RUHR-UNIVERSITÄT BOCHUM

RUB

Datenschutz und Sicherheit von Instant-Messaging-Protokollen

a-i3/BSI-Symposium 2017

21.04.17

Faculty of Electrical Engineering and Information Technology
Chair for Network and Data Security
Paul Rösler

Agenda

- Motivation
- Introduction to Technical Concepts
- Protocol Weaknesses
- Conclusion

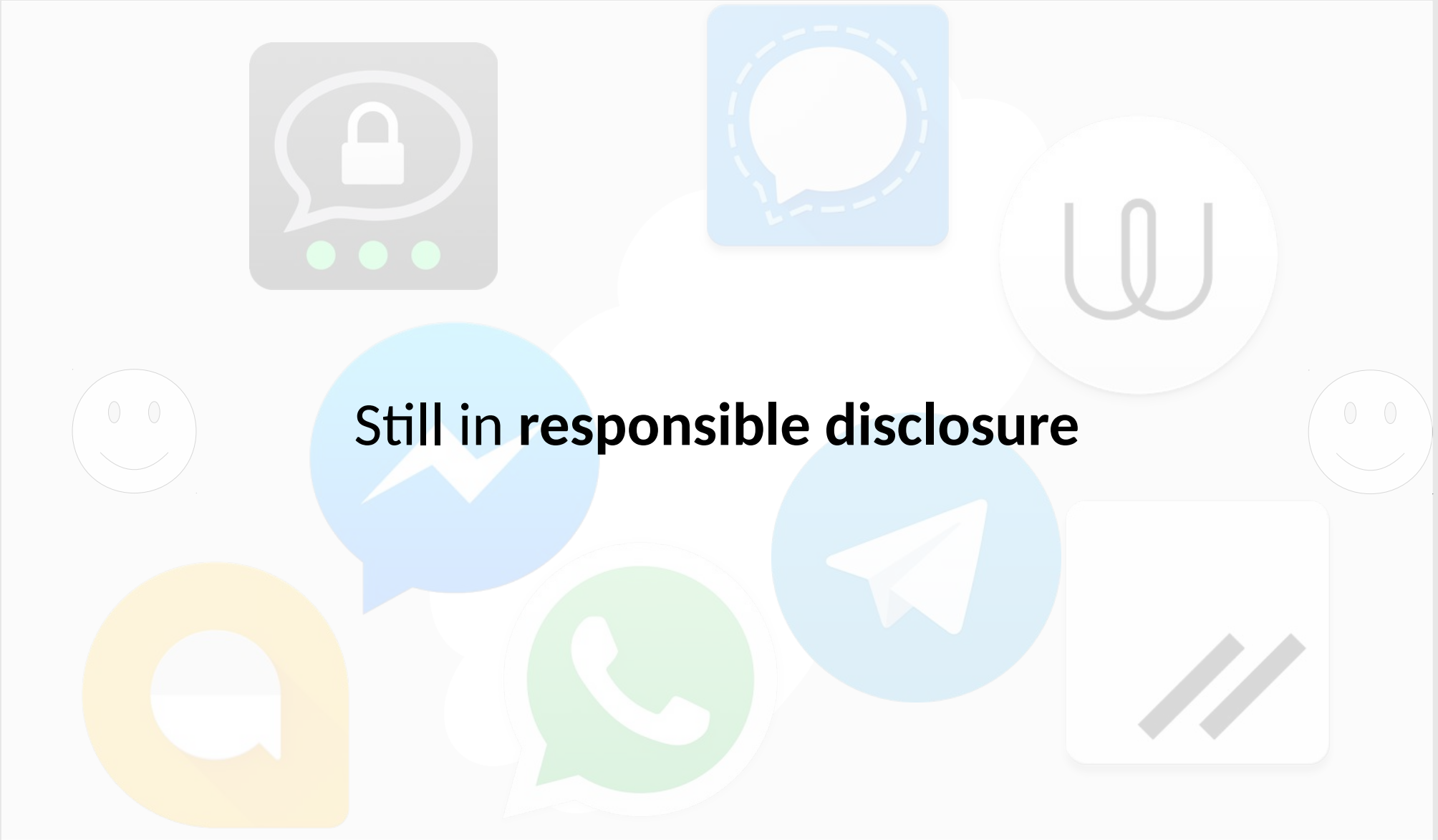
Chair for Network and Data Security
Prof. Dr. Jörg Schwenk

