

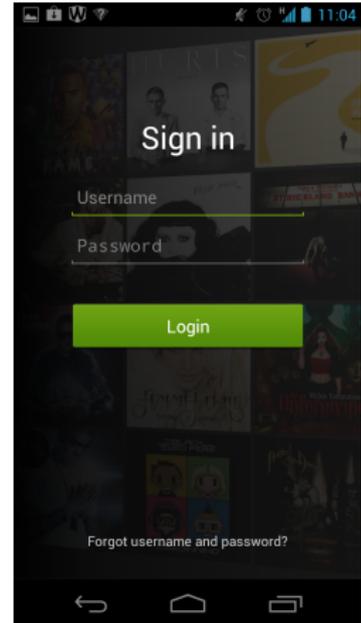
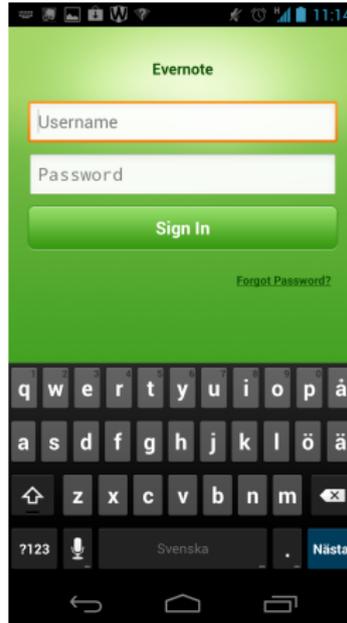
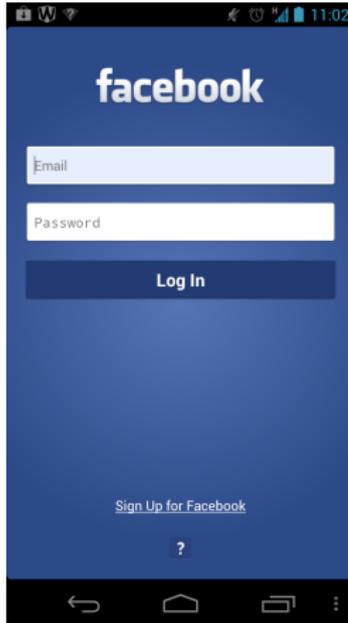
Passwords in Peer-to-Peer

Gunnar Kreitz, Oleksandr Bodriagov, Benjamin Greschbach,
Guillermo Rodríguez-Cano, and Sonja Buchegger

KTH – Royal Institute of Technology

IEEE P2P'12, September 4 2012

Modern End-User Services



Logging in to P2P?

What was the last P2P application you logged in to?

The Easy Case

The screenshot shows the uTorrent 1.7.1 interface. The main window displays a list of torrents. The first torrent, 'oCo_2.2.1_Win32Intel_instal... 1', is currently downloading at 81.76% completion. The second torrent, 'KNOPPIX_V5.1.1DVO-2007-01-04-EH... 2', is at 0.5% completion. The third torrent, 'abunb-7.04-desktop-C86.iso 3', is in a 'Queued' state at 0.0% completion.

Name	#	Size	Done	Status	Seeds	Peers	Down Speed	Up Speed	ETA	Uploaded	Ratio	Avail.	Label
oCo_2.2.1_Win32Intel_instal...	1	208 MB	170 MB	Downloading	56 (74)	9 (82)	463.9 kB/s	6.3 kB/s	5m	672 kB	0.006	57...	
KNOPPIX_V5.1.1DVO-2007-01-04-EH...	2	4.02 GB	20 MB	Downloading	0 (0)	0 (0)	256.4 kB/s	20.3 kB/s	4h 53m	3.73 MB	0.002	67...	
abunb-7.04-desktop-C86.iso	3	697 MB	0 MB	Queued	0 (0)	0 (0)	0	0	∞	0.0 kB	0.000	0.000	

The bottom panel shows the 'General' tab for the selected torrent. It displays progress bars for 'Downloaded' (0.9%) and 'Availability' (59.98%).

