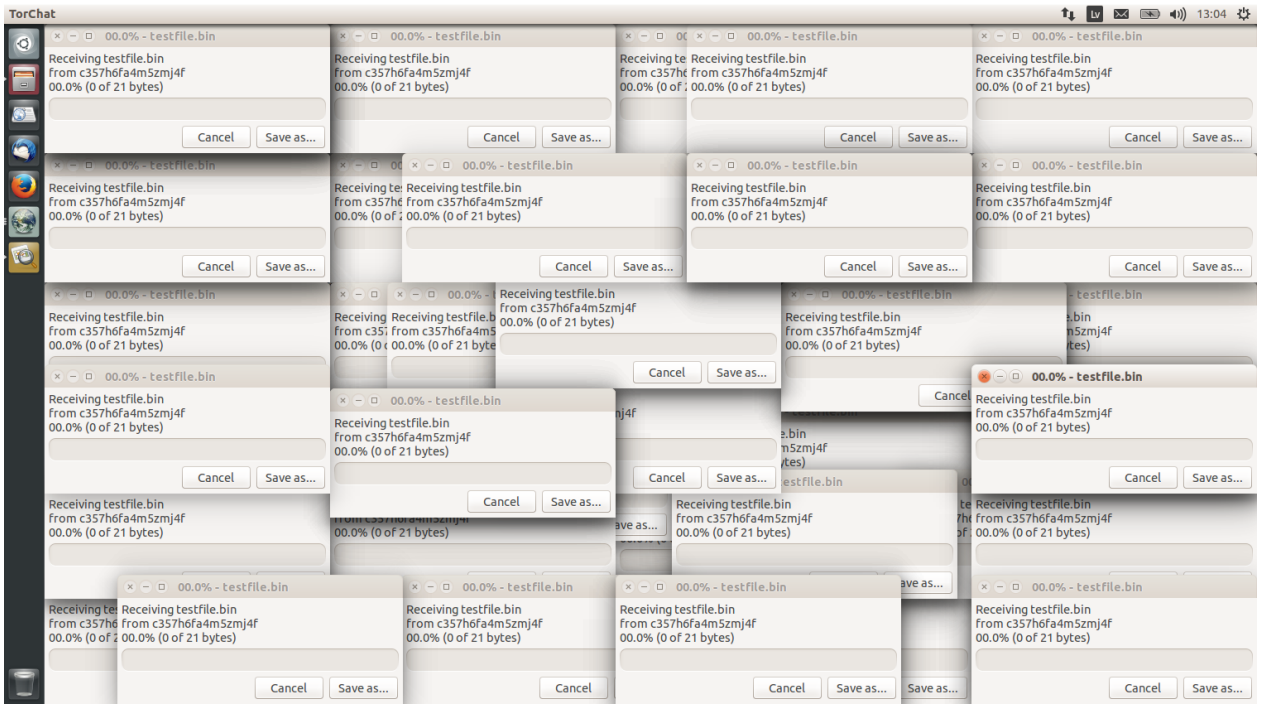
- Leaks profile information
- Contact confusion attack



Findings (3)

Denial-of-service attacks:

- No limits for message length
  - The command is buffered in memory
  - No limit for chat message
- Filetransfers accepted automatically



Conclusion

- TorChat design is sound
- TorChat implementation has flaws
- The flaws can be easily fixed

Thank you!

Questions?