

Controlled Anonymous Connections

Claudia Díaz -- COSIC (KULeuven)

5th APES Workshop

23/11/2004

Overview

- ❑ Introduction
 - ❑ Research and contributions for anonymous connections
 - ❑ Anonymity Requirements
 - ❑ Anonymity control at communication layer
 - ❑ Building block: anonymous communication infrastructure
 - ❑ Model for controlled anonymous connections
 - ❑ Evaluation of anonymous connection systems
 - ❑ Conclusions and Future Work
-
- ❑ Demo MIXimulator
-

Introduction

- Anonymous Connections (-> Anonymous Communication Systems)
 - Unlinkability of inputs/outputs
 - Anonymous Communication Infrastructure
 - Real-time / application independent
 - Application
 - Anonymous web browsing (Anonymizer: anonymous towards recipient)
 - Anonymous email system (Mixmaster: anonymous towards global passive attackers)
 - Building block
 - Internet communication is traceable
 - IP numbers / other information is visible to the recipient and to observers
 - Anonymous applications cannot be implemented on top of non anonymous communication layers
-

Research Contributions (1)

- “Anonymous communication” (Díaz and Preneel, WHOLES’04)
 - Overview of the state-of-the-art of anonymous communication system
 - Guidelines to structure the study of mixes and dummy traffic
 - “Mix cascades vs. peer-to-peer: is one concept superior?” (Böhme, Danezis, Díaz, Köpsell and Pfitzmann, PET’04)
 - Symmetric (P2P) – Asymmetric (client-server)
 - Flexibility of routing (Cascades, Restricted routes, Free routes)
 - Advantages and disadvantages of these options
-

Research Contributions (2)

- “Taxonomy of mixes and dummy traffic” (Díaz and Preneel, I-NetSec’04)
 - Framework and a taxonomy for the classification and analysis of mixes and dummy traffic
 - Discussion of the different issues involved in the design of anonymous connection systems.
 - Methodology of analysis
 - “Reasoning about the Anonymity Provided by Pool Mixes that Generate Dummy Traffic” (Díaz and Preneel, IHW’04)
 - Extend previous work on anonymity metrics
 - Compact formulas to compute the anonymity of generalized mixes
 - Introduction of dummy traffic in the metrics
-

Research Contributions (3)

- “Comparison between two practical mix designs” (Díaz, Sassaman and Dewitte, ESORICS’04)
 - Analysis of the anonymity provided by Mixmaster and Reliable
 - Analysis input data: not Poisson!
 - Different anonymity for the same input traffic
 - Software tool: Java Simulators of Mixmaster and Reliable
 - Development of anonymity metrics for continuous mixes for non Poisson input traffic
 - Identification of implementation weaknesses
-

Requirements for Anonymous Communication Infrastructures (1)

- ❑ Application-independent communication layer
 - ❑ Good anonymity level (quantity of anonymity - metrics)
 - ❑ Secure anonymity (quality of anonymity)
 - Unlinkability
 - Load balancing (floods/low traffic)
 - Implementation issues (e.g., randomness sources)
 - User experience (skilled/unskilled user)
 - Attack model
 - End-to-end intersection attacks
-

Requirements for Anonymous Communication Infrastructures (2)

- ❑ Availability requirements
 - Access points
 - Operation of the network (DoS attacks)
 - Exit points
 - ❑ Incentives to cooperate / Usability
 - Important for anonymity set size
 - ❑ Scalability
 - ❑ Performance
 - ❑ Unobservability
 - ❑ Open source / verifiable code
-

Conditional Anonymity?

- ❑ Law enforcement / accountability vs. Freedom of speech / access to information
 - ❑ Layered view: anonymity implemented at all levels
 - ❑ Conditional anonymity can be implemented on top of unconditional anonymity. Not vice versa
 - ❑ Current challenges
 - Trust model
 - ❑ Incentives for the users
 - Performance
 - Scalability
 - ❑ Conditional Anonymity can be implemented at the application layer, depending on the particular control requirements and risks
 - Global/Local deanonymization
-

Anonymity Control

- Access control blocks
 - Micro-payments to nodes
 - Proof of subscription
 - Exit policies
 - Black lists
 - White lists
 - Control protocols to detect/exclude malicious participants
 - Reputation systems
-

Building Block: Anonymous Communication Infrastructure

- If the communication layer is not anonymized, efforts to anonymize participants at the application layer are useless
 - Application independent
 - Efficient
 - Secure
 - Robust
-

Evaluation of Anonymous Connection Systems: Requirements

- Trust model
 - Application-independence
 - Unlinkability
 - Load balancing
 - User experience / Usability
 - Implementation issues
 - Attack model
 - Availability
 - Entry points
 - Exit points
 - Possible routes / Robustness network
 - Incentives to cooperate
 - Unobservability
 - Scalability
 - Performance
 - Anonymity control
-

Evaluation of Anonymous Connection Systems

- Asymmetric (client-server) systems:
 - Anonymizer
 - Onion Routing
 - TOR
 - Web MIXes (JAP)
 - Freedom Network
 - Anonymity Network
 - Covert Channels in HTTP
 - Caching systems
-

Evaluation of Anonymous Connection Systems

□ Symmetric (P2P) systems:

- Pipenet
 - Tarzan
 - MorphMix
 - Crowds
 - Hordes
 - Herbivore
 - GNUnet
 - p⁵
 - Cebolla
-

Evaluation of TOR (1)

- Trust Model
 - Routing: Distributed among nodes in path
 - Directory servers: Trusted to provide true information
 - Application Independence
 - Supports TCP-based applications
 - Unlinkability
 - *Leaky pipe* topology
 - Load balancing
 - Congestion control
 - No dummy traffic
-

Evaluation of TOR (2)

- Implementation issues
 - Separates “protocol cleaning” from anonymity
 - Attack model
 - Perfect forward secrecy (stronger than OR against malicious nodes)
 - End-to-end integrity checking (tagging attacks)
 - No reordering: vulnerable to traffic analysis attacks
 - User experience
 - Node operators / end users
 - Availability
 - Free route network
 - Directory servers: information on topology
-

Evaluation of TOR (3)

- Incentives to cooperate
 - Variable exit policies
 - Scalability
 - Free route
 - Performance
 - No delaying
 - Unobservability
 - Not provided
 - Anonymity control
 - Exit policies
-

Conclusions

- ❑ Model for anonymity control at the communication layer:
 - Access control
 - Control protocols
 - Exit policies
 - ❑ Conditional anonymity at the application layer (?)
 - ❑ Definition of requirements
 - ❑ Evaluation of 17 systems
 - ❑ Theoretical tools for the analysis of anonymous connections (5 research papers)
 - ❑ Software tools for the design and analysis of anonymous connection networks (2 simulators)
-

Future Work

- ❑ Extension of anonymity metrics to anonymity networks
 - ❑ Better characterization of Quality of Anonymity (under attacks)
 - ❑ Definition of control requirements
 - Legal requirements
 - ❑ Further work on attack models
 - ❑ Implementation of control mechanisms in real systems
 - ❑ Batching and Dummy traffic strategies for real-time anonymous connections
-

MIXimulator

- Implemented in Java
 - Windows
 - Linux
 - Graphical User Interface
 - Design of Mix networks
 - Free route
 - Cascade
 - Hybrid topologies
 - Mixes implemented: threshold/timed, simple/pool/dynamic pool
 - Flexible dummy traffic policies
 - User patterns: different groups
 - Computes anonymity / delay for each mix
-