Nymble: Blocking Misbehaving Users in Anonymizing Networks

I590 Advanced Topics in Privacy Presented by Lusha Wang

What's the problem

- Web services deny access of *misbehaving* users by IP address blocking.
- What if misbehaving users hide *behind an anonymizing network* such as Tor
- *Exit nodes* will be blocked
- *Behaving users* ` requests will also be denied

Contributions

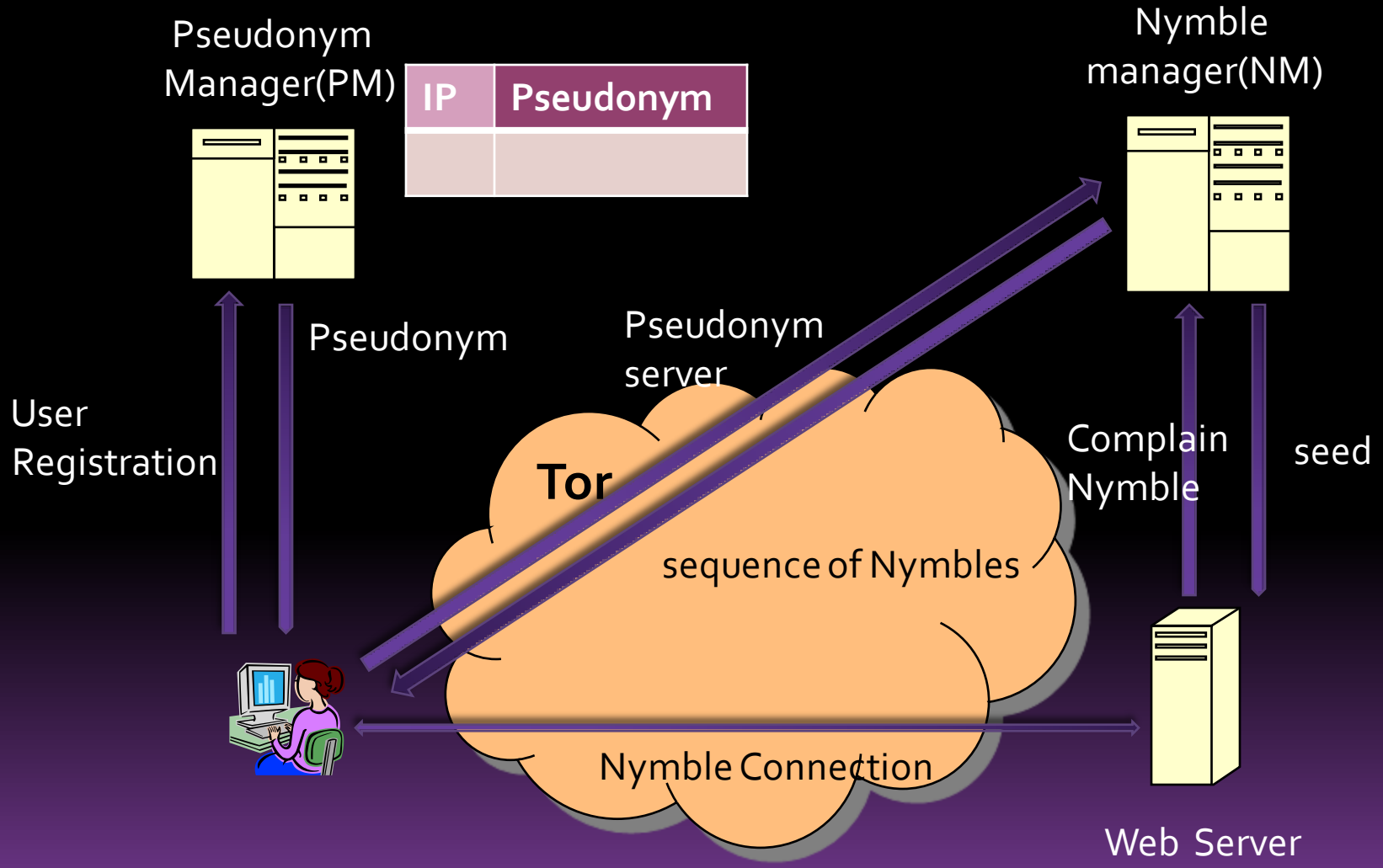
- This paper provides a system called *Nymble* to blacklist users of an anonymizing network and not compromise users' privacy.
- This system employs *symmetric cryptography* to achieve better performance compared with alternatives
- This system is implemented and performance evaluation shows that it is *practical* for usage.