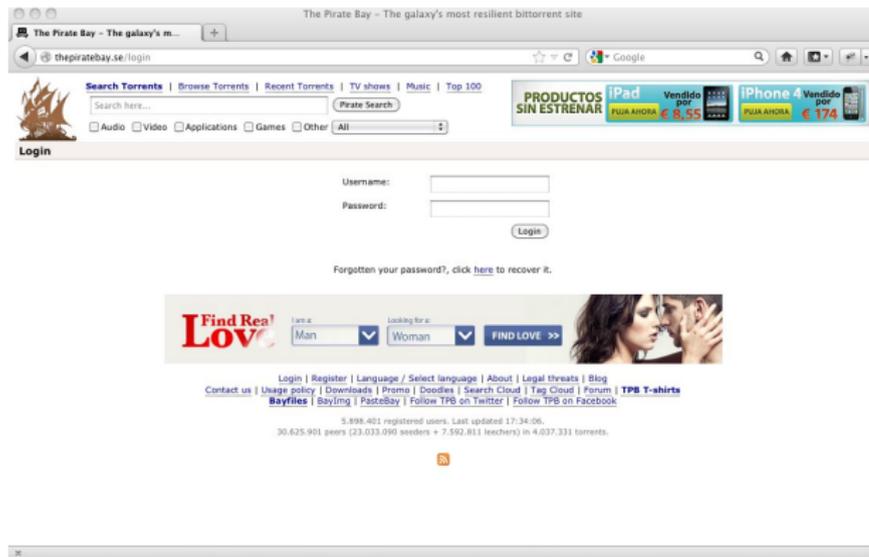
Transfer
 Time Elapsed: 4m 46s
 Downloaded: 37.9 MB
 Uploaded: 3.73 MB
 Seeds: 59 of 65 connected (195 in swarm)
 Web Seeds:

Tracker
 Tracker URL: http://torrent.unix-eg.uni-kl.de/announce
 Tracker Status: working
 Update In: 25:15
 DHT Status: announce in 17 minutes (got 12 peers)

General
 Save As: C:\Downloads\KNOPPIX_V5.1.1DVO-2007-01-04-EH
 Total Size: 4.02 GB (37.9 MB done)
 Created On: 1/8/2007 12:42:34 AM
 Comment: KNOPPIX_V5.1.1DVO-2007-01-04-EH

At the bottom, it shows DHT nodes (278) and a green checkmark indicating the torrent is healthy (D: 726.3 MB/s T: 138.4 MB U: 34.7 MB/s T: 5.2 MB).

Sometimes we Want Authentication



The screenshot shows a web browser window with the URL `thepiratebay.se/login`. The page title is "The Pirate Bay - The galaxy's most resilient bittorrent site". The browser's address bar shows the URL and search engines like Google. The page content includes a navigation menu with links for "Search Torrents", "Browse Torrents", "Recent Torrents", "TV shows", "Music", and "Top 100". There is a search bar with the text "Pirate Search" and a dropdown menu for categories: "Audio", "Video", "Applications", "Games", and "Other". A banner advertisement for "PRODUCTOS SIN ESTRENAR" is visible, featuring "iPad" and "iPhone 4" with prices like "€ 8,55" and "€ 174". Below the banner is a "Login" section with a "Username:" field, a "Password:" field, and a "Login" button. A link for "Forgotten your password?, click here to recover it." is also present. At the bottom of the page, there is a "Find Real Love" advertisement with a "FIND LOVE >>" button and a small image of a couple. The footer contains various links like "Login", "Register", "Language", "About", "Legal threats", "Blog", "Contact us", "Usage policy", "Downloads", "Promo", "Doodles", "Search Cloud", "Tag Cloud", "Forum", "TPB T-shirts", "Bayfiles", "Baying", "PasteBay", "Follow TPB on Twitter", and "Follow TPB on Facebook". It also displays statistics: "5.898.401 registered users. Last updated 17:34:06. 30.625.901 peers (23.033.090 seeders + 7.592.811 leechers) in 4.037.331 torrents."