Instant Messaging

Chair for Network and Data Security
Prof. Dr. Jörg Schwenk

Instant Messaging

Instant Messaging



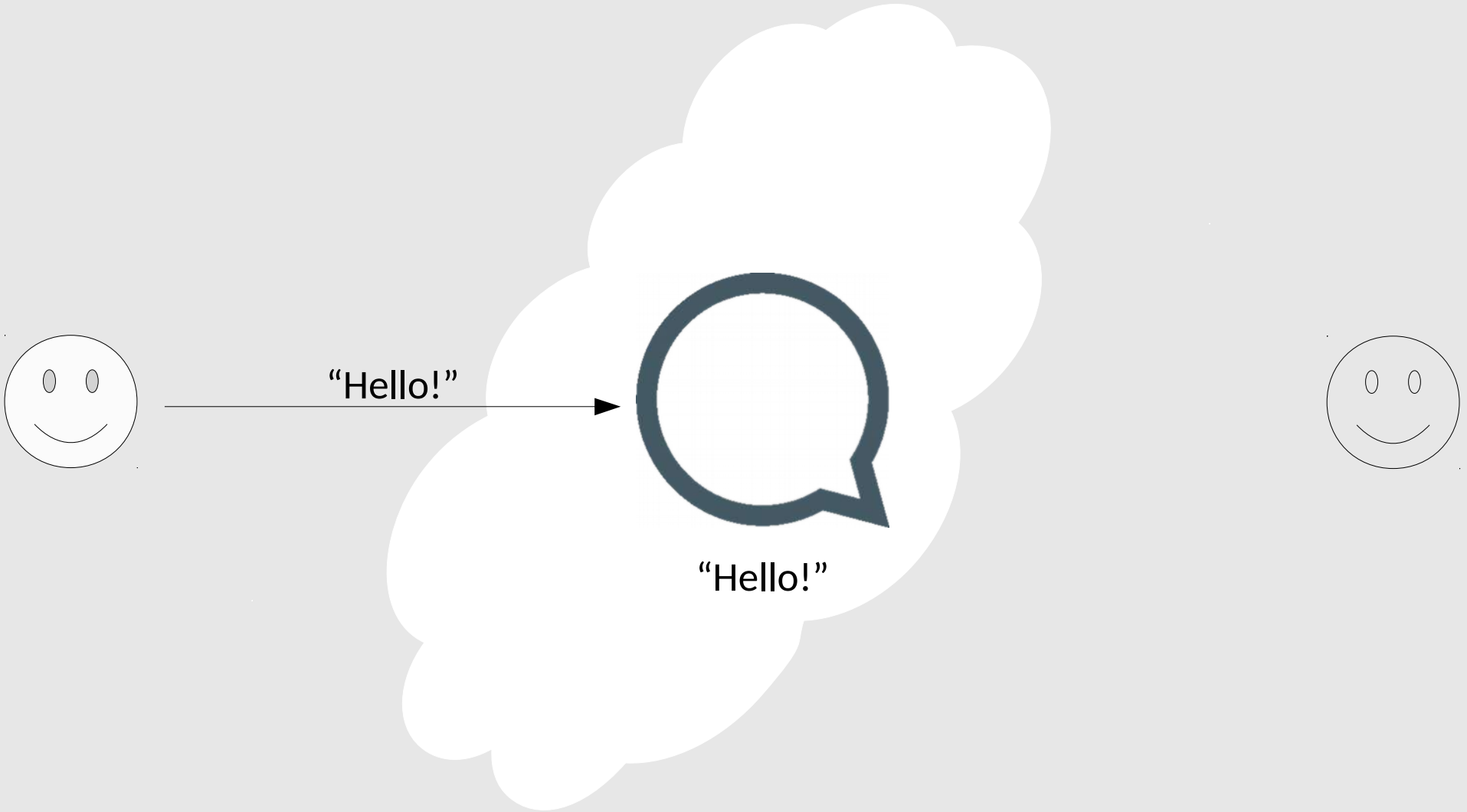
Still in **responsible disclosure**

Chair for Network and Data Security
Prof. Dr. Jörg Schwenk

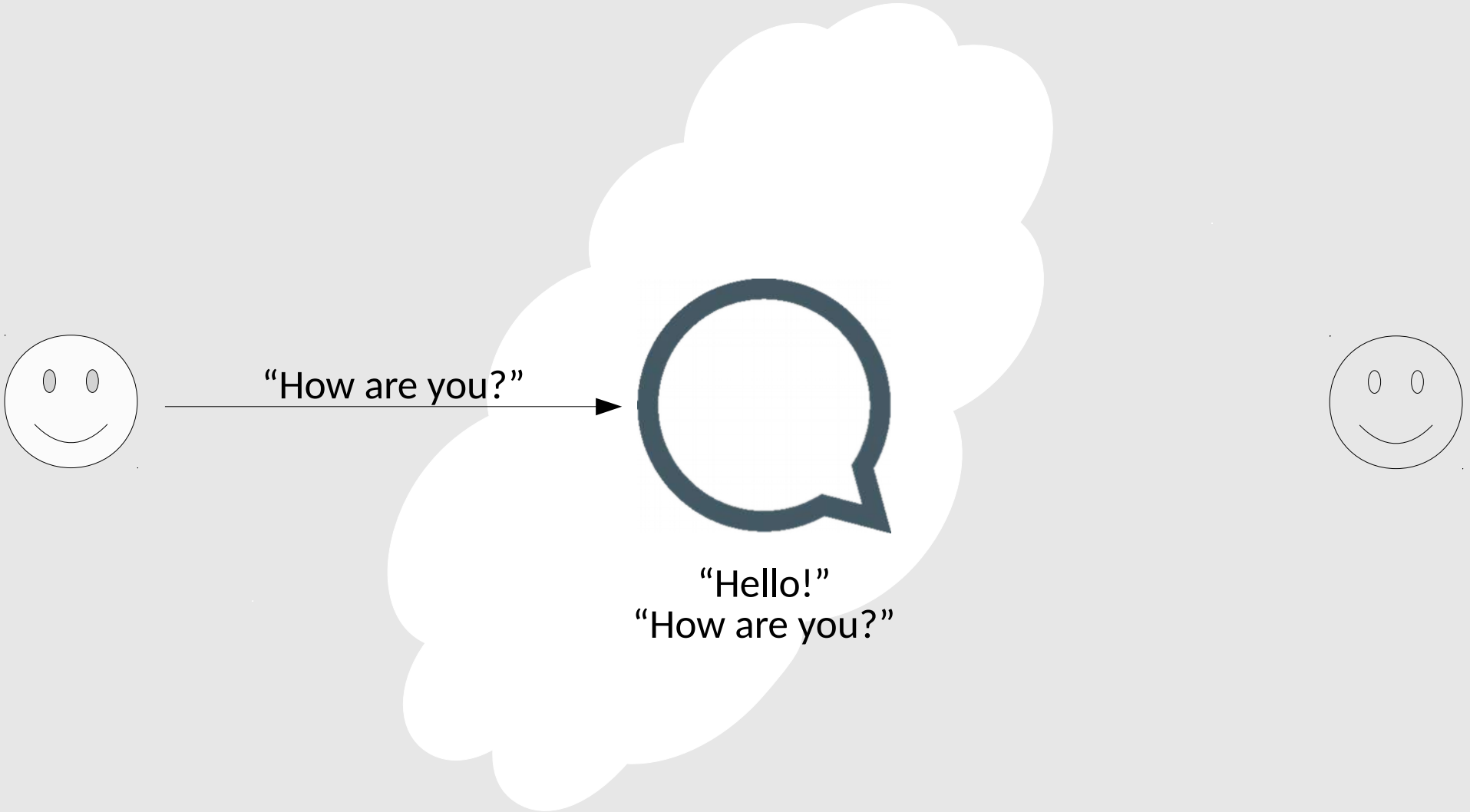
Instant Messaging

Instant Messaging

Instant Messaging



Instant Messaging



Instant Messaging

Chair for Network and Data Security
Prof. Dr. Jörg Schwenk

Instant Messaging

Instant Messaging

“Hello!”

“How are you?”

Motivation

Target:
- Security
- Privacy

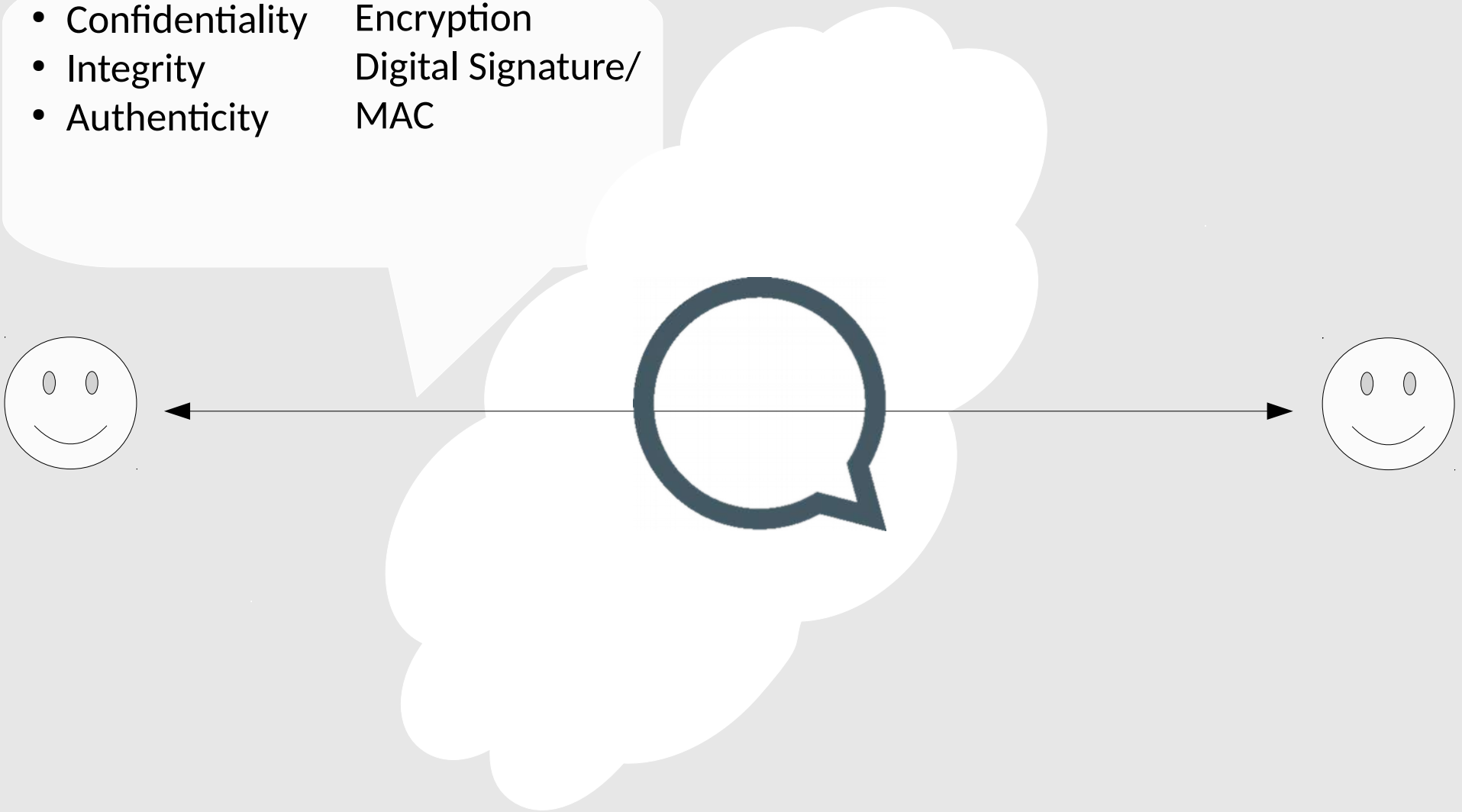
Not target:
- Safety

Motivation

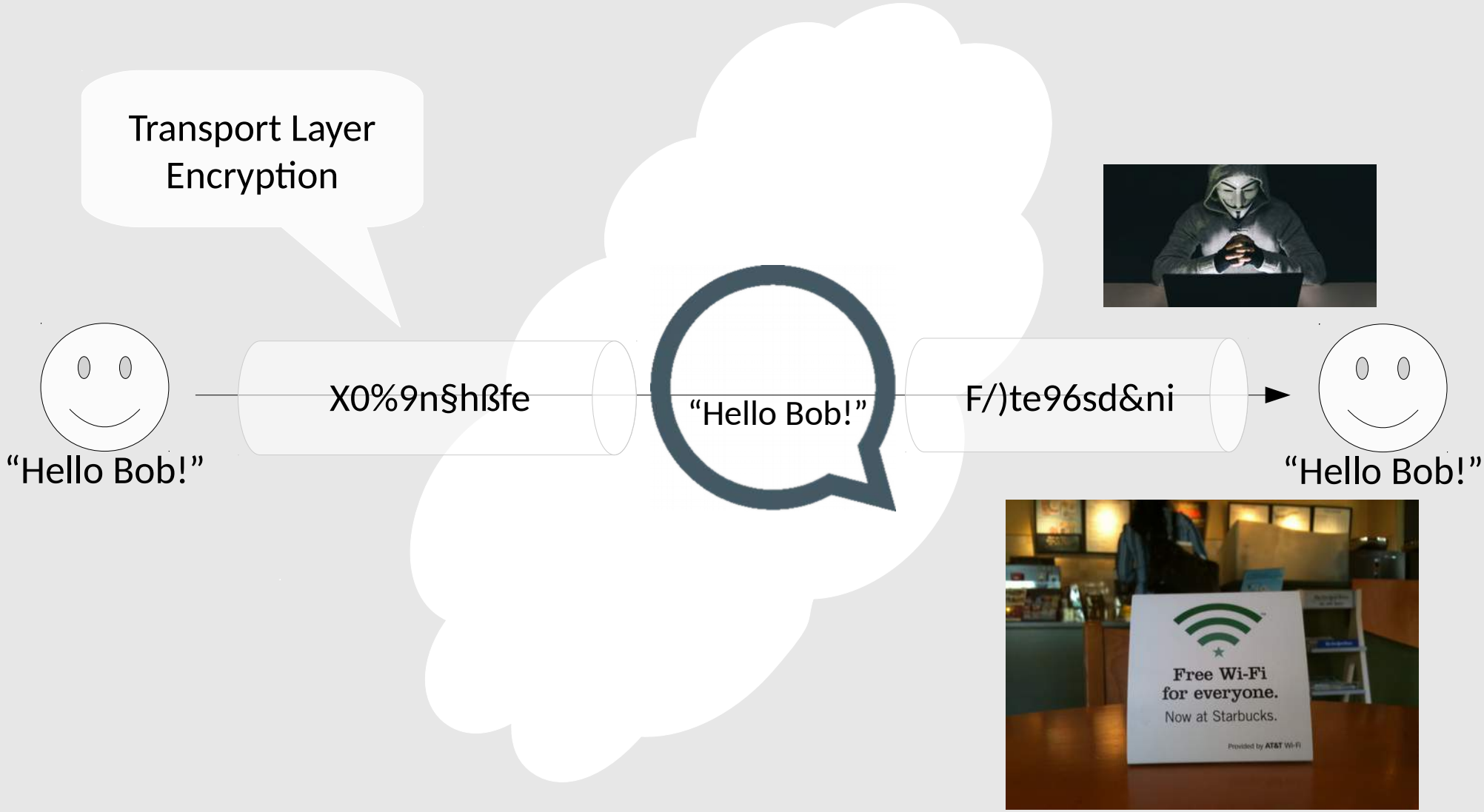
- Confidentiality
- Integrity
- Authenticity
  + Availability

Motivation

- Confidentiality — Encryption
- Integrity — Digital Signature/
- Authenticity — MAC



Motivation


Transport Layer Encryption
X0%9n§hßfe
“Hello Bob!”
“Hello Bob!”
F/)te96sd&ni
“Hello Bob!”
Free Wi-Fi
for everyone.
Now at Starbucks.