Nymble System: Properties

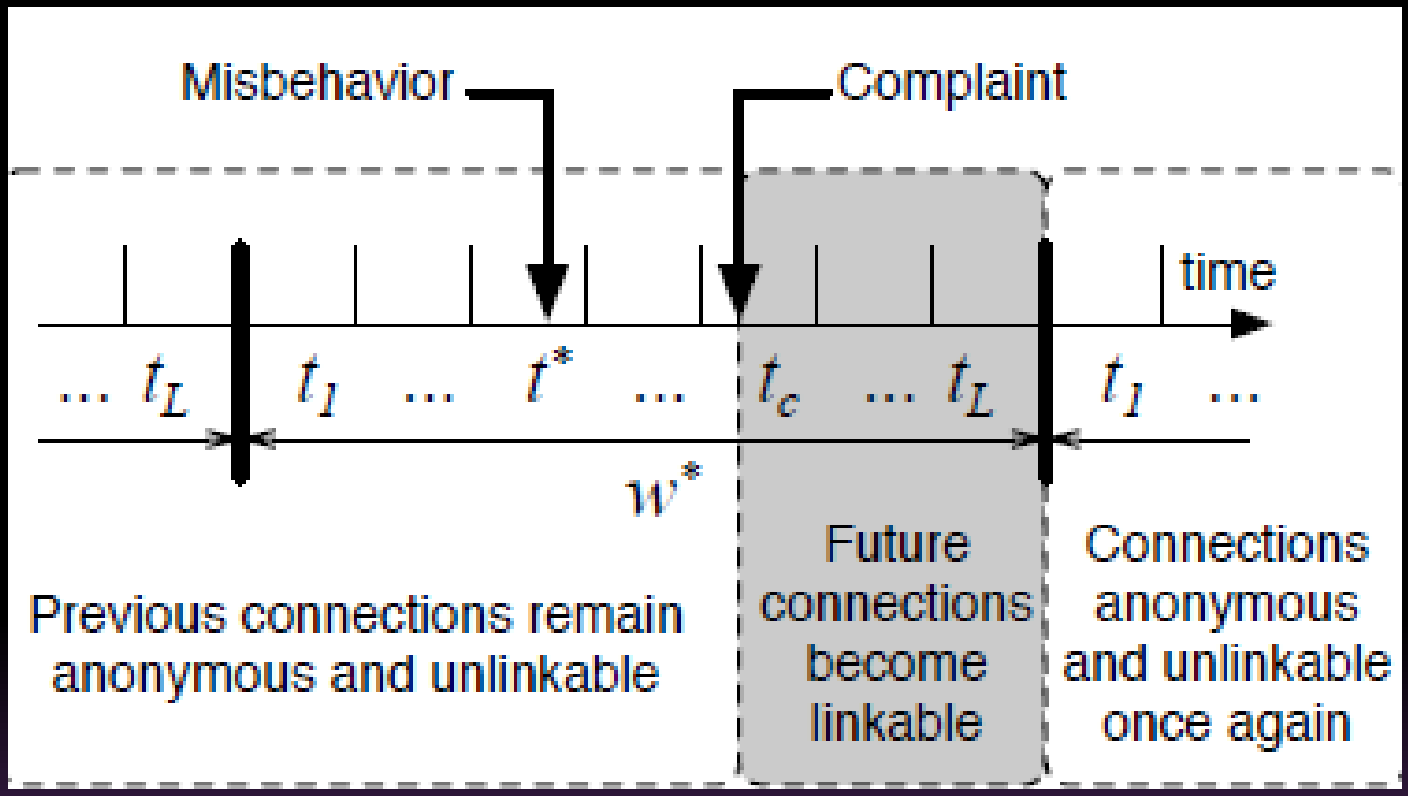
- Authenticate users anonymously
- Backward unlinkability
- Subjective blacklisting
- Fast authentication speeds
- Rate-limit anonymous connections
- Users can verify if they are in the blacklist
- Resources are binds to nymbles