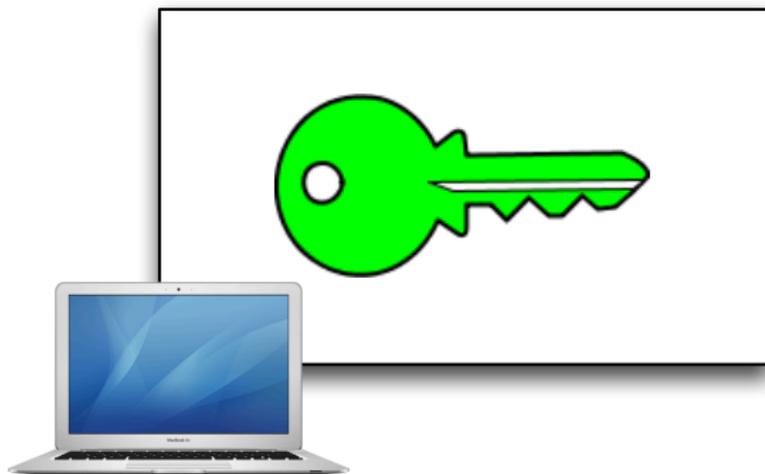
Standard P2P Solution

- ▶ Generate a cryptographic key
- ▶ Whoever knows key is authenticated as user
- ▶ On a single machine it Just Works™

Standard P2P Solution

- ▶ Generate a cryptographic key
- ▶ Whoever knows key is authenticated as user
- ▶ On a single machine it Just Works™
- ▶ ...but, needs to be copied to smartphone.

Standard P2P Solution Depicted



Problem Crops up in P2P Backup

- ▶ Default solution fails spectacularly for backup
- ▶ Some punt problem to user: back up the key separately
- ▶ Some derive master key from a password