Motivation

X0%9n§hßfe

5$c2mqa1r

F/)te96sd&ni

“Hello Bob!”

“Hello Bob!”

Transport Layer Encryption
+
End-to-End Encryption

Chair for Network and Data Security
Prof. Dr. Jörg Schwenk

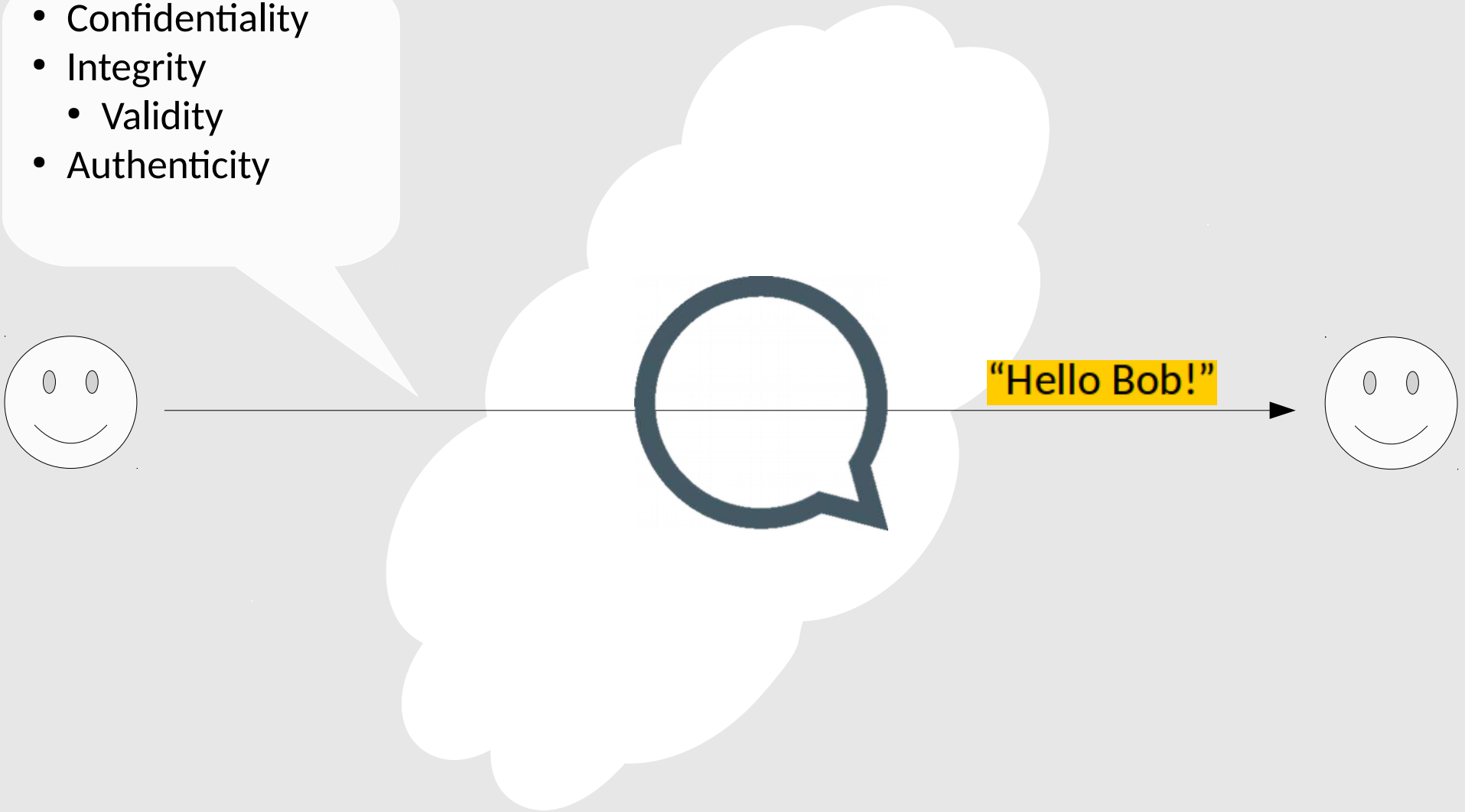
Introduction to Technical Concepts

- Confidentiality ✓
- Integrity ✓
- Authenticity ✓

Chair for Network and Data Security
Prof. Dr. Jörg Schwenk

Introduction to Technical Concepts

