

## Anonymous communication

**Claudia Díaz and Bart Preneel**  
**COSIC group**  
**K.U.Leuven**

## Outline

- ⌘ Introduction: motivation for anonymity
- ⌘ Anonymous communications
- ⌘ The Mix
- ⌘ Mix network topologies
- ⌘ Anonymity metrics
- ⌘ Anonymity control
- ⌘ Conclusions and future work

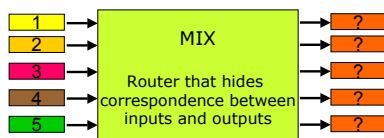
## Introduction

- ⌘ Privacy is not only confidentiality of the information but also not revealing information about who is communicating with whom
- ⌘ Motivation for anonymity
  - ☒ Anonymity is a tool to preserve privacy
  - ☒ If the communication is not anonymous, the anonymity implemented at higher levels is useless in many applications
  - ☒ For many applications (e.g., web browsing) the identity of the user is not needed by the service provider

## Anonymous communication

- ⌘ An anonymous communication network preserves the privacy of the user towards the other end and towards third parties
- ⌘ Building blocks for anonymous communication:
  - ☒ Mixes (Mix networks) -- Onion
  - ☒ P2P models -- Crowds
  - ☒ Multicast protocols -- Hordes

## Mixes



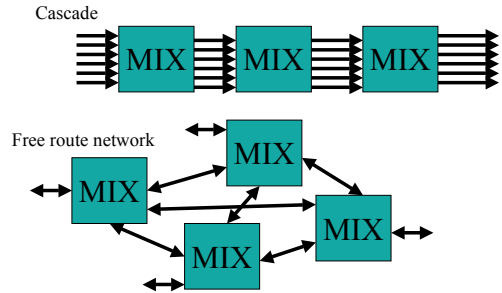
## Mixes

- ⌘ Mixes modify
  - ☒ The appearance of the messages
    - ☒ Encryption
    - ☒ Padding
  - ☒ The flow of messages
    - ☒ Reordering
    - ☒ Delaying
    - ☒ Real-time requirements!

## Mix types

- ⌘ Pool mixes
  - ☒ The mix flushes when a certain condition is fulfilled, it could be reaching a threshold or the expiration of a timeout
  - ☒ The mix may keep a certain amount of messages from one round to the other (to increase the anonymity)
- ⌘ Continuous mixes (stop-and-go)
  - ☒ Messages are delayed following an exponential distribution
  - ☒ The delay is independent of the traffic

## Mix network topologies



## Anonymity metrics

- ⌘ An attacker may be able to obtain probabilistic information about the real initiator of a request by performing traffic analysis on the system
- ⌘ The attack model has to be clearly defined
- ⌘ Metrics based on the information-theoretic concept of entropy (the entropy measures the 'uncertainty')
  - ☒ Depends on: anonymity set size and distribution of probabilities
- ⌘ Sender and recipient anonymity

## Dummy traffic

- ⌘ Fake messages introduced to confuse the attacker
  - ☒ Created by mixes and/or users; discarded by mixes
  - ☒ Dummies improve the anonymity (by making more difficult the traffic analysis)
  - ☒ Very useful on low traffic conditions
- ⌘ Example: Pinenet

## Dummy traffic

- ⌘ But... dummies have a cost!
  - ☒ Find the best tradeoff (anonymity/cost)
- ⌘ Open questions:
  - ☒ what is the best distribution of dummies?
  - ☒ Which route length should they have?
  - ☒ Should it depend on real traffic?
- ⌘ Dummy traffic may also be used to detect active attacks

## Anonymity control

- ⌘ What if something goes wrong?
  - ☒ Anonymity control should be implemented in order to comply with legal and government requirements
  - ☒ Honest users should remain anonymous while misbehaving users should be identified
  - ☒ Model for anonymity control:
    - ☒ Controlled unconditional anonymity
    - ☒ User-controlled conditional anonymity
    - ☒ Trustee-controlled conditional anonymity

## Conclusions

- ⌘ Motivation for anonymous communication
- ⌘ Description of the main issues related to anonymous communication
  - ☒ Mixes, mix networks
  - ☒ Anonymity metrics
  - ☒ Dummy traffic
  - ☒ Anonymity control

## Future work

- ⌘ Mixes:
  - ☒ What is the best mix design?
- ⌘ Anonymity metrics:
  - ☒ Study the impact of dummy traffic on the anonymity
  - ☒ Find metrics that compute the end-to-end anonymity
- ⌘ Dummy traffic
  - ☒ what is the best dummy traffic policy?
- ⌘ Anonymity control
  - ☒ Find practical and secure designs