Target Scenario



Application

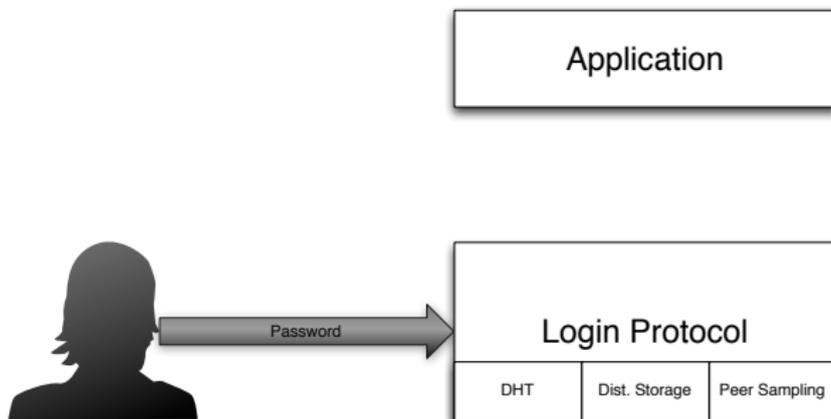
Login Protocol

DHT

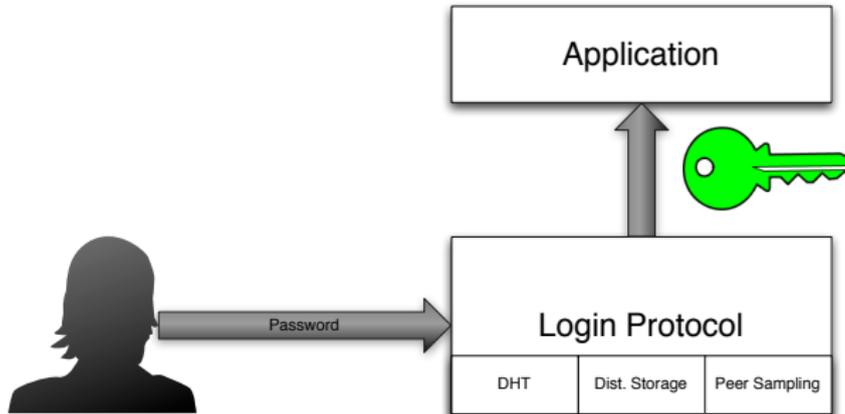
Dist. Storage

Peer Sampling

Target Scenario



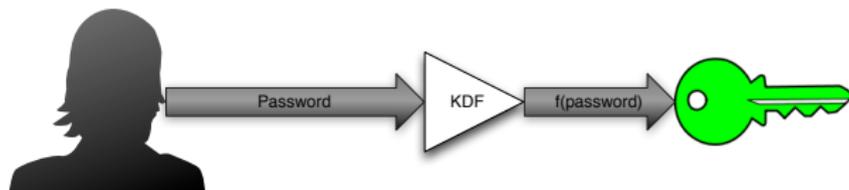
Target Scenario



The Basic Solution

- ▶ Basic solution: derive key from user-entered password
- ▶ Cryptographic key-derivation function (PBKDF-2, bcrypt)

Basic Solution Depicted



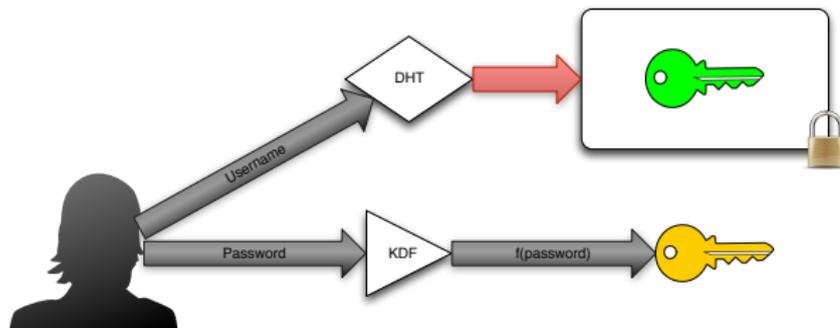
Adding some flexibility

- ▶ Tying key we use to password can be limiting
- ▶ Add a *key store* where keys we need are stored
- ▶ Key store is encrypted with key derived from password

Locating the key store

- ▶ How does one find the key store?
- ▶ Lookup service (DHT) mapping username to storage location
- ▶ Needs to be write-once to prevent DoS

Flexible Basic Solution Depicted



Why not just use a Cloud?

- ▶ Censorship resistance
- ▶ Administrative cost
- ▶ Requires trust in cloud provider

Why not just use a Cloud?

- ▶ Censorship resistance
- ▶ Administrative cost
- ▶ Requires trust in cloud provider
- ▶ Our protocol can be deployed on cloud storage

Remember Me

Sign in Google

Username

Password

Stay signed in

Can't access your account?

Sign in to Yahoo!

https://login.yahoo.com/config/login?.src=flickrsignin&pc=8190&scrumb=0&pd=cX3Q

YAHOO! Yahoo! | Help

Don't have a Yahoo! ID?

OR

Sign in with:

Sign in to Yahoo!

Yahoo! ID

(e.g. free2thyme@yahoo.com)

Password

Keep me signed in
(Uncheck if on a shared computer)

[I can't access my account](#) | [Help](#)

Copyright © 2012 Yahoo! Inc. All rights reserved.
[Copyright® Policy](#) | [Terms of Service](#) | [Guide to Online Security](#) | [Privacy Policy](#)

Requirements

- ▶ Password must not be recoverable from device
- ▶ Must be able to revoke stored credentials on other devices