- Confidentiality
- Integrity
  - Validity
- Authenticity

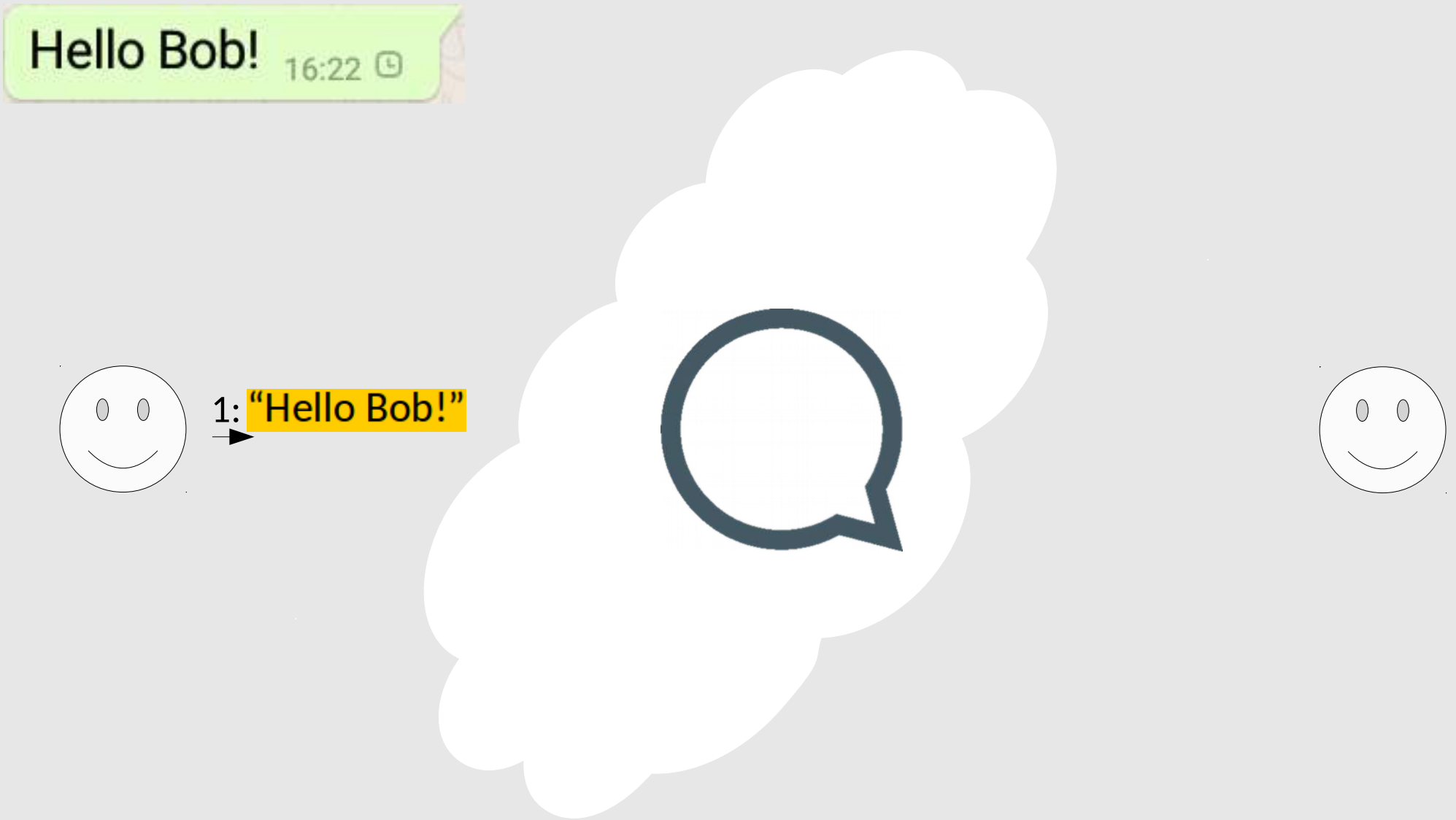


Chair for Network and Data Security
Prof. Dr. Jörg Schwenk

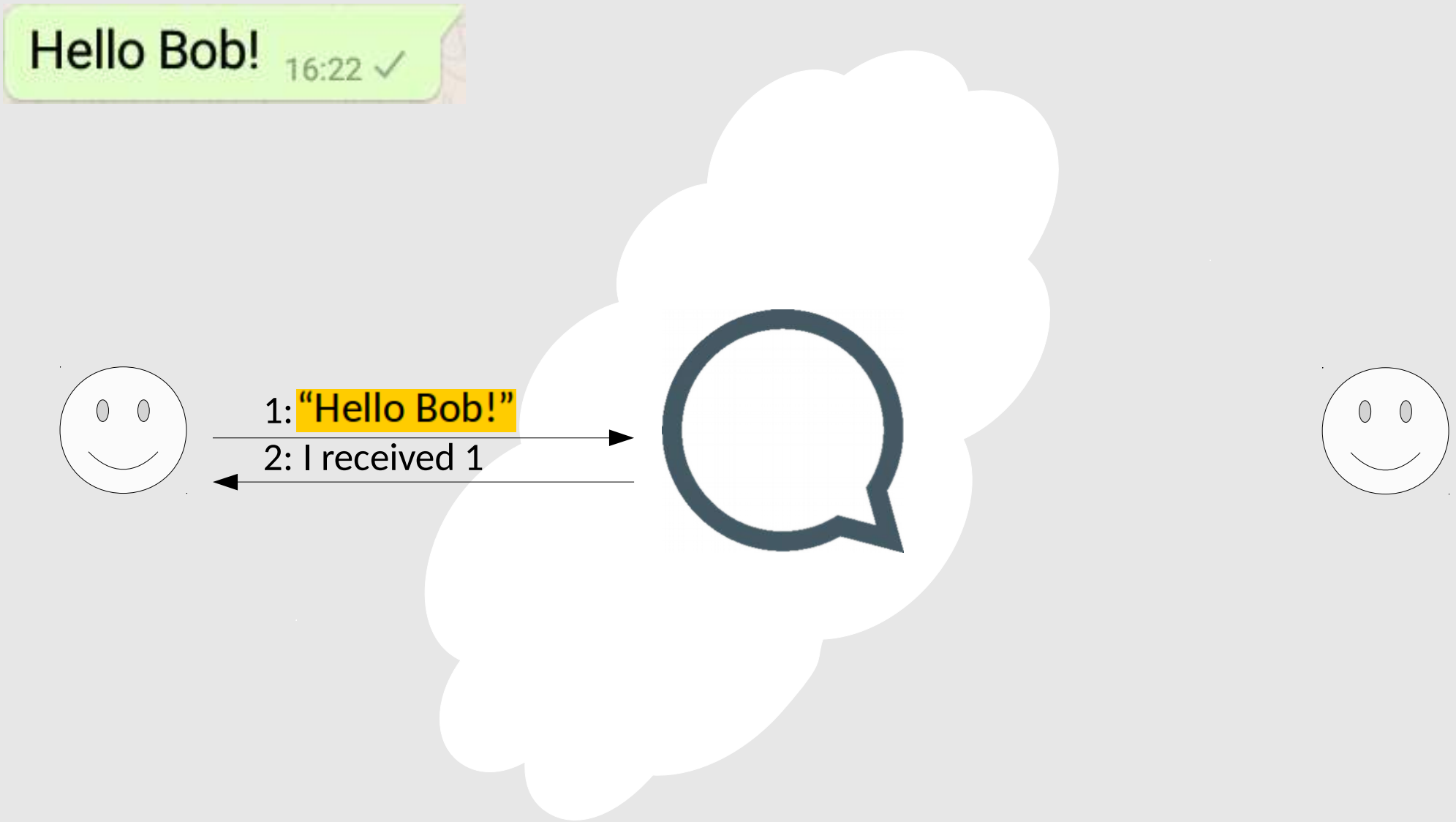
Introduction to Technical Concepts

- Confidentiality
- Integrity
  - Validity
- Authenticity

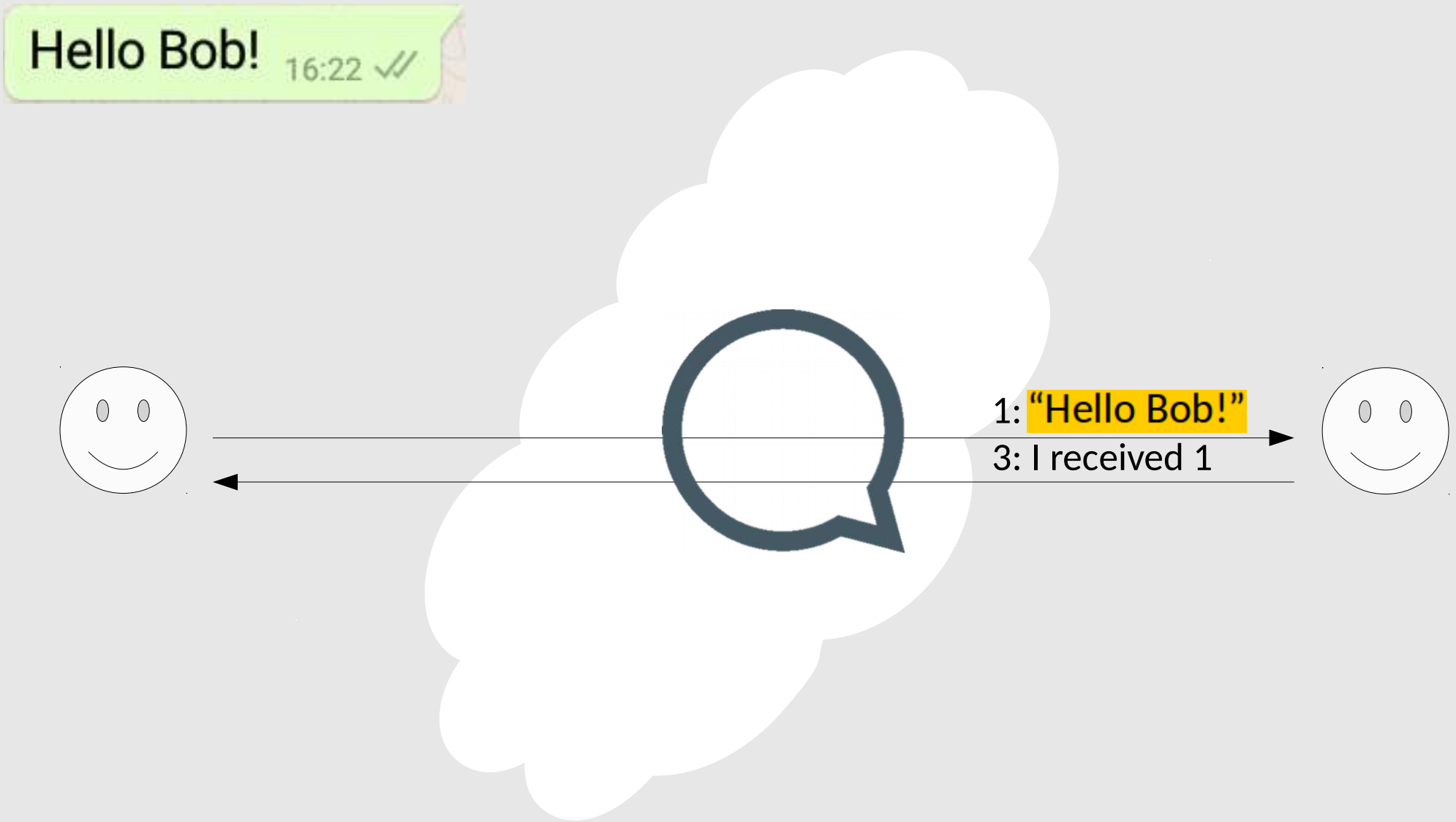
Protocol Weaknesses



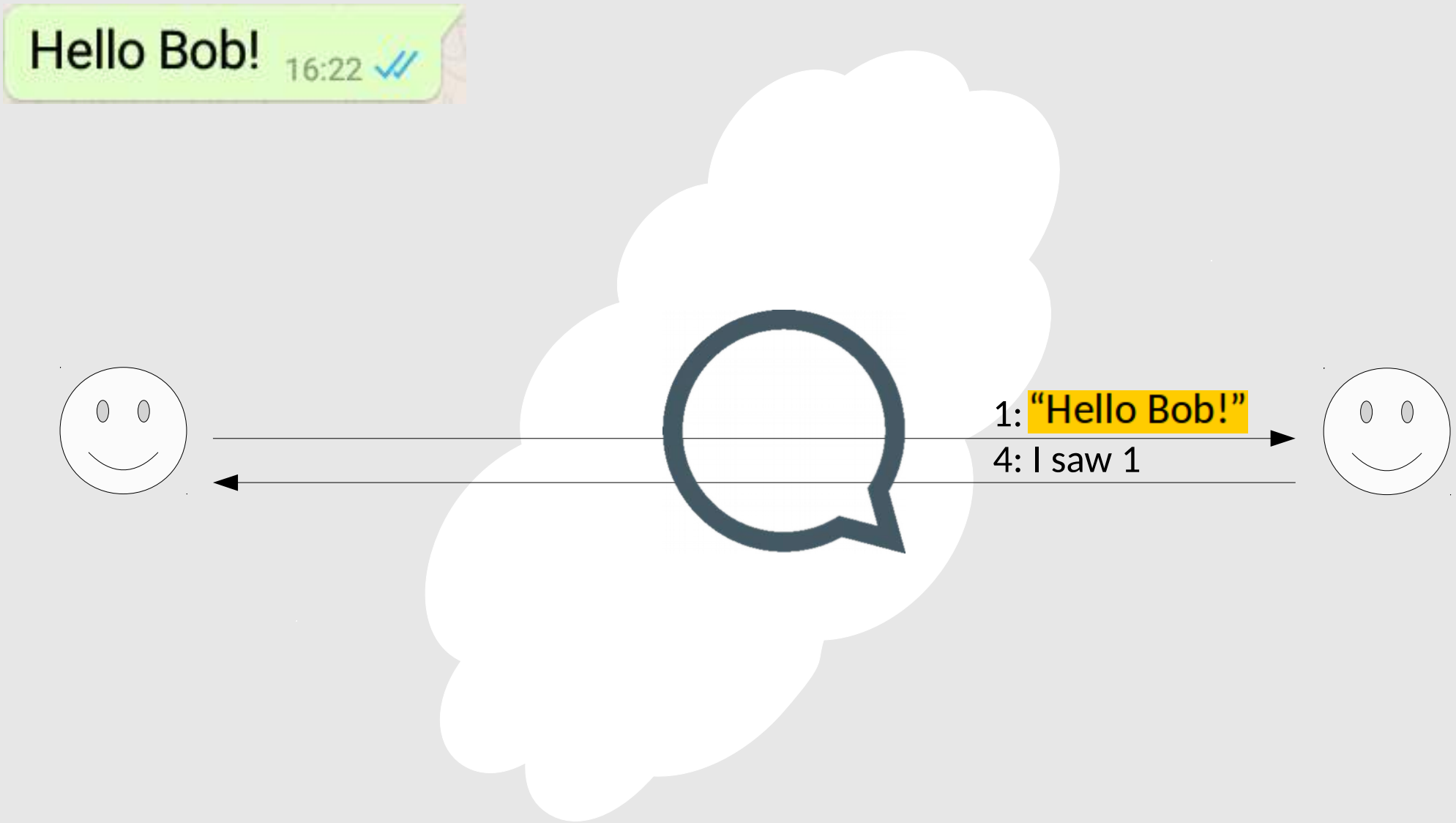
Protocol Weaknesses



