Web Authentication using Third-parties in Untrusted Environments

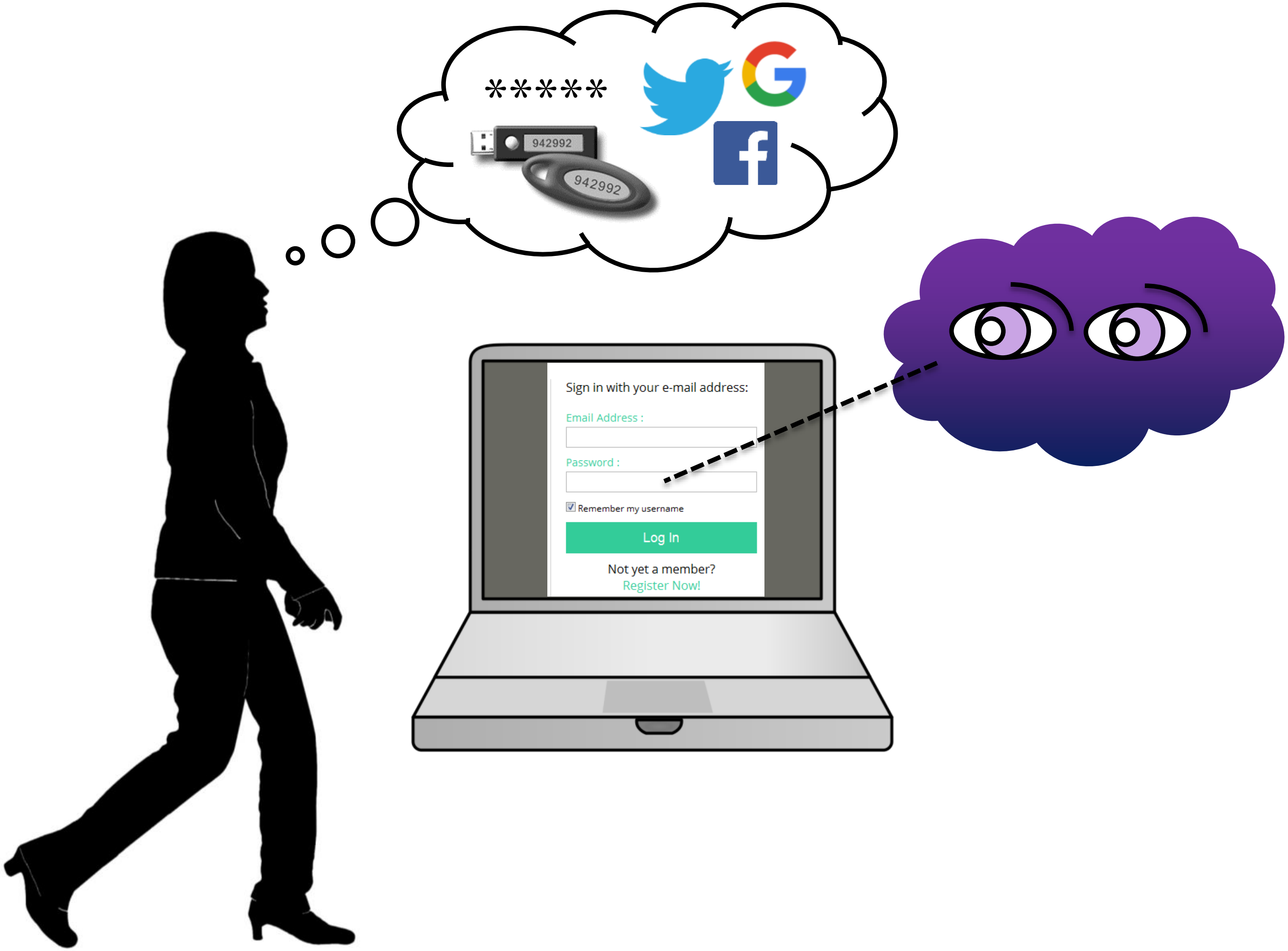
Anna Vapen

PhD Thesis Presentation 2016-09-30

Supervisors: Nahid Shahmehri, Niklas Carlsson

LINKÖPING UNIVERSITY

ELLIIT



Sign in with your e-mail address:

Email Address :

Password :

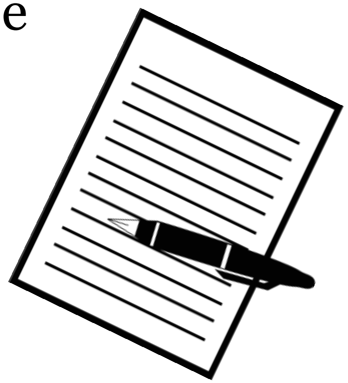
☑ Remember my username

Log In

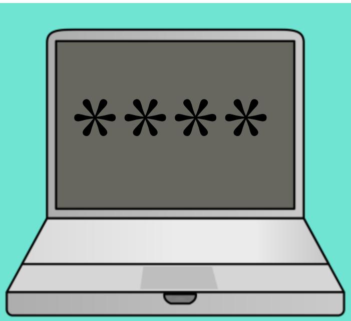
Not yet a member?
Register Now!

Agenda

1. Background
2. Research problems
3. Analysis
   - Web authentication and untrusted computers
   - The third-party authentication landscape
   - Third-parties and privacy risks
4. Contributions

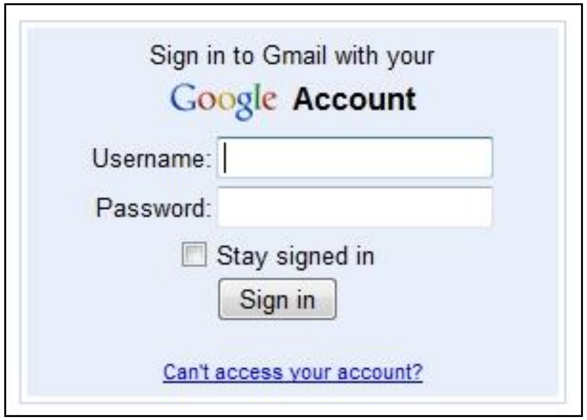


Background



Web Authentication

- Method to prove that you are a specific person
- Personal web experience
  - User accounts require authentication



Sign in to Gmail with your

Google Account

Username:

Password:

□ Stay signed in

Sign in

Can't access your account?

Example: Signing in to Google with username and password

Password Challenges

Most common web authentication method

Simple setup

Reused on several sites

Written down

Alternative methods

Time consuming

Additional equipment

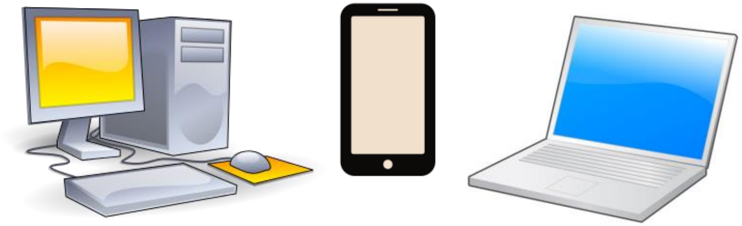
Replay attacks

Forgotten by the user

Mobile Users and Untrusted Environments

- Mobile users
  - Different devices
  - Different places

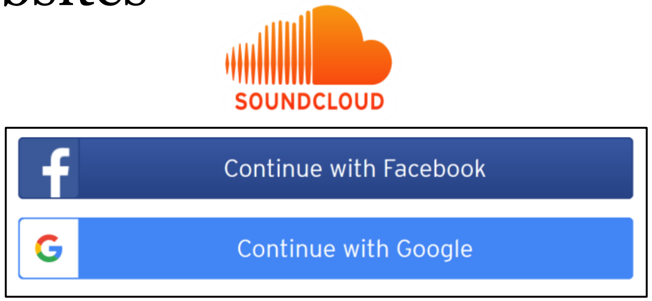
- Untrusted environments
  - Infected computer
  - Untrusted WiFi network