High-level Overview

Server	Pseudonym



Blacklisting a User



- Likability window ; Time period

Purpose of Linkablity Window

- *Dynamism*

  IP addresses can be reassigned to other users

- *Forgiveness*

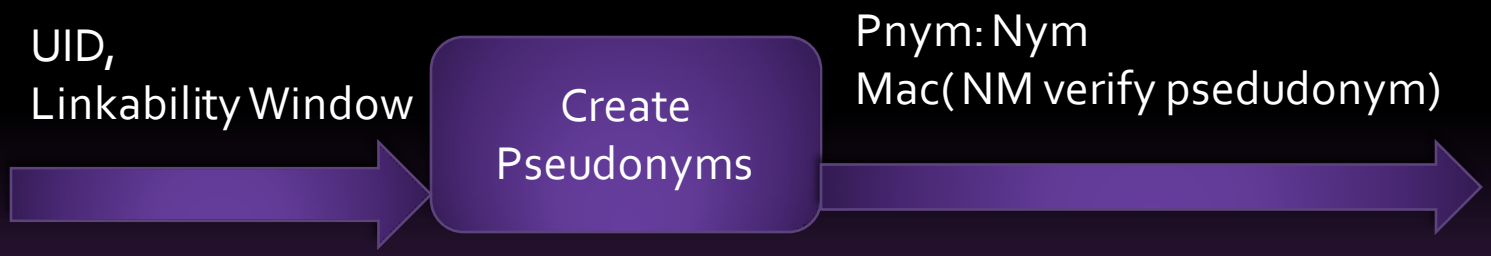
  Forgive misbehaving users after a certain period of time

