Intersection Attacks on Web-Mixes: Bringing the Theory into Praxis

Dogan Kesdogan, Lexi Pimenidis, and Tobias Kölsch

RWTH AACHEN

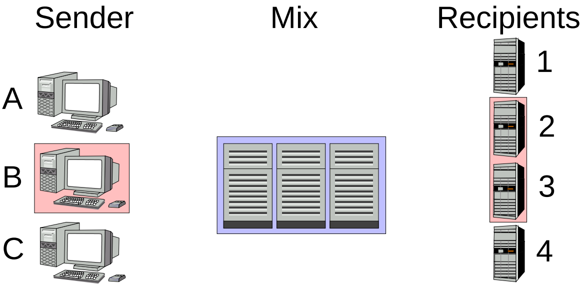
Overview

- Motivation
- Model & Attacks
- Environment
- Results
- Conclusion

Motivation

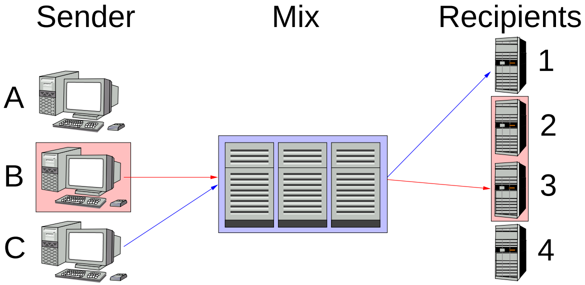
- Most evaluation based on simulations
- No knowledge about accuracy of model
- Unrealistic assumptions
- Real traffic as basis for evaluation

Anonymity Sets



Observation

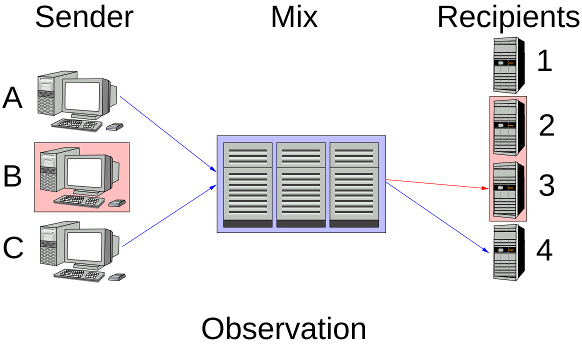
Anonymity Sets



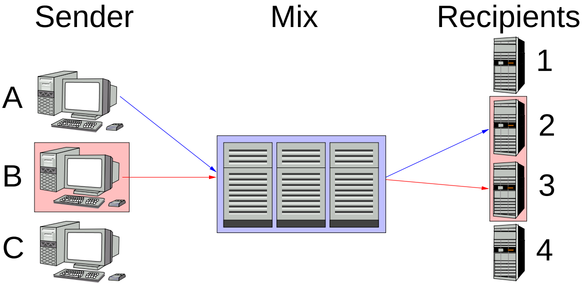
Observation

1 3

Anonymity Sets



Anonymity Sets



Observation

2 3

Attacks on Anonymity Sets

- Contextual attacks
- Based on recurrent user behavior
- Repeated observations
- Disclosure attack
- Hitting set attack
- Estimation of peer partners

