A look into the Mobile Messaging Black Box

33rd Chaos Commmunication Congress #33c3

Roland Schilling `@NerdingByDoing`
Frieder Steinmetz `@twillnix`

November 20, 2016

Hamburg University of Technology
Security in Distributed Applications

Introduction

Messaging - An Analogy

- You're at a party
- Friend approaches you and needs to tell you something in private
- What do you expect when you say private?
- You enter a separate room, you trust the location
- What does a separate room offer you?
  - Authenticity
  - Integrity
  - Forward Secrecy
  - Future Secrecy
  - Plausible Deniability

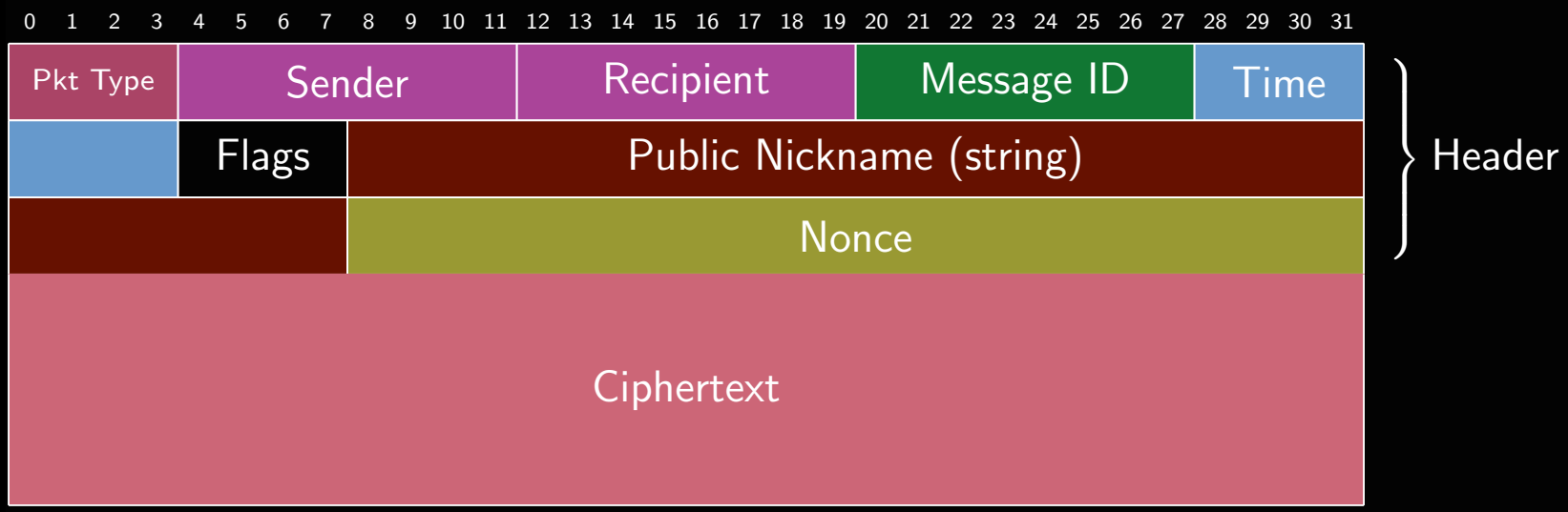
Case Study - Signal

Reverse-Engineering Threema

Enter Threema

Threema Packet Format

Message Packet (Threema Protocol Layer)

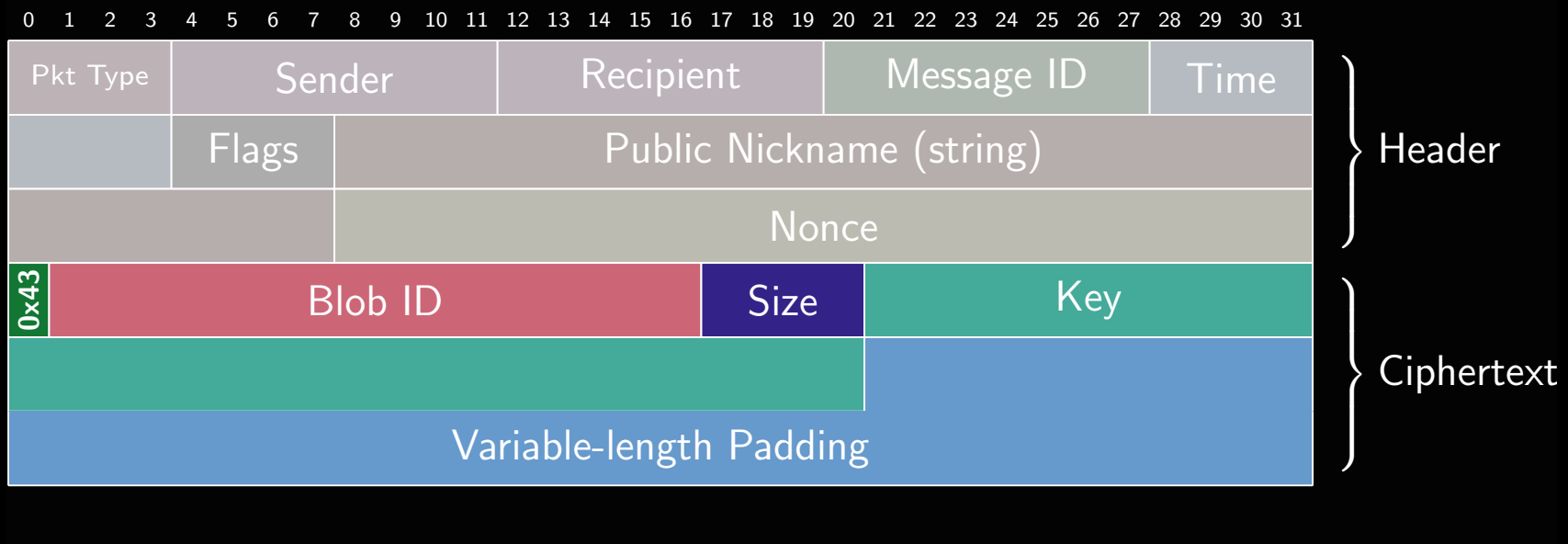


Threema: Special Messages

- Polls
- Images with Caption
  - Case of caption leak found
- Audio Messages
  - Leak Android version
  - Possible stagefright vector

Threema Image Messages

Image Message



Threema Audio Messages

Audio Message