Towards Language-Based Anonymous Communication

Aslan Askarov (postdoc)

School of Engineering and Applied Sciences, Harvard University

Privacy Tools for Sharing Research Data

A National Science Foundation Secure and Trustworthy Cyberspace Project

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 anonymity network

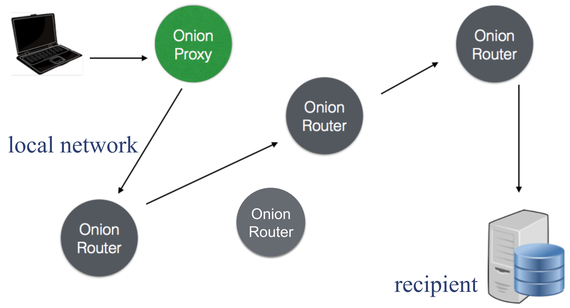
Applications are typically unaware of the anonymous communication

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)

auction participation is public

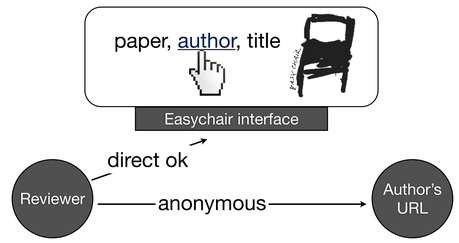
winner is secret

current_max is secret

```
/* auction participants submit their bids in a few rounds */
for (int round = 0; round < n_rounds; round ++)
  for (Participant p: participants)
    /* request updated bid from each participant */
    int b = p.requestBid(current_max);
    if (b > current_max) /* update winning bid */
        current_max = b;
        winner = p;
/* contact winner to process payment */
winner.requestPayment(); /* may reveal winner identity */
```

EXAMPLE – SELECTIVE ANONYMITY

(remote recipient attacker)



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 $\preceq$ Identifiable url Common $\preceq$ Anonymous url

Type system

Level of information that is sent

No previous anonymous communication with this *url*

$$\frac{\Gamma \vdash e : \iota \qquad \Gamma(ch) = \text{Identifiable } url \qquad pc \sqcup \iota \preceq \text{Identifiable } url}{\Gamma, pc \vdash \text{output } e \text{ to } ch : \{\text{Identifiable } url\}}$$

Anonymity effect after this command

Propagation of anonymity effects

$$\frac{\Gamma, pc \vdash c_1 : S_1 \qquad \Gamma, pc \oplus S_1 \vdash c_2 : S_2}{\Gamma, pc \vdash c_1; c_2 : S_1 \cup S_2}$$

EXAMPLE PROGRAM


```
input frontPagePreference from LOCALSTORE;
output frontPagePreference to NEWSPAPER;
input news from NEWSPAPER; // direct OK

/* Dangerous */
if frontPagePrefernce == "Finance" then
    input ads from AD1 // must be anonymous
else
    input ads from AD2 // must be anonymous
```

ONGOING AND FUTURE WORK

- Mixed communication model can provide better performance when using anonymous communication
- Security theorem: well-typed programs in a mixed model are no less secure than in all-anonymous model
  - Parameterized over anonymity security metric
- Usability of the programming model

- Defenses against active attackers
  - Extending communication protocols by propagating application-level information to mitigate active timing attacks

REFERENCES

Towards Language-Based Network Anonymity (white paper). Aslan Askarov and Stephen Chong. DIMACS Working Group on Measuring Anonymity, May 30-31, 2013

CONTACT

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