TÉCNICO LISBOA

CipherChat

Secure chat for Android

SIRS Alameda 2013

The Problem

- Many services store your passwords in an unsecure manner, and low standard security policies
  - The Adobe leak
  - Sony’s Password leak
- Communication is made through unsecure applications, protocols and channels
- Users’ privacy is not respected
- Known backdoors on existing services

Proposition

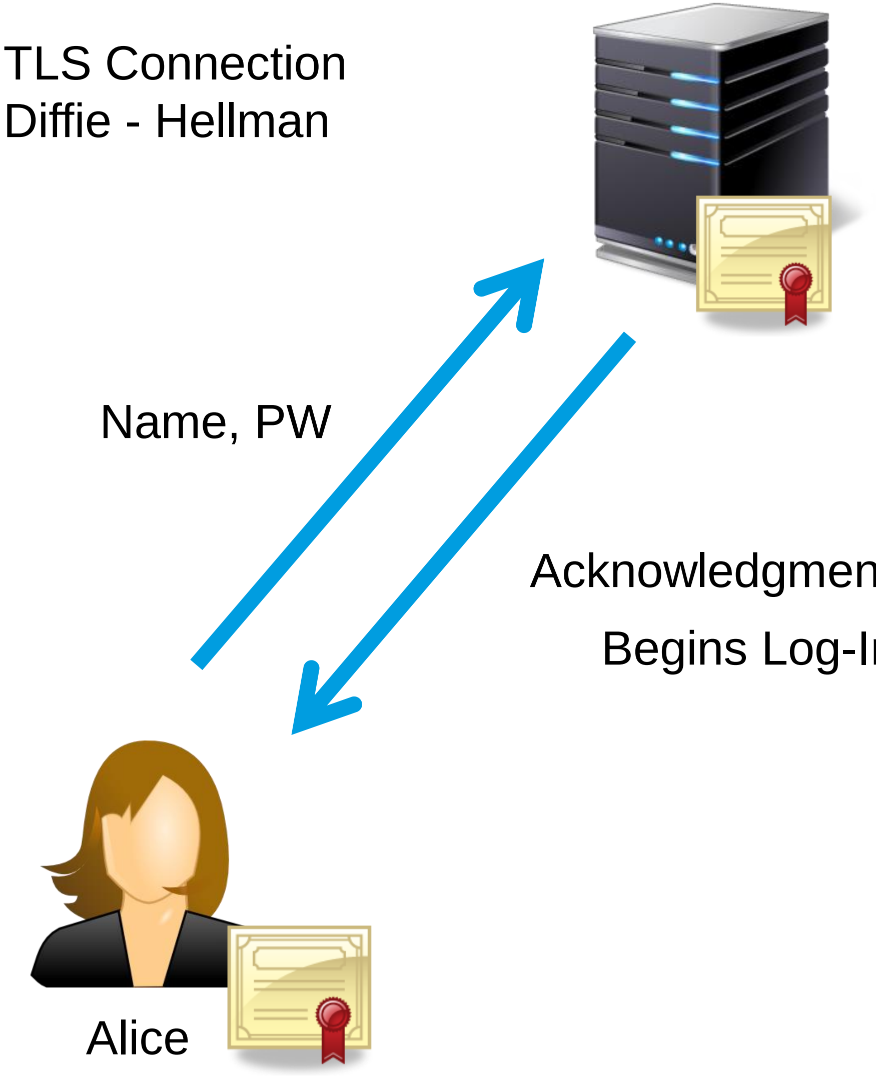
- Create a Ciphered one-to-one chat application
- Have a secured server
- Guarantee users’ protection from attackers
- Available in any network

Registration

TLS Connection
Diffie - Hellman

Server

Password + Salt → Hash (SHA-256)