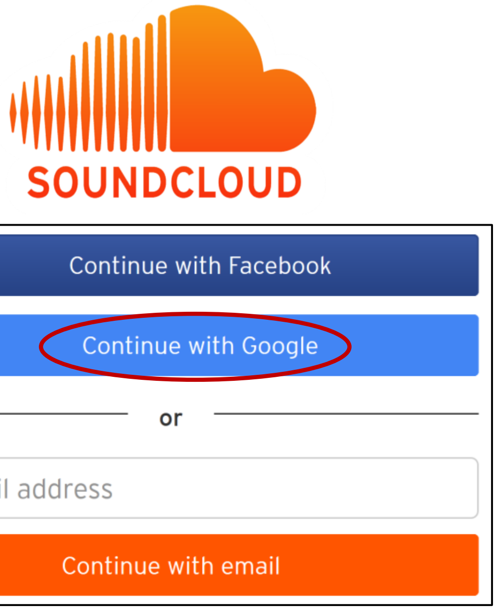
Third-party Web Authentication

- Use an **IDP** (identity provider) account to access many **RPs** (relying parties)

- Fewer logins – simplify authentication
- Information sharing between websites
  - Privacy leaks!



Third-party Authentication Scenario

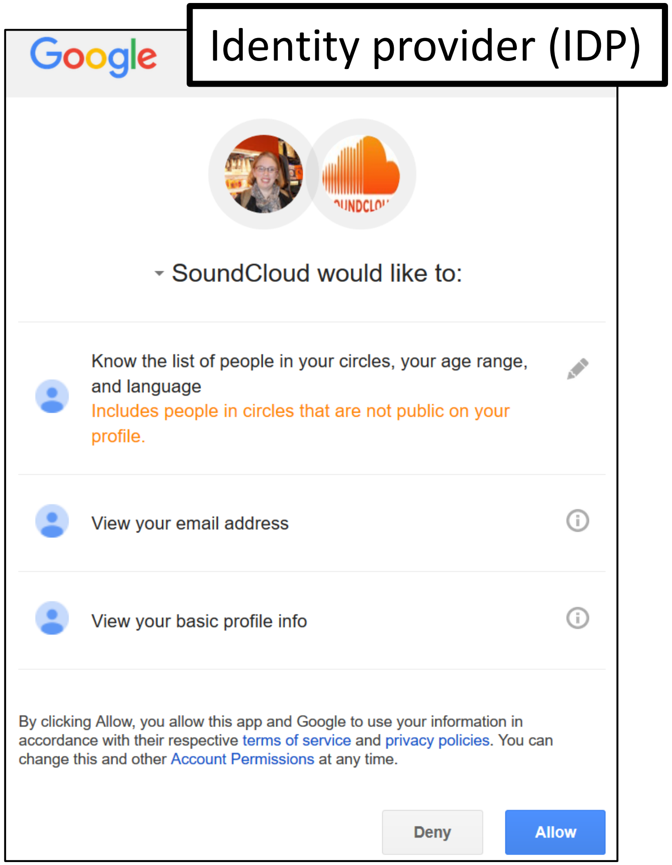


SOUNDCLOUD

Relying party (RP)

Redirect

Logged in



Identity provider (IDP)

SoundCloud would like to:

Know the list of people in your circles, your age range, and language
Includes people in circles that are not public on your profile.

View your email address

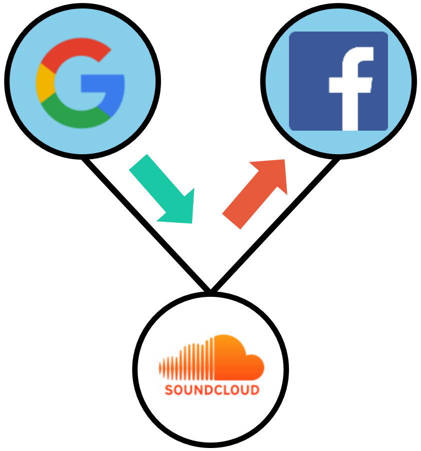
View your basic profile info

By clicking Allow, you allow this app and Google to use your information in accordance with their respective terms of service and privacy policies. You can change this and other Account Permissions at any time.