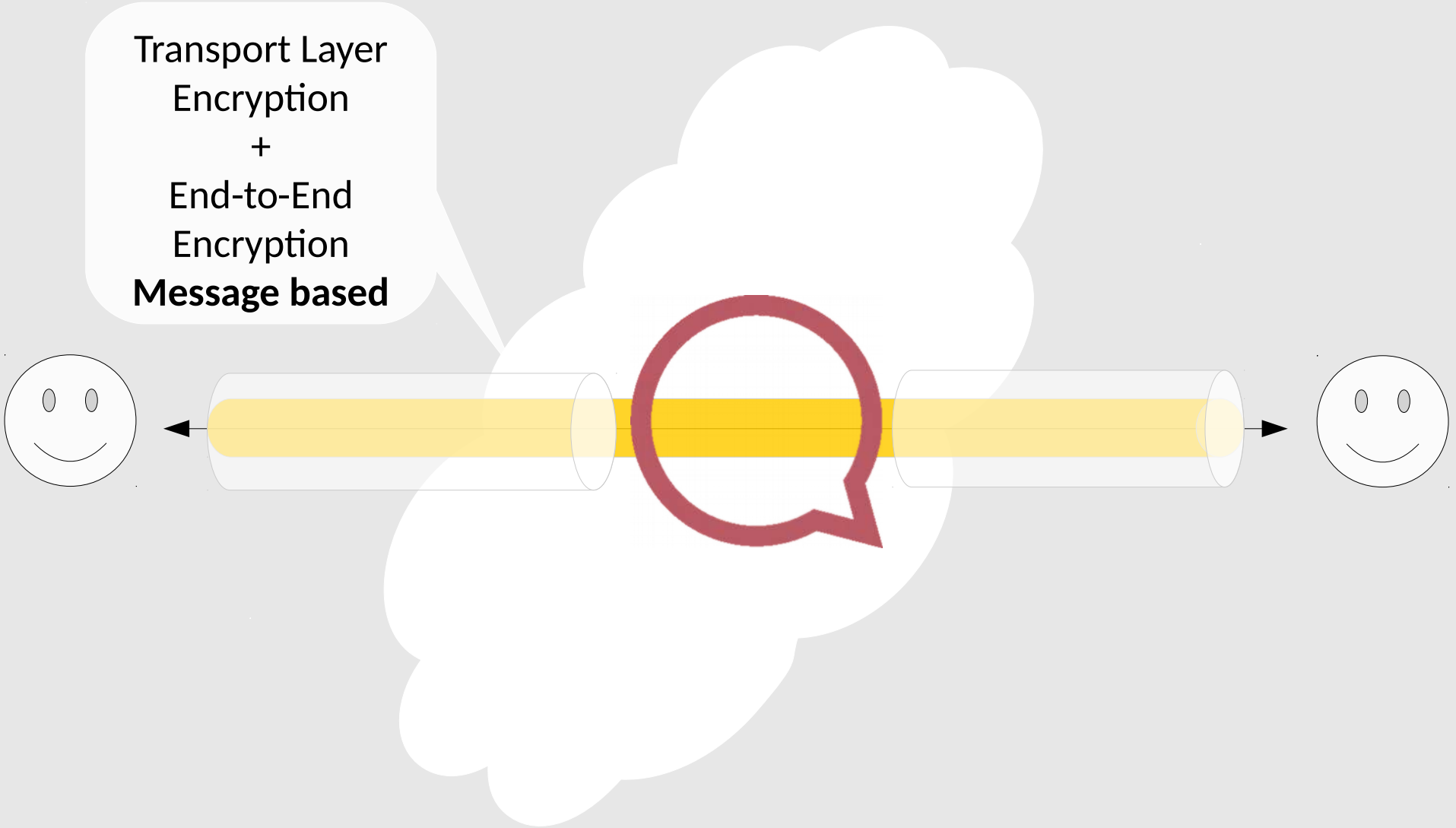
Protocol Weaknesses



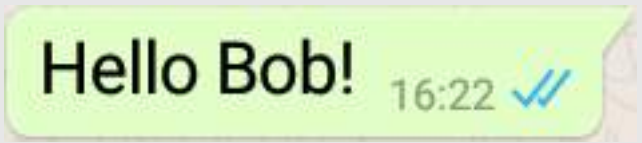
Protocol Weaknesses



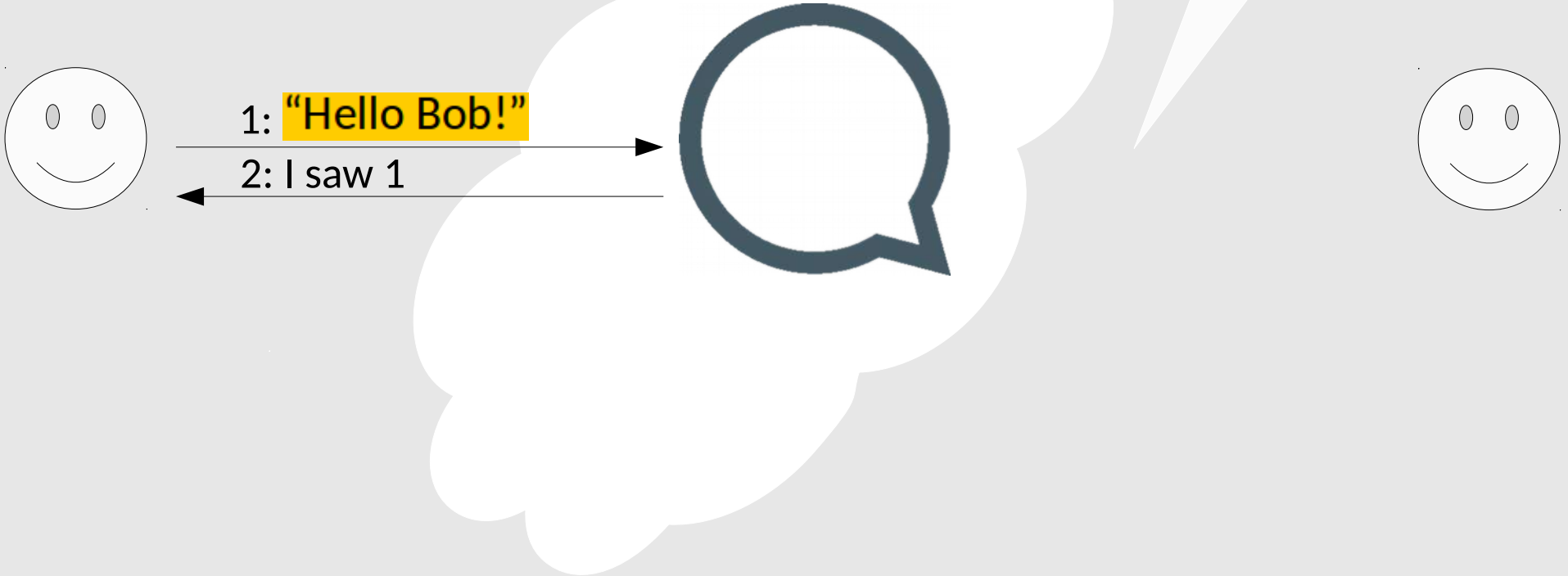
Motivation


Transport Layer
Encryption
+
End-to-End
Encryption
Message based

Protocol Weaknesses



All analyzed protocols vulnerable



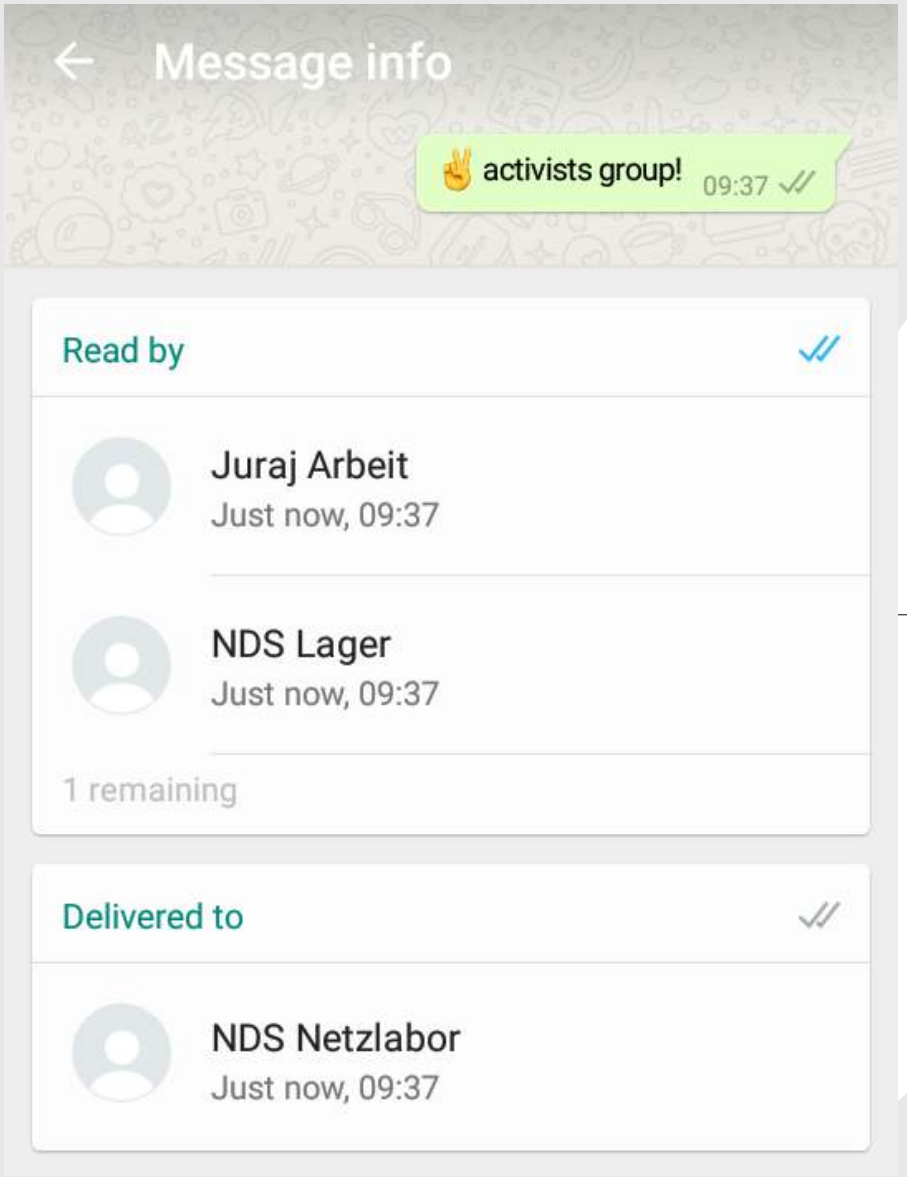
Chair for Network and Data Security
Prof. Dr. Jörg Schwenk