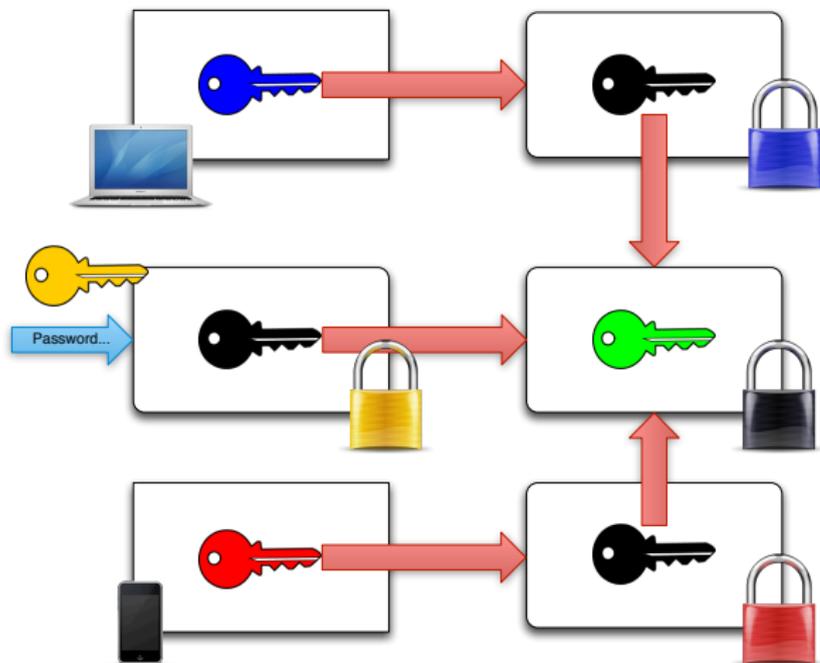
Design

- ▶ All problems in computer science can be solved by another level of indirection

Design

- ▶ All problems in computer science can be solved by another level of indirection
- ▶ For each device, a device login information file in distributed storage
- ▶ File contains encrypted copy of key store key
- ▶ Device stores key to decrypt its device login file