Research Problems

Research Problems

1. Web authentication
   - For mobile users in untrusted environments?
2. Third-party authentication
   - Usage over time?
   - How to measure?
3. Privacy risks
   - Information flows between parties?



Web Authentication and Untrusted Computers

Mobile Phones as Authentication Devices

Strong authentication

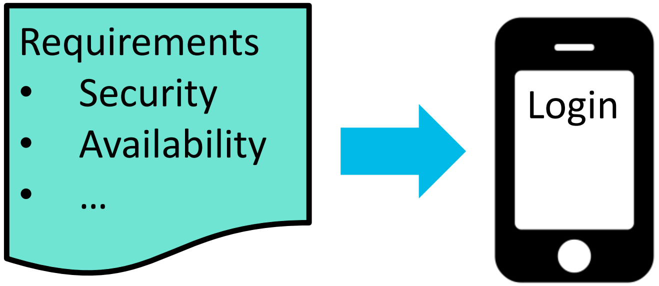
Carried by the user

Security problems

Comparing solutions?

Design and Evaluation Method

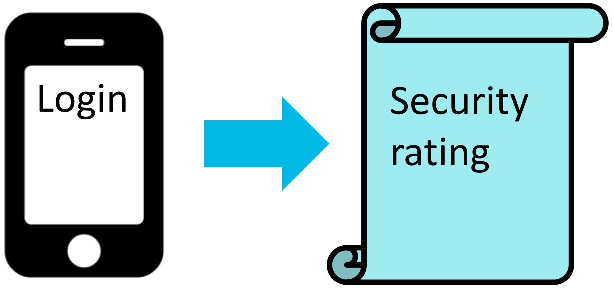
- Design
  - Select requirements
  - Get design suggestions



Requirements
- Security
- Availability
- …

Login

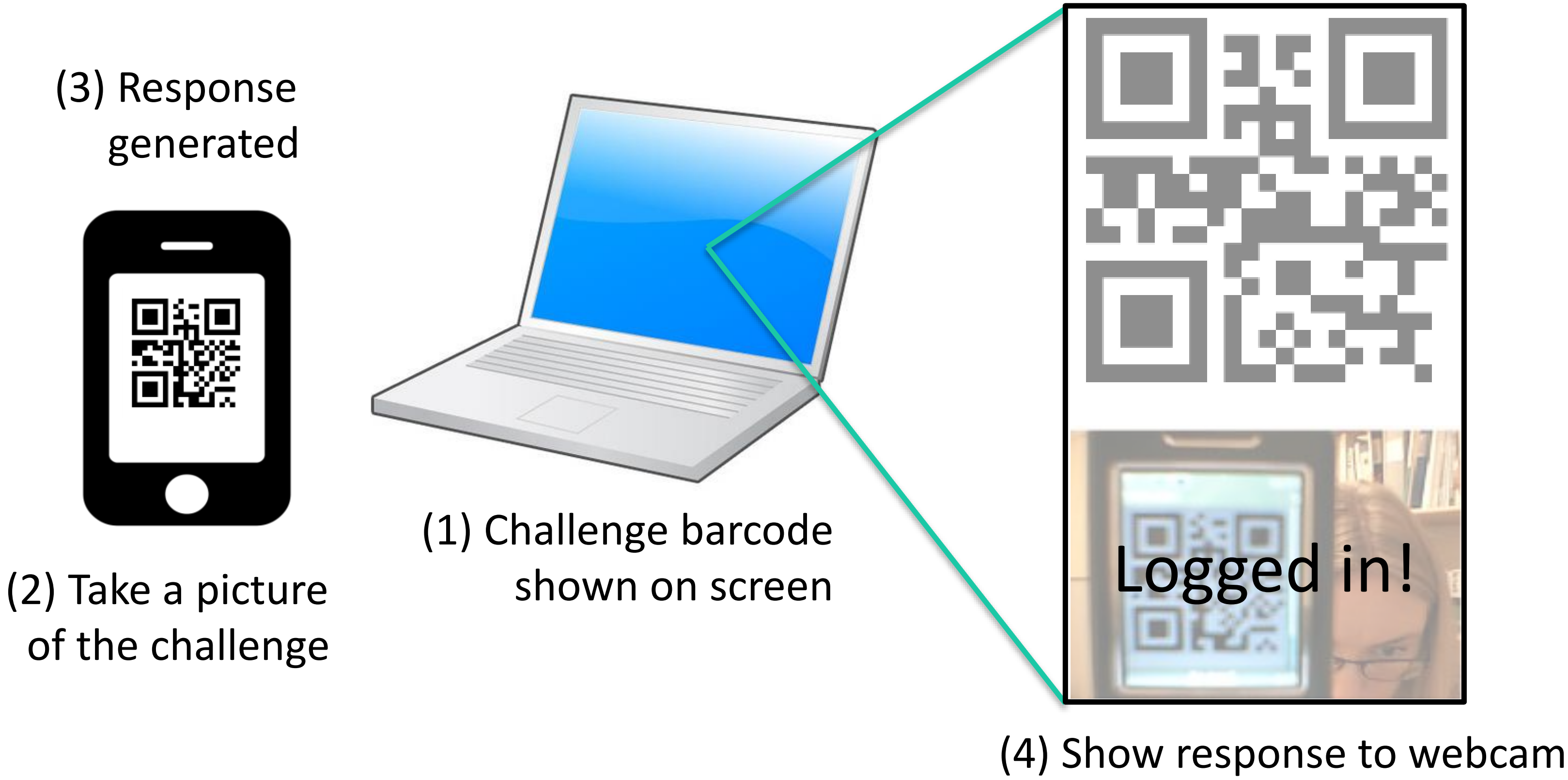
- Evaluation
  - Start with an existing design
  - Get a security rating of the design