Name, PW

Acknowledgment

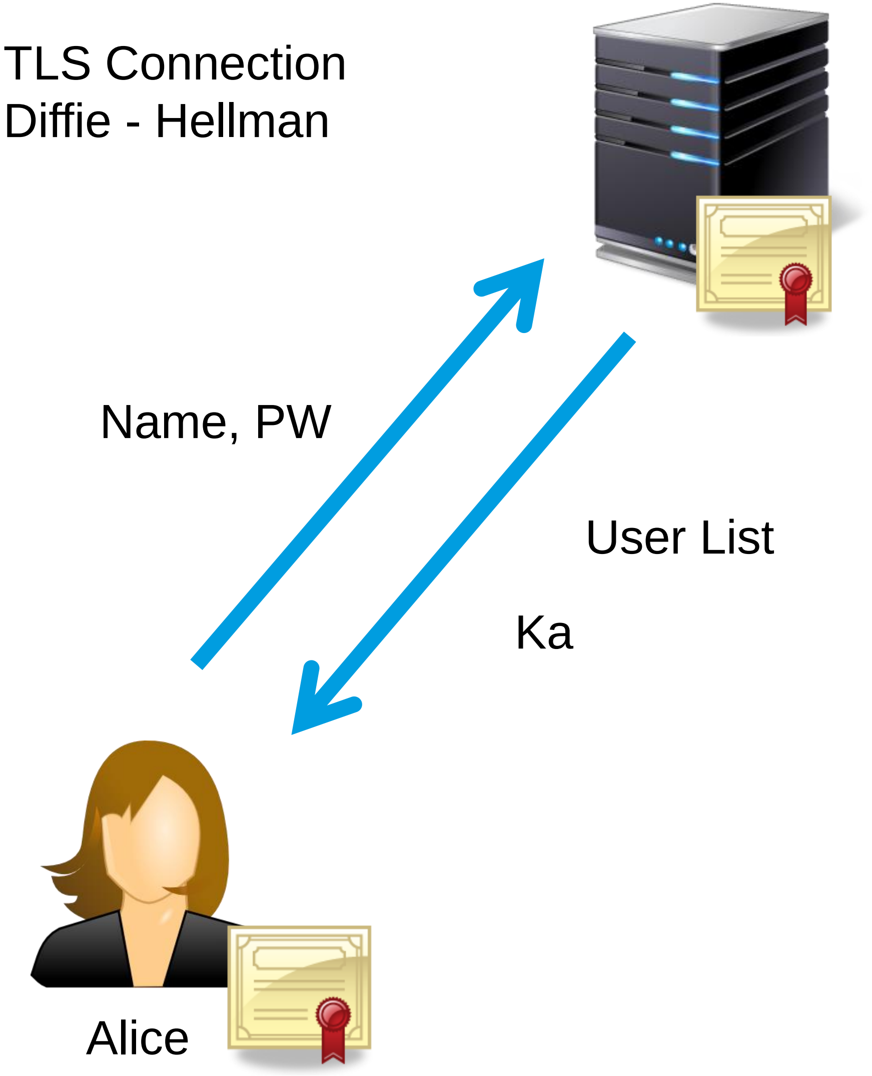
Alice

Begins Log-In process

Every exchanged message has a
Time-Stamp and HMAC
for freshness and integrity

Log-In

TLS Connection
Diffie - Hellman



Server

Checks Password Hash
Creates Key Encryption Key (Ka)