Introduction to Technical Concepts

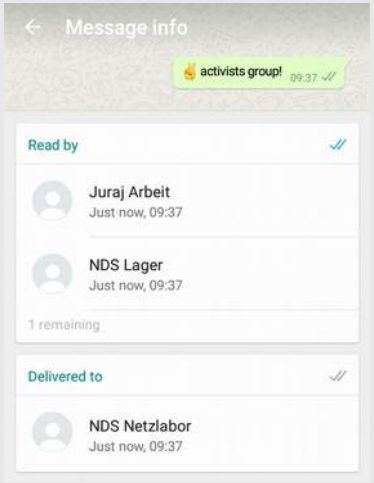
- Confidentiality
- Integrity
  - Validity
- Authenticity

Chair for Network and Data Security
Prof. Dr. Jörg Schwenk

Introduction to Technical Concepts

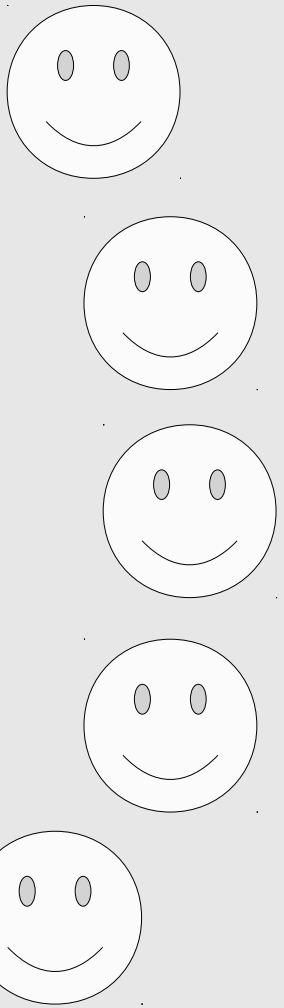


Protocol Weaknesses



1: "✌ activists group!"

2..n: Alice, Bob, ... saw 1



All analyzed protocols vulnerable

Chair for Network and Data Security
Prof. Dr. Jörg Schwenk

Introduction to Technical Concepts

- Confidentiality
  - Closeness
- Integrity
  - Validity
- Authenticity

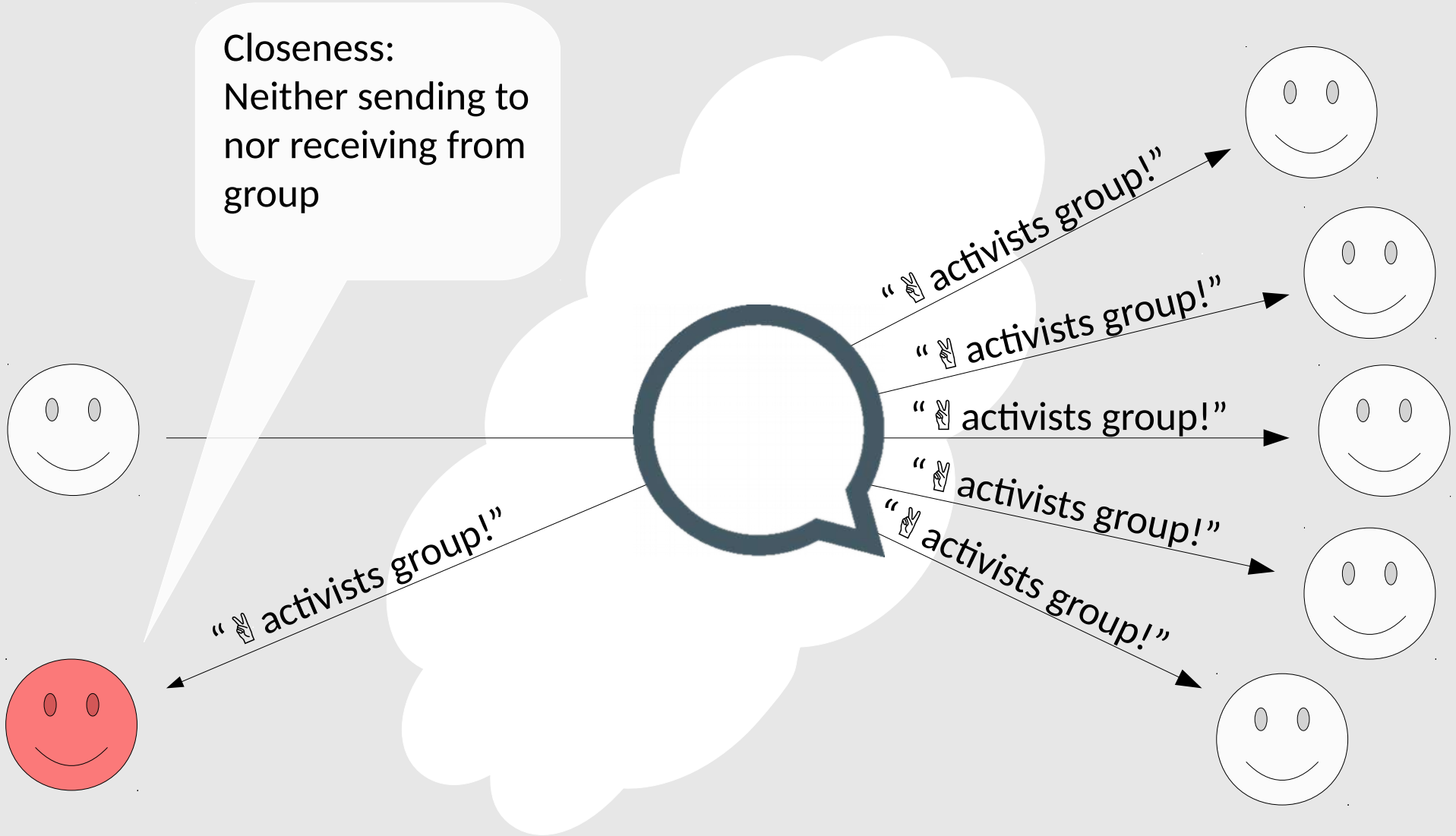
Chair for Network and Data Security
Prof. Dr. Jörg Schwenk

Introduction to Technical Concepts

- Confidentiality
  - Closeness
- Integrity
  - Validity
- Authenticity

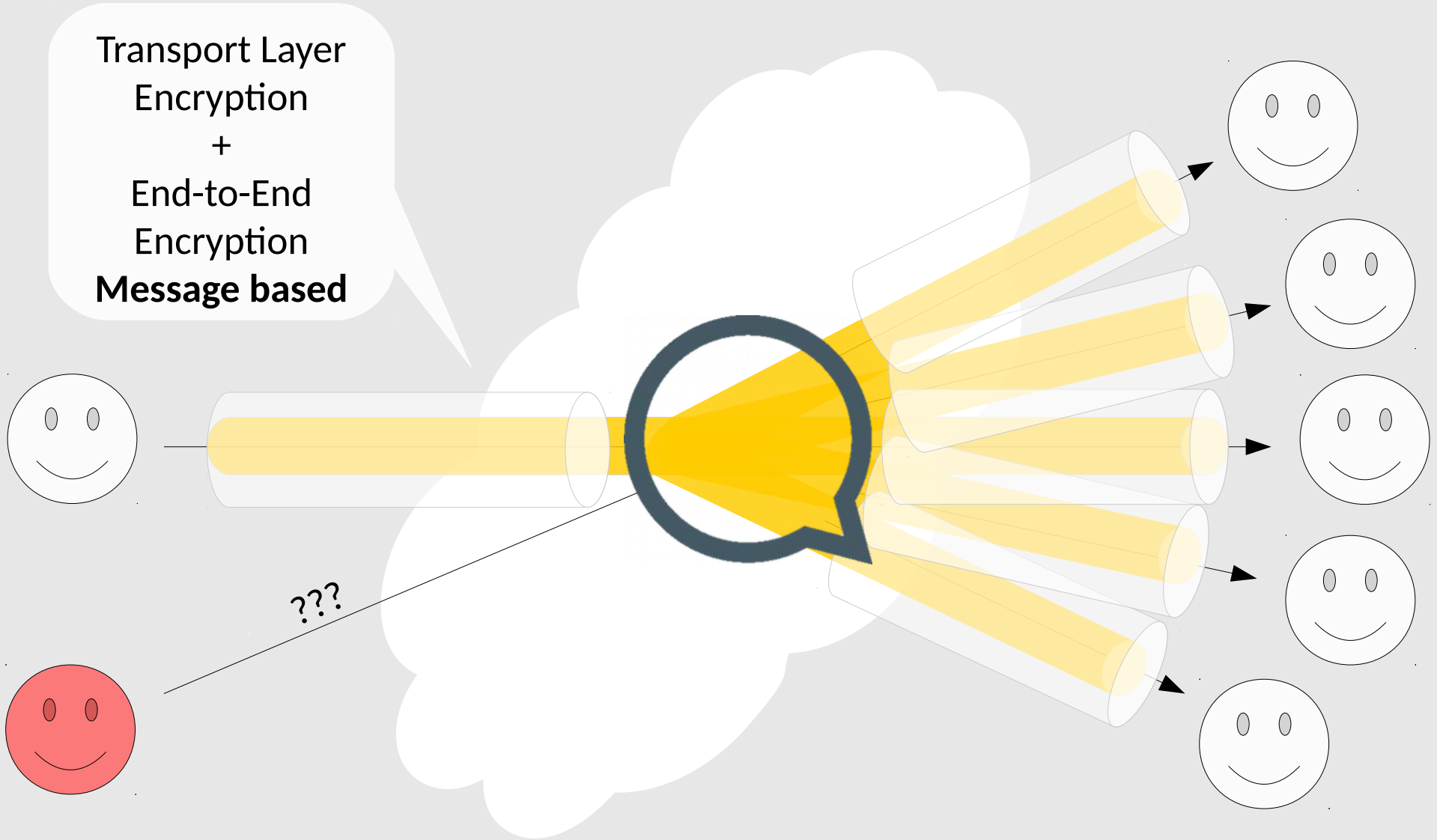
Chair for Network and Data Security
Prof. Dr. Jörg Schwenk