Login

Security rating

Optical Authentication Proof-of-Concept



(3) Response generated

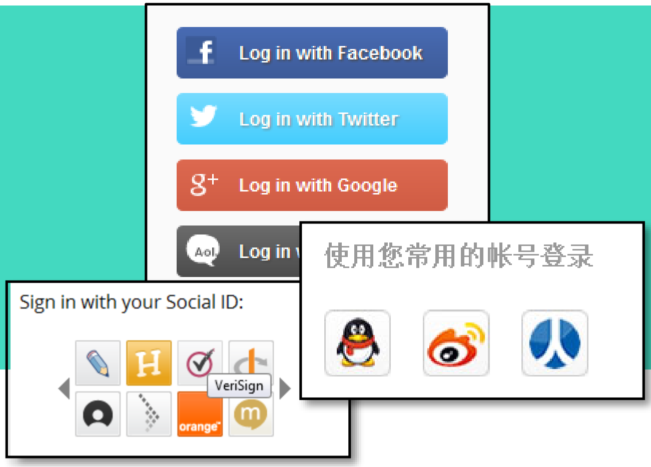
(2) Take a picture of the challenge

(1) Challenge barcode shown on screen

Logged in!

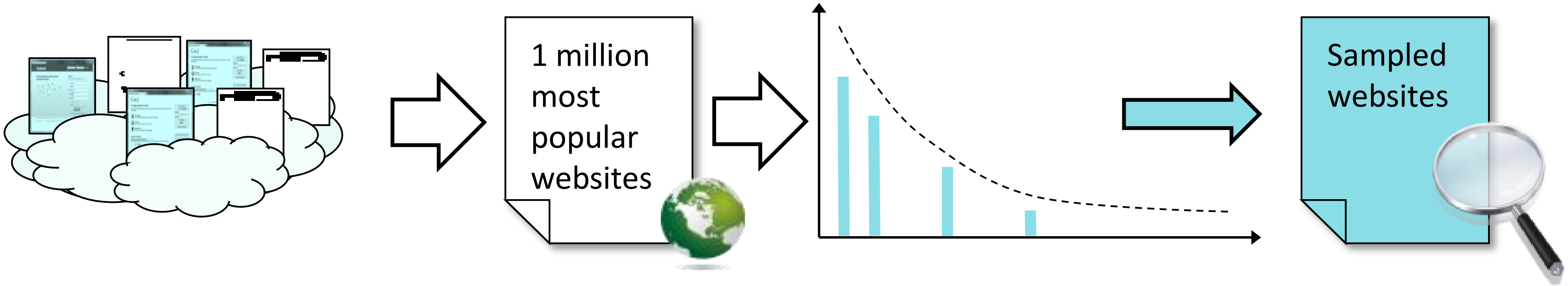
(4) Show response to webcam

The Third-party Authentication Landscape



Data Collection

- Popularity-based logarithmic sampling
  - 80,000 points uniformly on a logarithmic range
  - Pareto-like distribution
  - Capturing data from different popularity segments

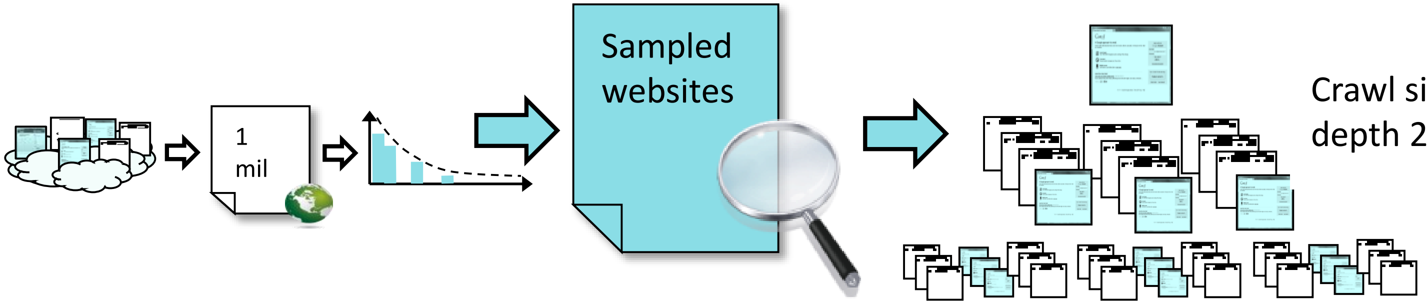


1 million most popular websites

Sampled websites

Large-scale Crawling

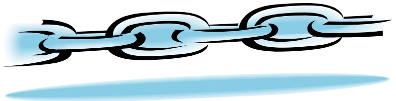
- Selenium-based crawling and relationship identification
- Able to process Web 2.0 sites with interactive elements
- Low number of false positives
- Validation with semi-manual classification and text-matching