Name, PW

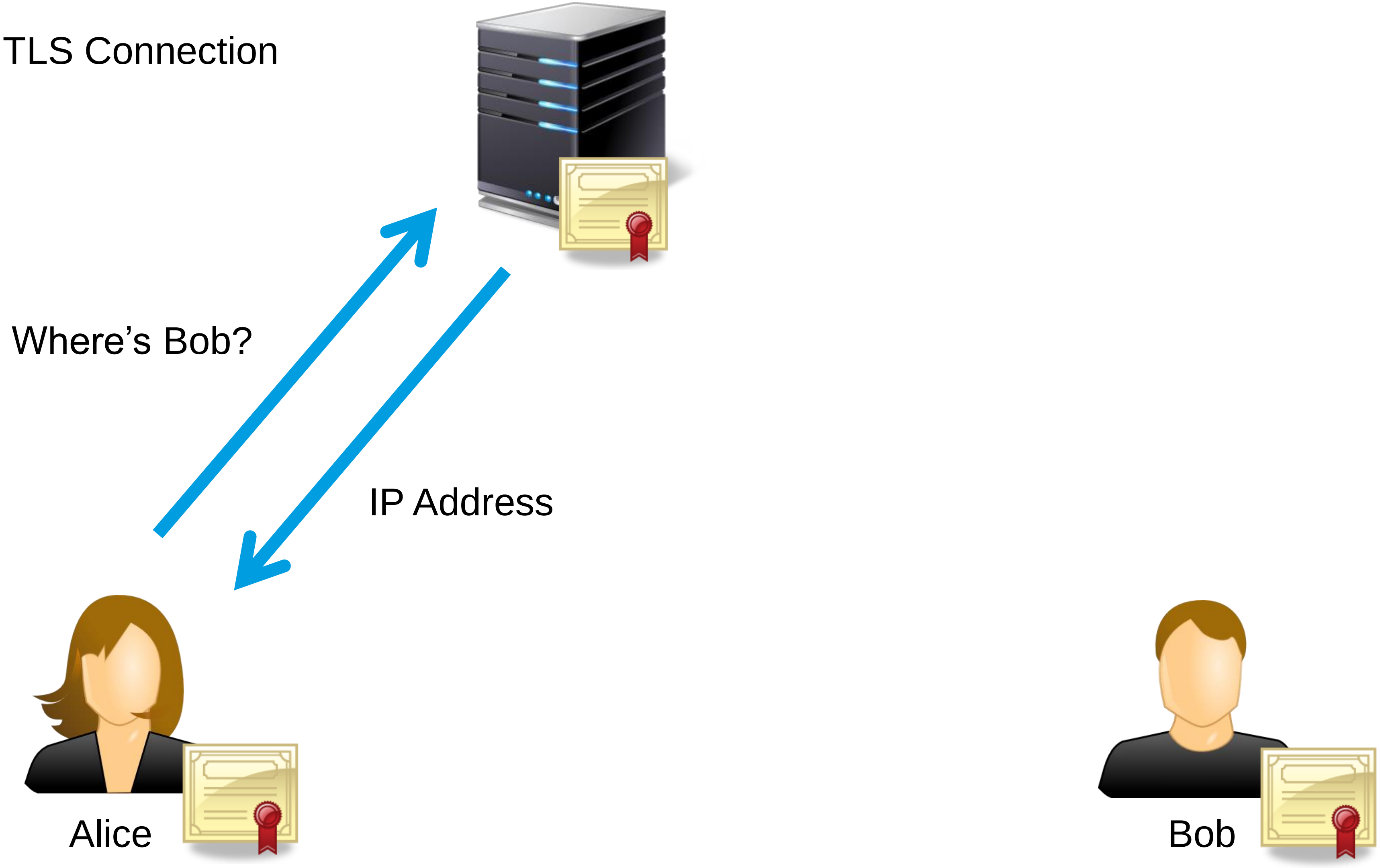
User List

Ka

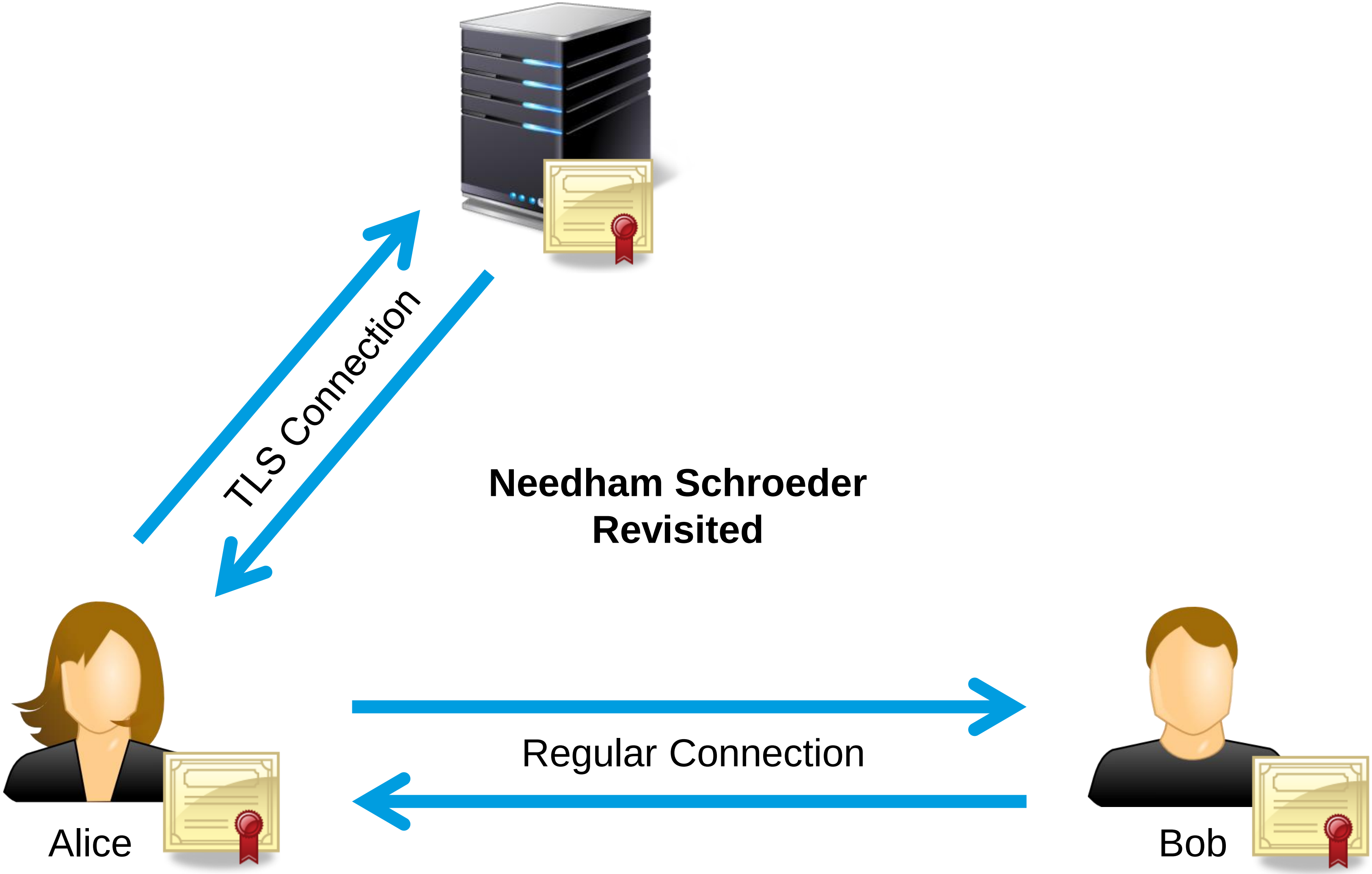
Alice

Starting Communication

TLS Connection

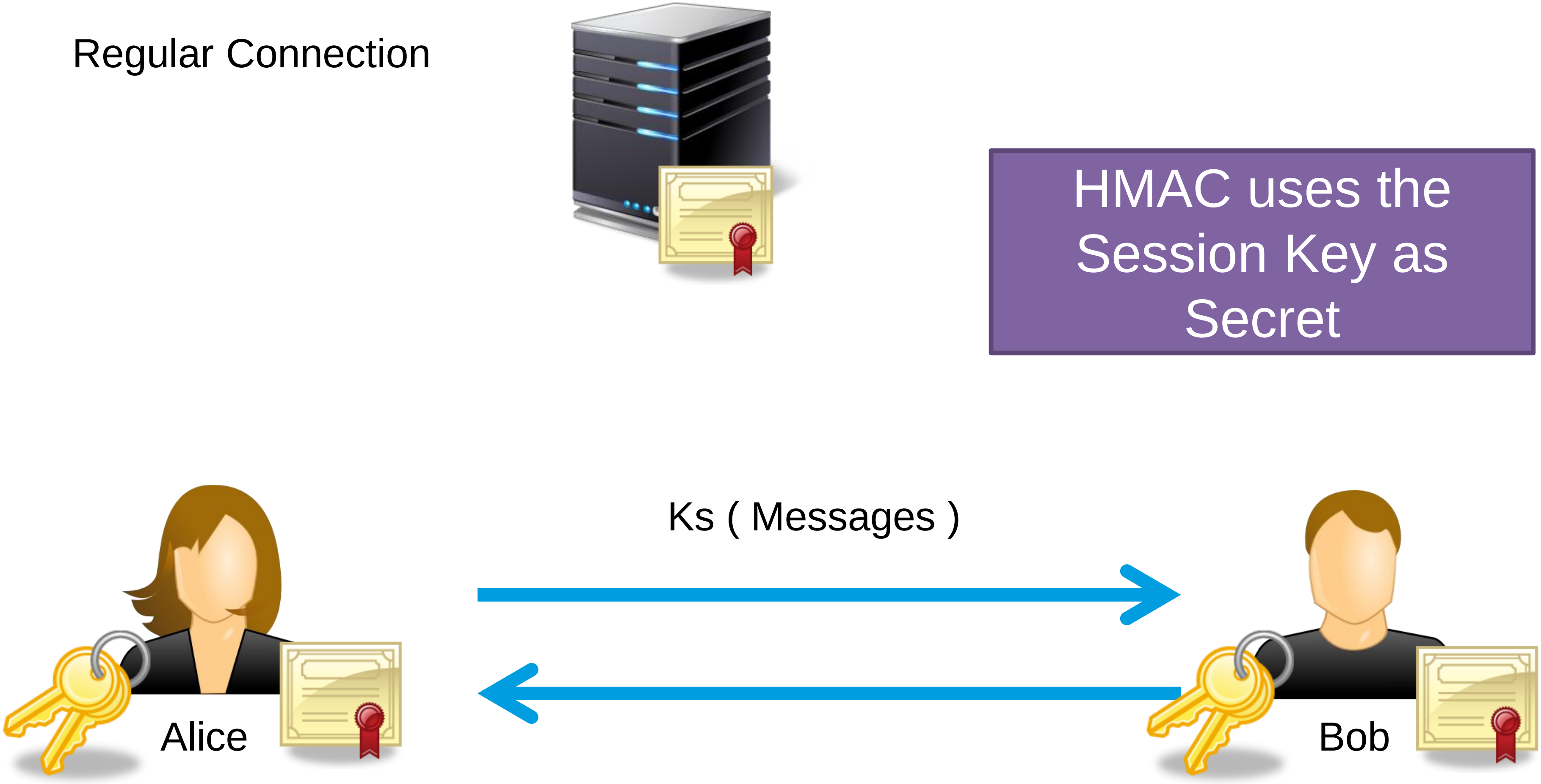


Starting Communication



Communication

Regular Connection