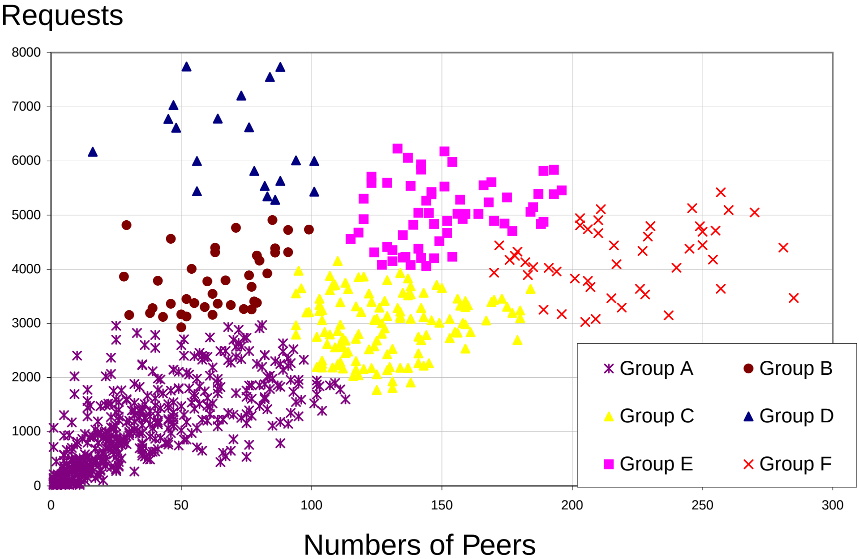
Environment

- Proxy logs of the RWTH-Aachen
  - Much web traffic included
  - Single users
  - Compound users behind one IP
- Real traffic pattern
- Preprocess files
- Simulate mix
  - Pick user
  - Pick period
  - Create anonymity sets

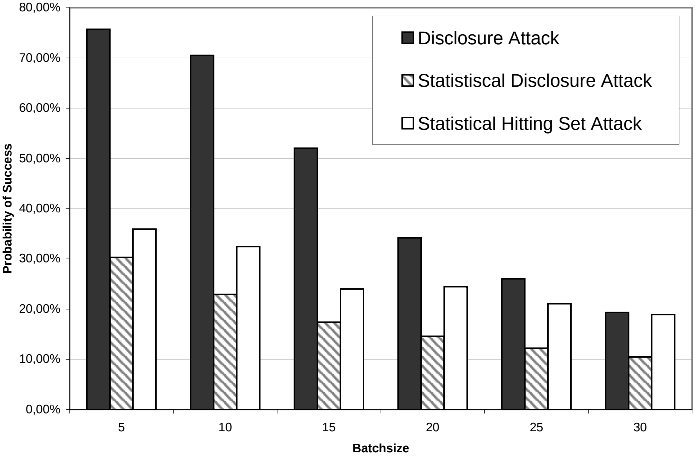
Environment

- Proxy logs of the RWTH-Aachen
  - Much web traffic included
  - Single users
  - Compound users behind one IP
- Real traffic pattern
- Preprocess files
- Simulate mix
  - Pick user
  - Pick period
  - Create anonymity sets

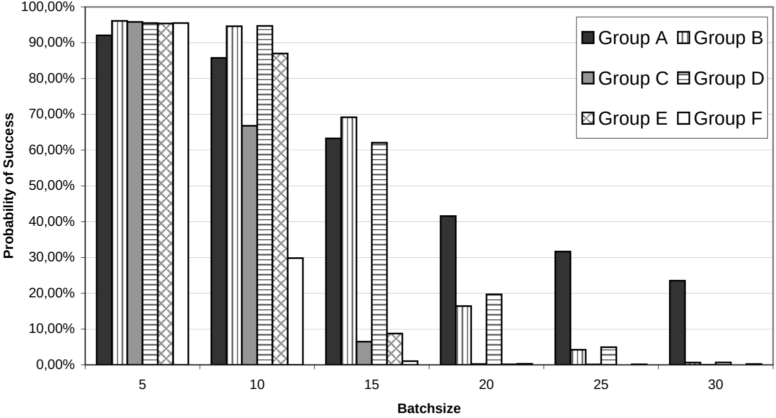
Classification of Users



Results: Comparison of Attacks



Results: Probability of Success



Evaluation

- Errors
- Error depends on type of user
- User behavior badly simulated
  - Results of earlier experiments only partly confirmed
  - Strong variations of page lookup frequency
  - 60% of pages accessed less than 10 times

Conclusion & Further Research

- Simulation of users not precise
- Attacks not as suited for real traffic
  - Some better than others
- Models of user behavior
- Develop new attacks
- Develop protection methods