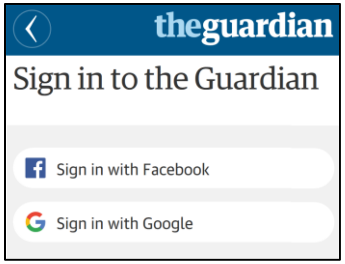


Collected Data

1.6 terabyte
analyzed data

25 million
analyzed links





theguardian

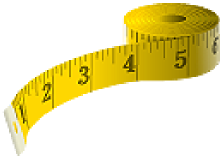
Sign in to the Guardian

Sign in with Facebook

Sign in with Google

3 329 unique relationships
50 IDPs and 1 865 RPs

WHOIS, server location,
and audience location



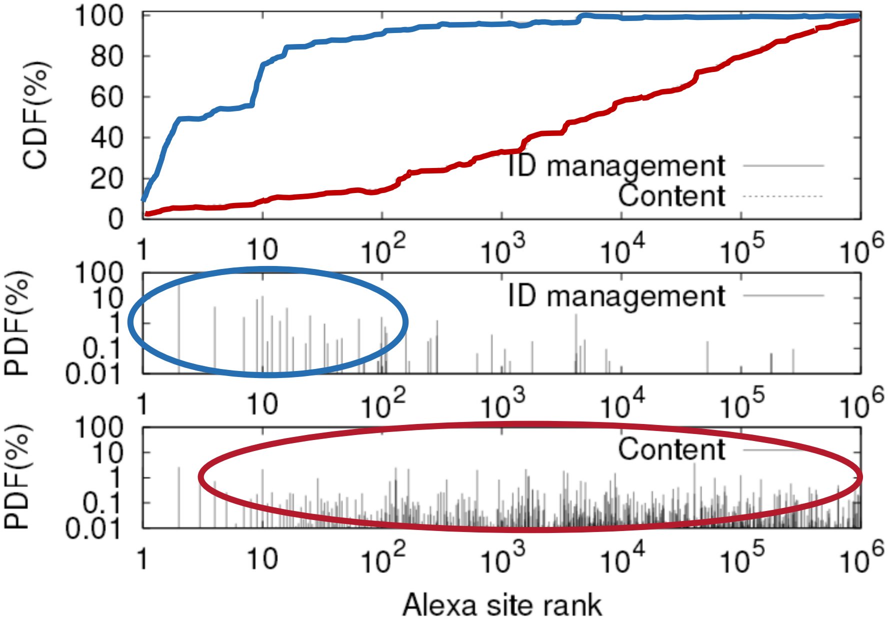
Total site size and number
of links and objects