Data Structures

- Pseudonym Manager issues pseudonyms to users

  UID: IP address

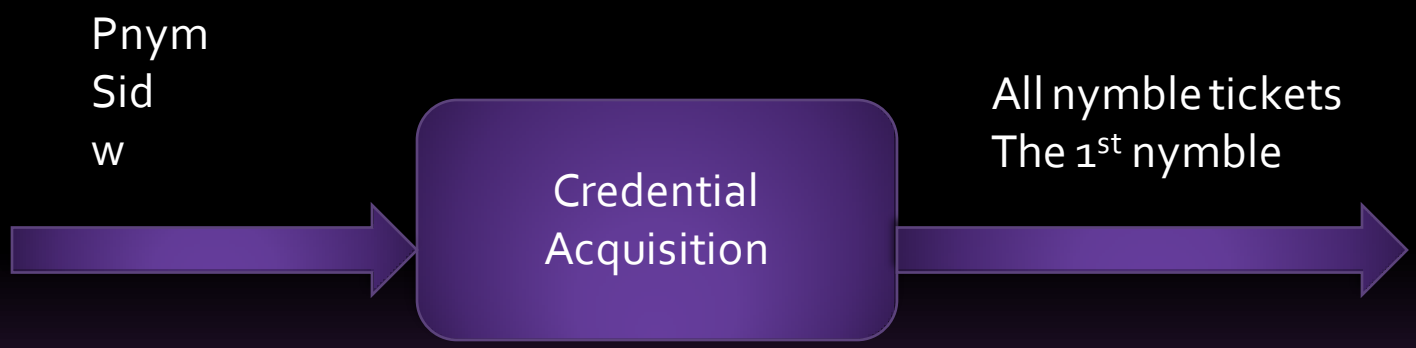
  not Tor exit node



Data Structures

- Seeds and nymbles

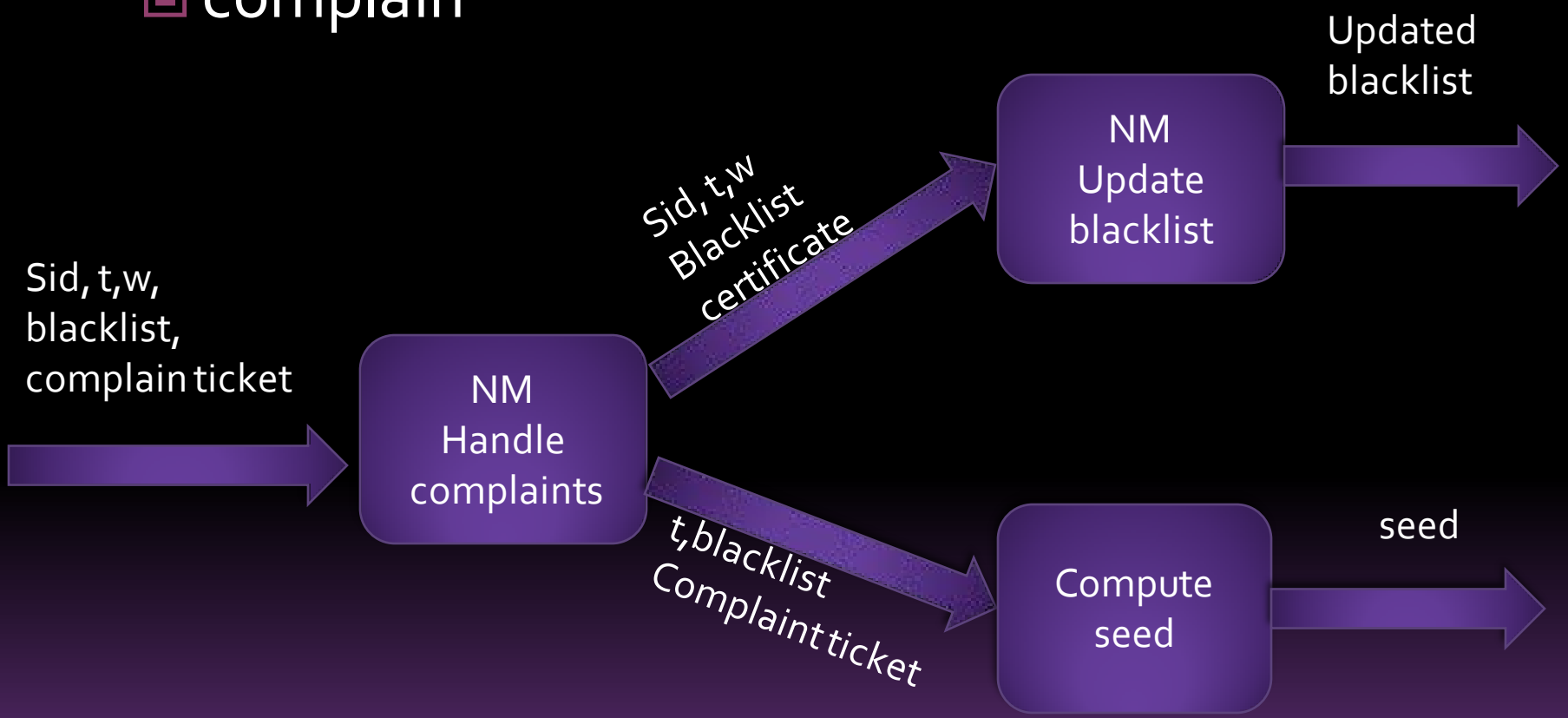
  Nymble is a pseudo-random number serves as an identifier for a particular time period and a specific user