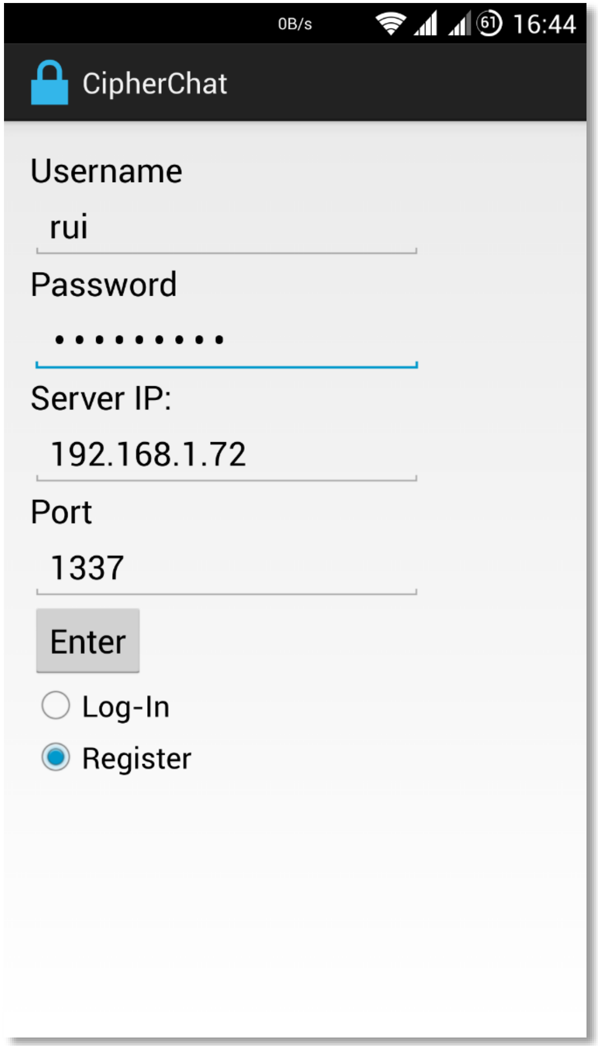


HMAC uses the Session Key as Secret

Security Features

- Registration and log-in are made through a secured TLS connection authenticated by a digital certificate
- TLS is used in Diffie-Hellman mode
- Server doesn’t store passwords
- User-to-user connection is started through Needham-Schroeder Revisited
- Every chat message is encrypted with AES/CBC/PKCS5Padding
- Data and application exchanges are all accompanied by a timestamp and an HMAC

Preview



Username

rui

Password

•••••••••

Server IP:

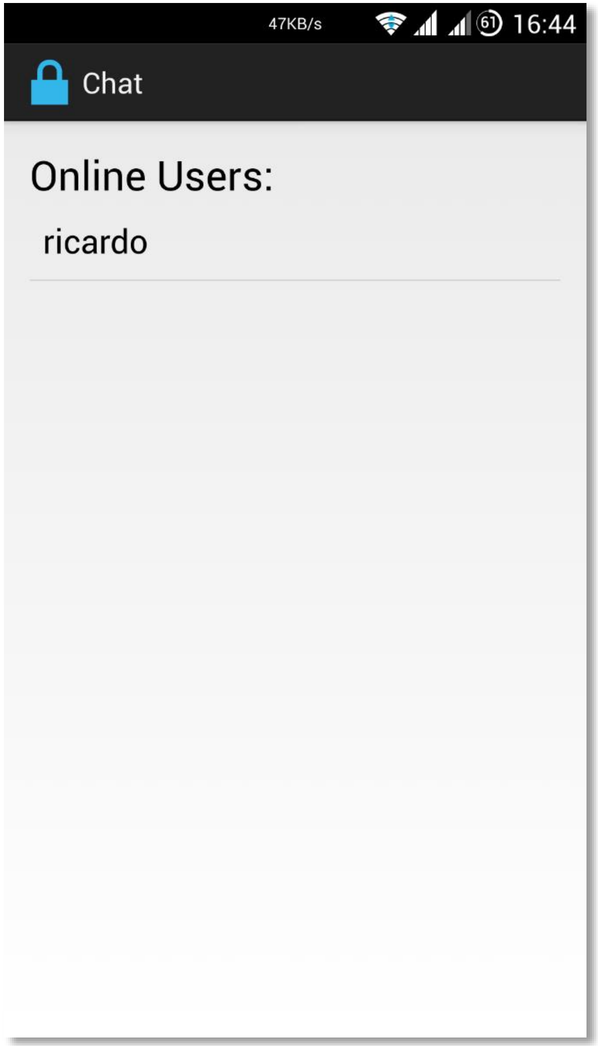
192.168.1.72

Port

1337

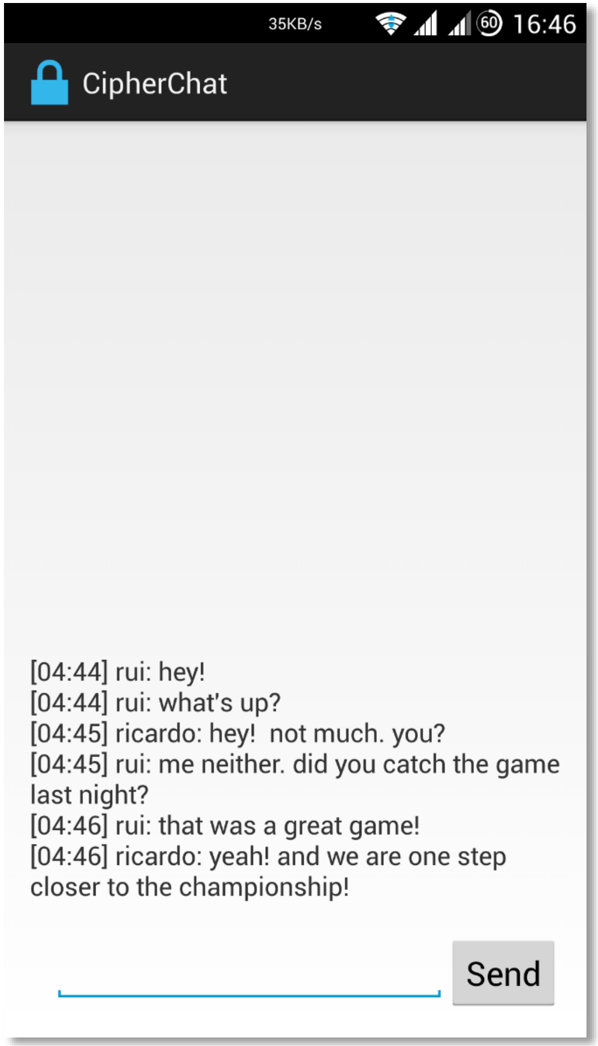
○ Log-In

● Register



Online Users:

ricardo



[04:44] rui: hey!
[04:44] rui: what's up?
[04:45] ricardo: hey! not much. you?
[04:45] rui: me neither. did you catch the game last night?
[04:46] rui: that was a great game!
[04:46] ricardo: yeah! and we are one step closer to the championship!

TÉCNICO LISBOA

CipherChat

for Android