Introduction to Technical Concepts

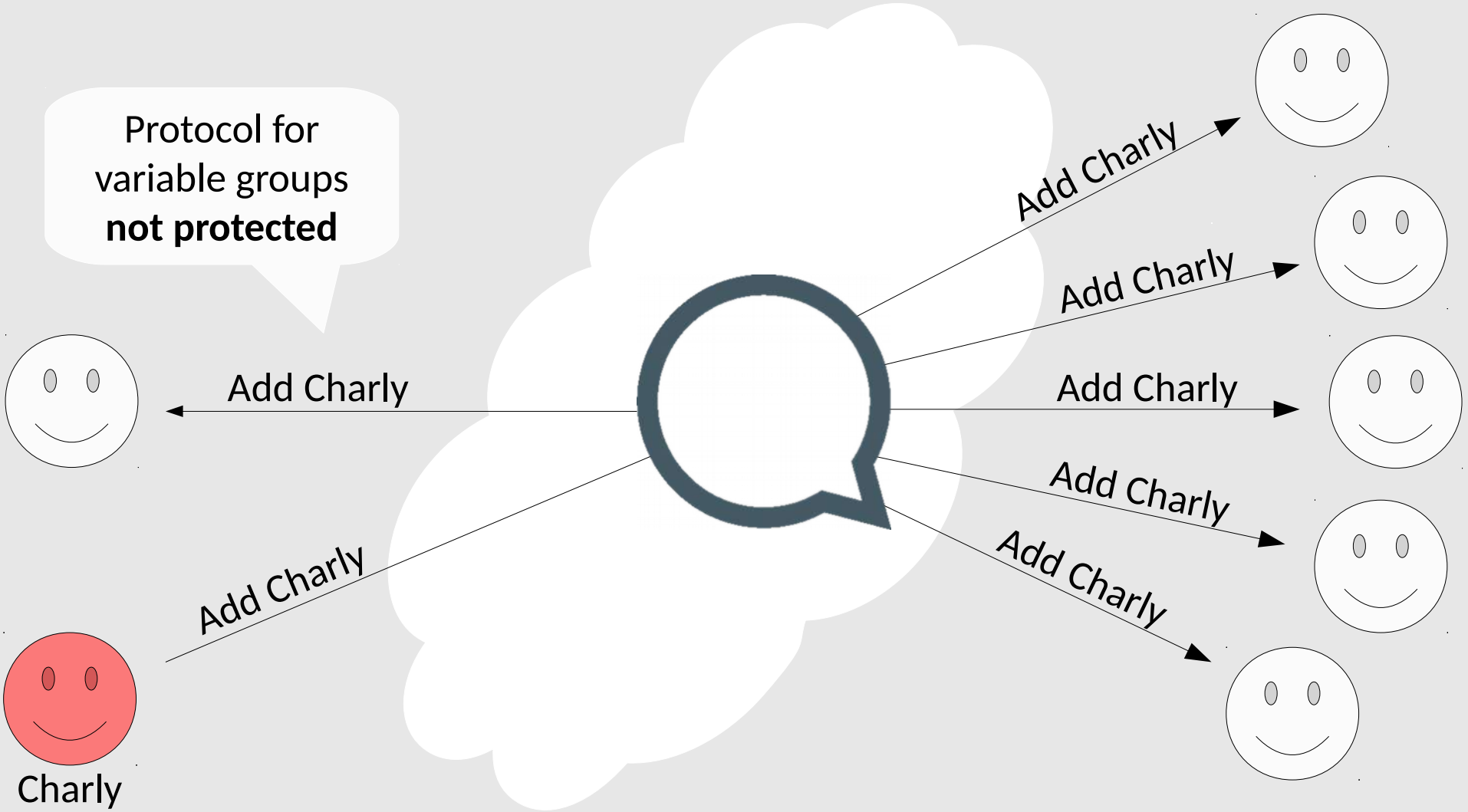


Chair for Network and Data Security
Prof. Dr. Jörg Schwenk

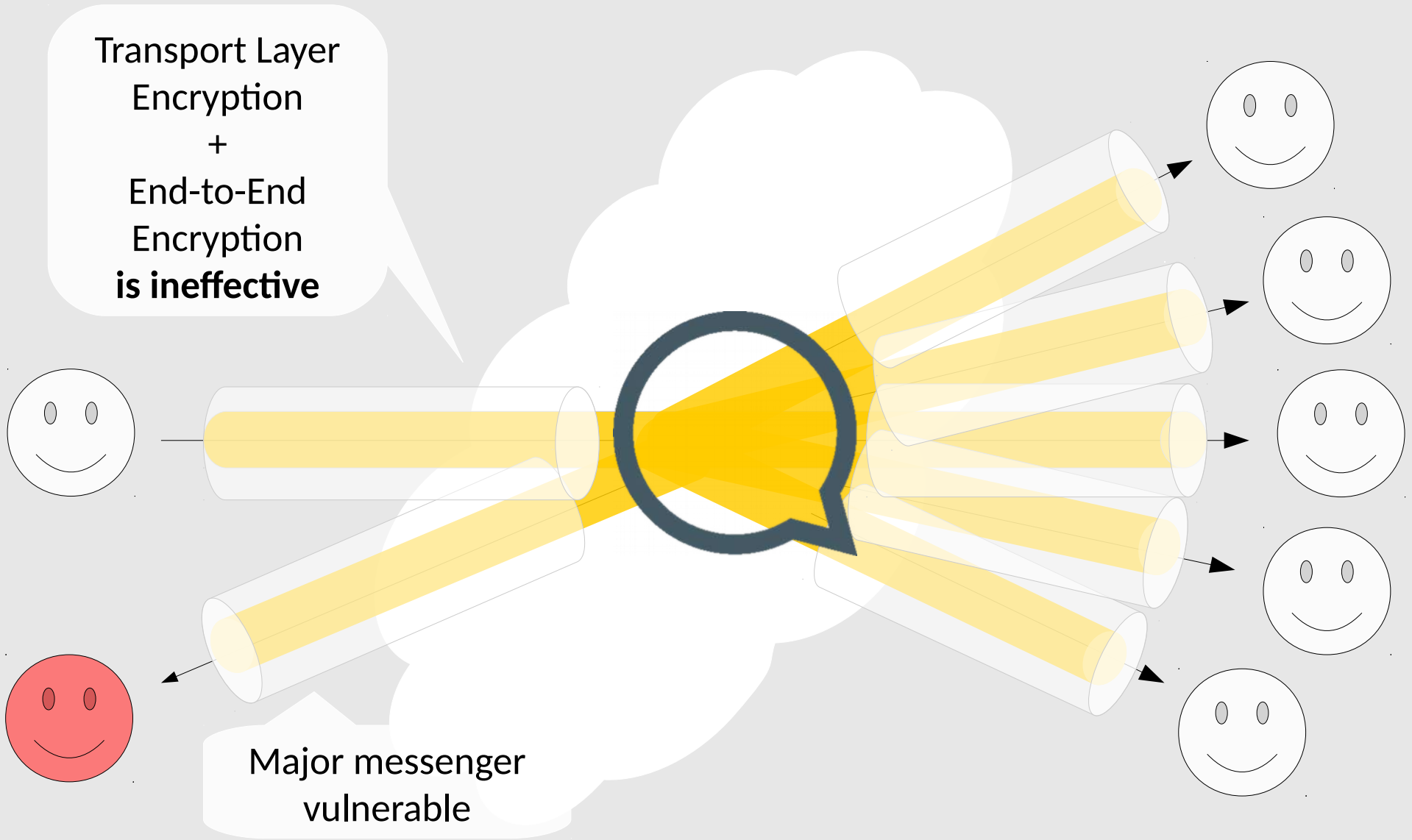
Introduction to Technical Concepts



Protocol Weaknesses

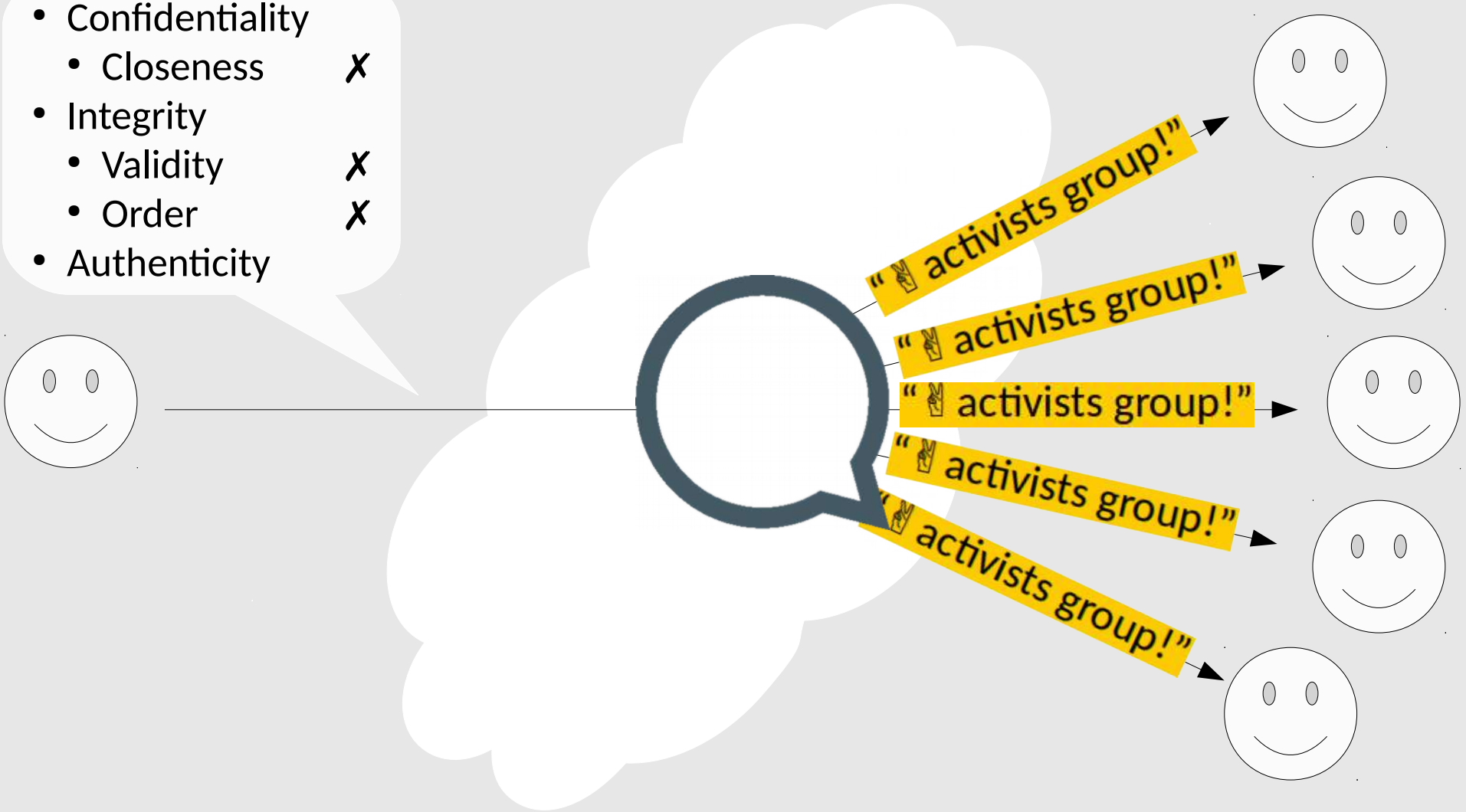


Protocol Weaknesses

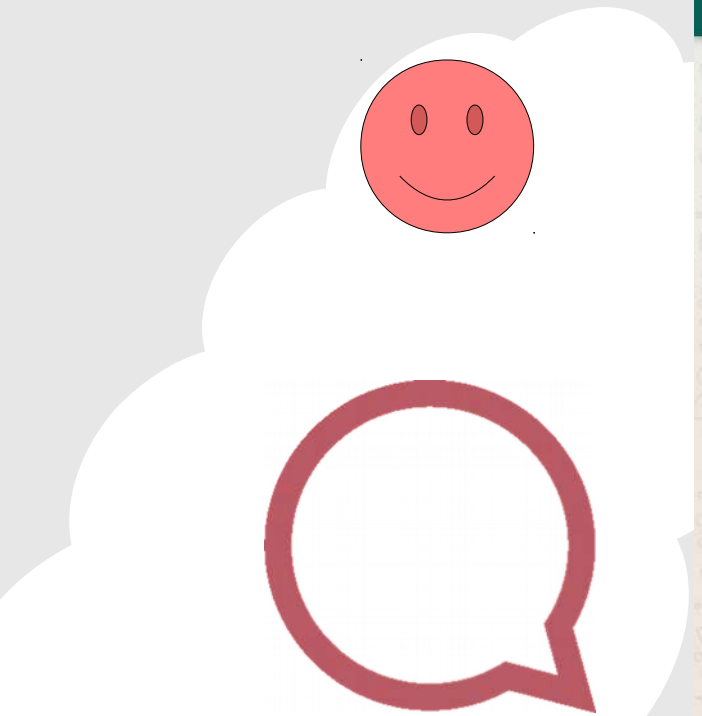


Protocol Weaknesses

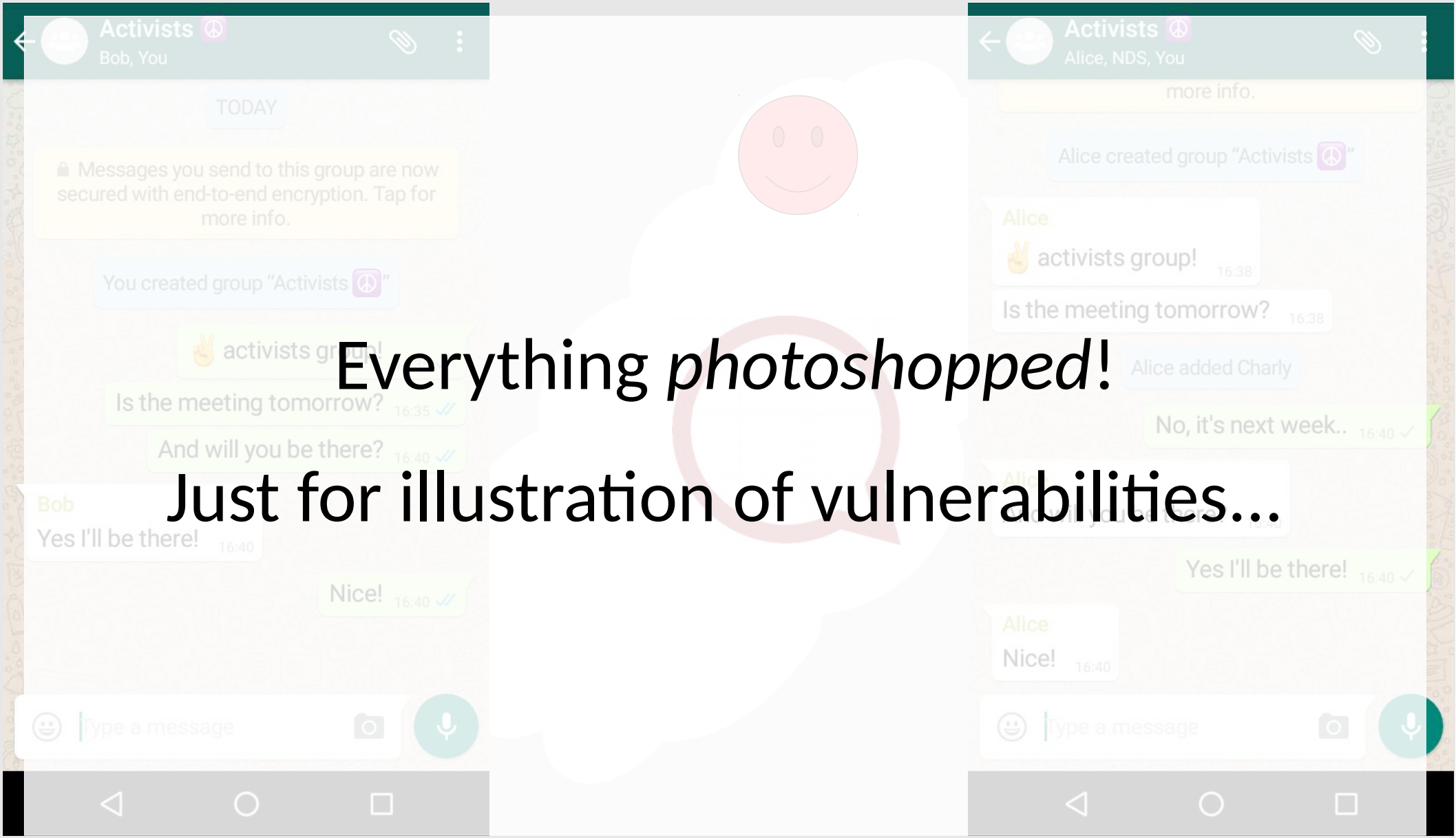
- Confidentiality
  - Closeness ✗
- Integrity
  - Validity ✗
  - Order ✗
- Authenticity



Protocol Weaknesses



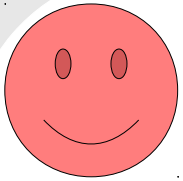
Protocol Weaknesses



Everything *photoshopped*!

Just for illustration of vulnerabilities…

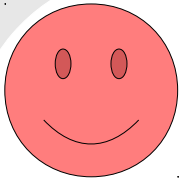
Protocol Weaknesses



Alice thinks:

- Meeting is tomorrow
- Bob will be there

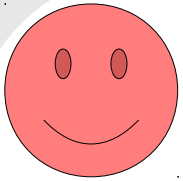
Protocol Weaknesses



Bob thinks:

- Meeting is next week
- Alice knows that meeting is next week
- Alice will be there
- Some Charly was added

Protocol Weaknesses



Attacker knows:

- Bob's meeting is next week
- Alice' meeting is not next week

Conclusion

- Confidentiality
  - Closeness ✗
- Integrity
  - Validity ✗
  - Order ✗
- Authenticity

We cannot trust
- The transcript
- That all members trustworthy

Provider can
- Intercept and eavesdrop
- Drop messages
- Reorder messages
- Send to groups

Conclusion

- Confidentiality
  - Closeness ✗
- Integrity
  - Validity ✗
  - Order ✗
- Authenticity

We cannot trust
- The transcript
- That all members trustworthy

End-to-end Encryption

≠

Security

Provider can
- Intercept and eavesdrop
- Drop messages
- Reorder messages
- Send to groups

RUHR-UNIVERSITÄT BOCHUM

RUB

Datenschutz und Sicherheit von Instant-Messaging-Protokollen

a-i3/BSI-Symposium 2017

21.04.17

Faculty of Electrical Engineering and Information Technology
Chair for Network and Data Security
Paul Rösler

Thank you for your attention!

Any questions?