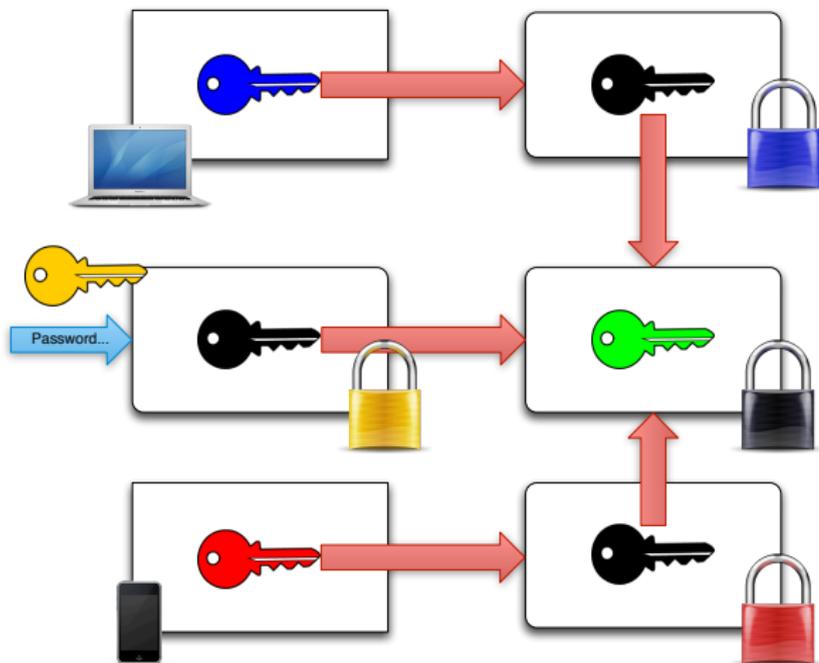
Simplified Remember Me in Pictures



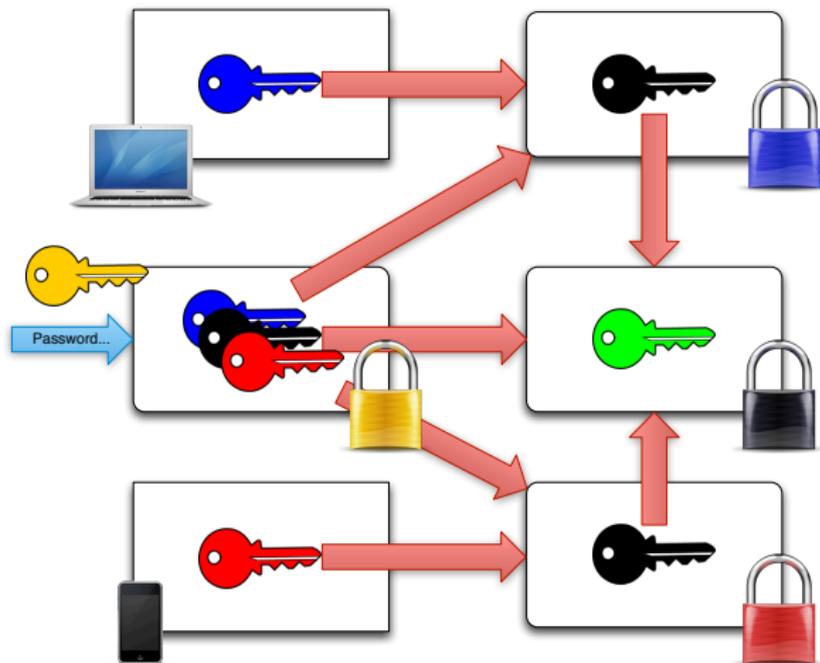
Revokation

- ▶ To support revokation, devices' keys are also escrowed
- ▶ Key store key is replaced
- ▶ All non-revoked devices' login information files are updated
- ▶ Application keys from key store must also be updated!

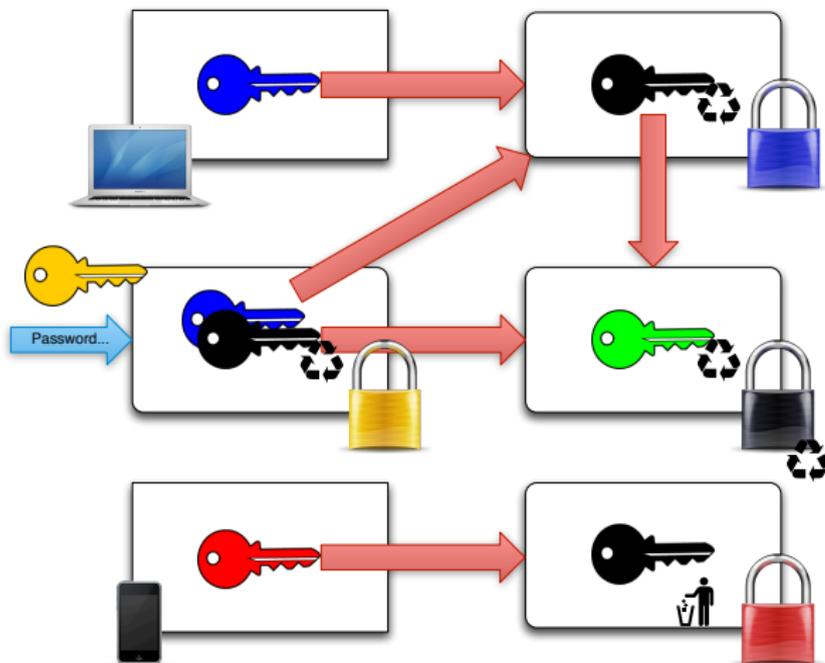
Remember Me in Pictures



Remember Me in Pictures



Remember Me in Pictures



Password Change

Change email address and password ✕

If you want to change your password or email address, just type your new email address and password!

Please enter your old password to confirm your changes.

Requirements

- ▶ User must know old password to change it

Authentication for distributed storage

- ▶ How to authenticate for the distributed storage (Catch-22)?

