Towards Language-Based Anonymous Communication
Aslan Askarov (postdoc)
School of Engineering and Applied Sciences, Harvard University

ABSTRACT

Traditional systems for network anonymity are designed to be application-agnostic. While this enables relatively simple deployment, many applications remain unaware of the anonymous nature of the underlying communication. Because security properties are usually application-specific, there is an opportunity to improve reasoning about anonymity guarantees by making applications aware of the anonymous nature of the underlying communication.

We propose a language-based approach to network anonymity. We distinguish between direct (or identifiable) and anonymous communication at the program source level. We introduce several classes of adversaries based on their ability to inspect anonymous traffic. A security type system regulates how anonymous information propagates within a program. This allows mixing of anonymous and identifiable communication within a single program, and may improve the overall performance while preserving anonymity.

OBJECTIVES

Improve security and performance of using anonymous communication by leveraging application-level reasoning

2002 – present
0.5 mln users

Users are typically aware that they use anonymous network
Applications are typically unaware of the anonymous communication

Different reasons for anonymous communication

- Hide communication from network adversary
  - Existence of a message may reveal sensitive information
  - We use programming languages techniques to soundly infer such messages
- Need to be anonymous to receiver
  - Sending identifiable information on anonymous connection is problematic
  - We prevent this at a language level

MODEL

- Two adversaries that correspond to different network fragments
  - Local network attacker
  - Remote recipient attacker
- Anonymous communication as a programming language construct
  - Need to ensure such construct is used securely

EXAMPLE – ONLINE AUCTION

(local network attacker)

Different types of attackers

- Remote recipient attacker
- Local network attacker

EXAMPLE – SELECTIVE ANONYMITY

(remote recipient attacker)

Anonymity levels

- Common
  - Information that is common knowledge, e.g., time/day
  - Identifiable url
  - Public identifiable information, e.g., name/id, that can be send to url
- Anonymous url
  - Data that must be communicated with url anonymously

Allowed information propagation

- Common ≤ Identifiable url
- Common ≤ Anonymous url

EXAMPLE PROGRAM

NEWS FRONT PAGE

ADS

input from LOCALSTORE;
output to NEWSPAPER;
input from NEWSPAPER; // direct OR
/* Dangerous */
if frontPagePreference == 'Finance' then
  input ads from AD1 // must be anonymous
else
  input ads from AD2 // must be anonymous

TYPING PROGRAMS AGAINST REMOTE RECIPIENT ATTACKER

Anonymity levels

- Common
  - Information that is common knowledge, e.g., time/day
  - Identifiable url
  - Public identifiable information, e.g., name/id, that can be send to url
- Anonymous url
  - Data that must be communicated with url anonymously

Allowed information propagation

- Common ≤ Identifiable url
- Common ≤ Anonymous url

Type system

Level of information that is sent

Level of previous anonymous communication with this url

Anonymity effect after this command

Propagation of anonymity effects

REFERENCES


CONTACT

Aslan Askarov (aslan@seas.harvard.edu)
Stephen Chong (chong@eecs.harvard.edu)