- Ticket: a nymble specific to a server, time period, and likability window

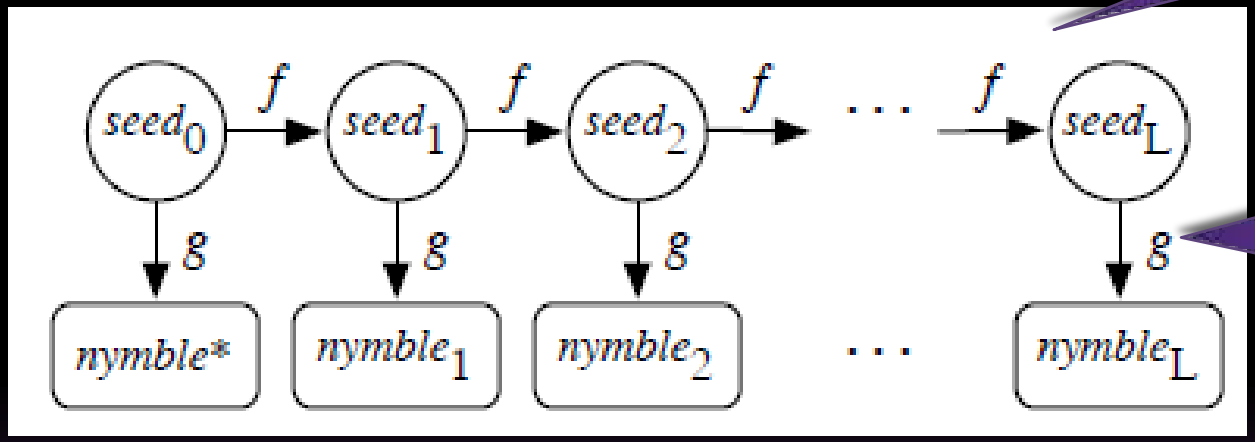
Data Structures

- complain



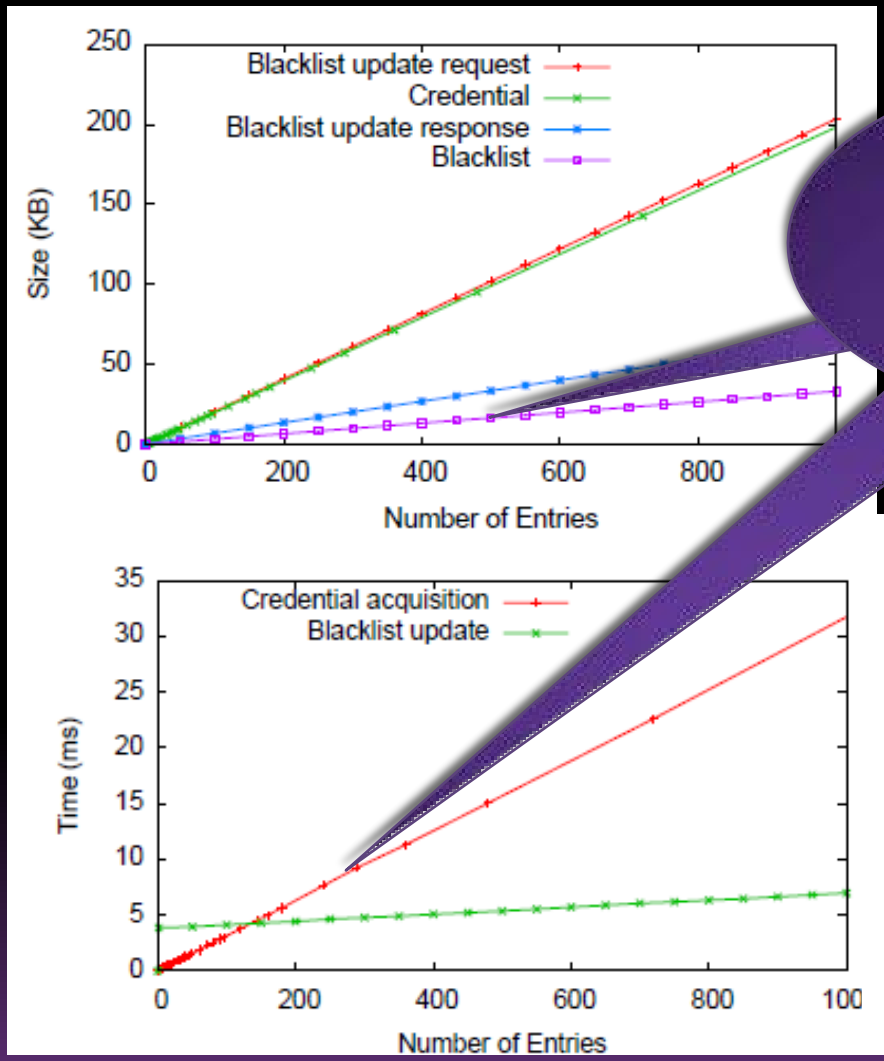
Data Structures

- Evolution of seed and nymbles

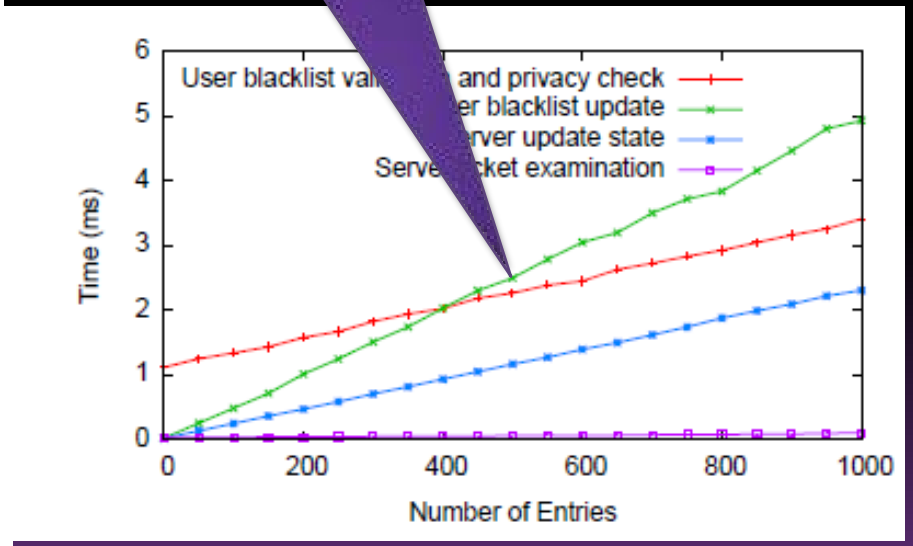


- Backward unlikability, anonymity
- f,g: cryptographic hash function

Performance Evaluation



500 nymbles in the blacklist
less than 3 ms to update



Linear time and space costs with the increase of number of entries