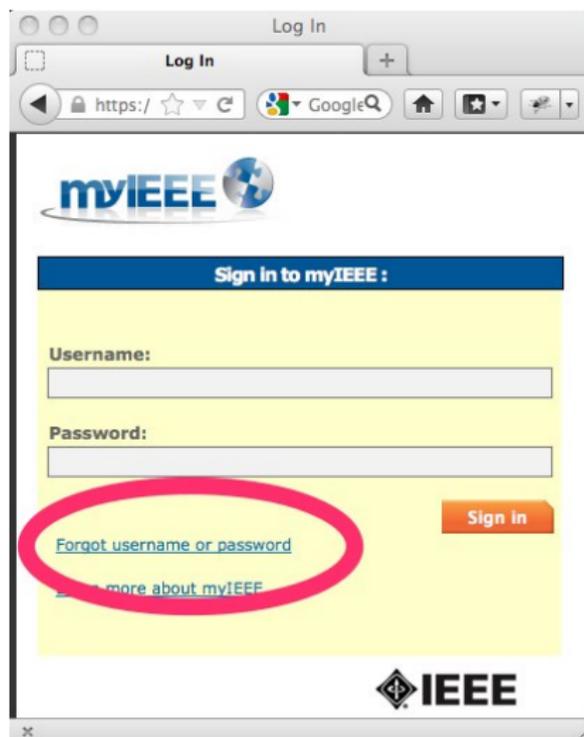
Authentication for distributed storage

- ▶ How to authenticate for the distributed storage (Catch-22)?
- ▶ With cryptographic keys, of course! (It's a normal P2P protocol)
- ▶ All files are world-readable, only writing requires key
- ▶ Write-permission for most files from key store
- ▶ Write-permission for login info only if one can decrypt login info

Design

- ▶ Using password, retrieve key needed to update login info
- ▶ Generate new key for key store
- ▶ Store new key store
- ▶ Update login info to point to new key store
- ▶ Update/remove device login information files

Forgotten Passwords



Requirements

- ▶ Should not reveal secret information to others
- ▶ Based on e-mail and/or security questions

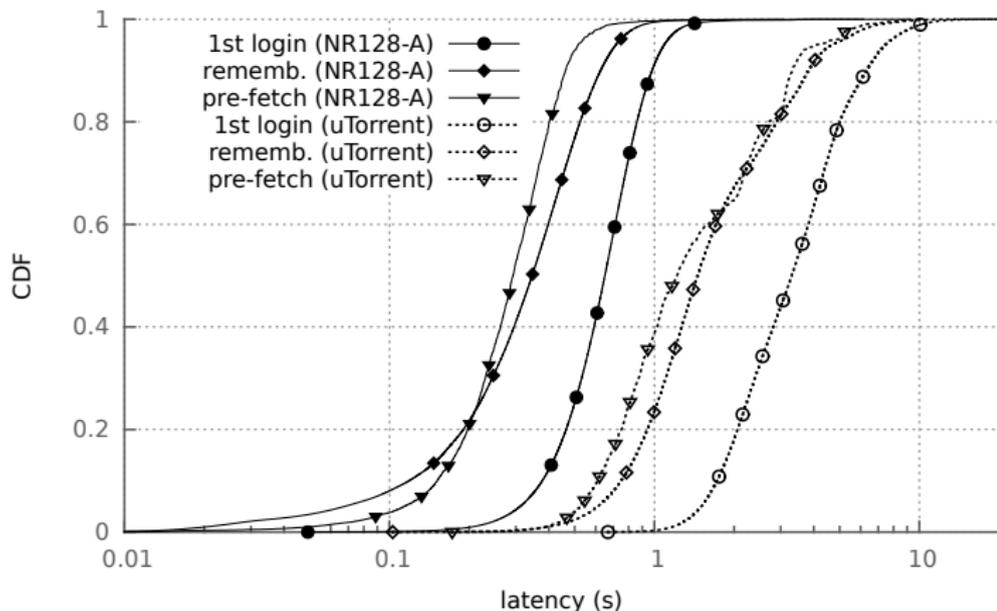
Design

- ▶ Two separate schemes for e-mail and questions
- ▶ Building on secret sharing
- ▶ For questions, shares are encrypted with key derived from answers
- ▶ For e-mail, shares are spread among random peers
- ▶ Using cryptographic commitments to only reveal e-mail address when actually used

Evaluation Setting

- ▶ Simulation using timing from Bittorrent DHT
- ▶ DHT timing by Jiménez et al (P2P'11)
- ▶ Excludes crypto computation (negligible aside from KDF)

Evaluation Results



Future Work

- ▶ Security proofs
- ▶ Prevent offline guessing attacks
- ▶ Implementation

Summary

- ▶ Fully distributed protocol supporting main features of password-based login
- ▶ Including “Remember me”, password change, password reset
- ▶ Room for future improvements