PAM'14, IC'16

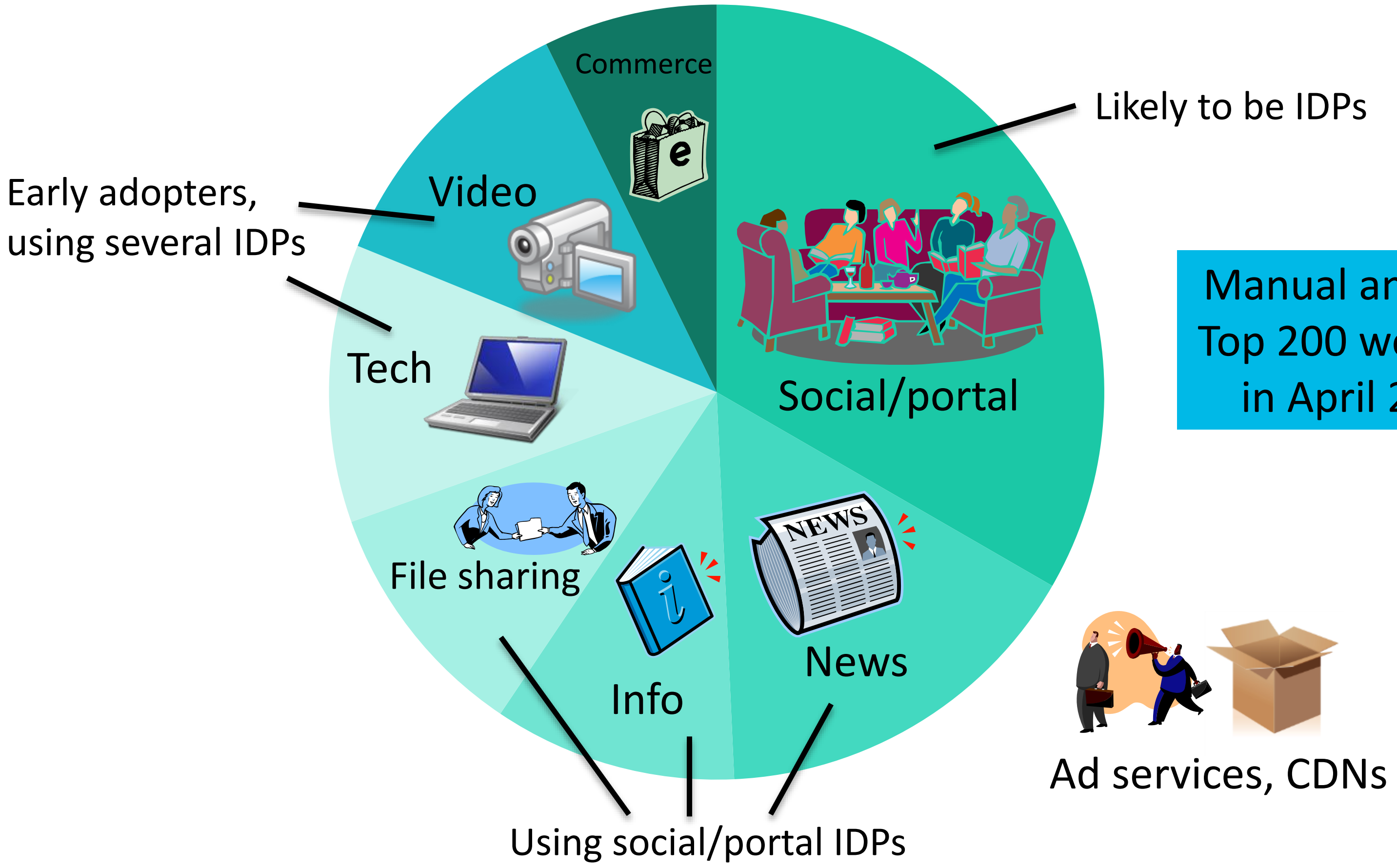
IDPs vs Content Sharing Services

Content sharing: Importing images, scripts etc. from other sites (third-party content providers)

IDPs are selected locally, in contrast to content services.



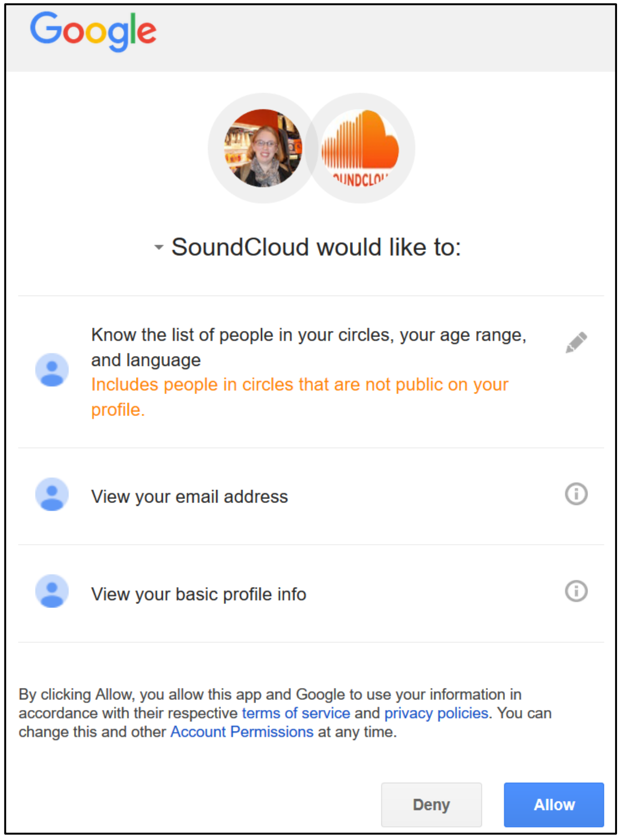
Service-based Analysis of RPs



Manual analysis: Top 200 websites in April 2012

Third-parties and Privacy Risks

App Rights and Information Flows



SoundCloud would like to:

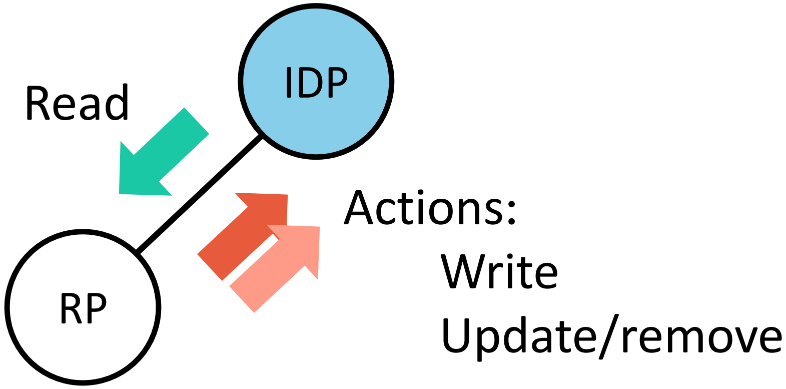
Know the list of people in your circles, your age range, and language
Includes people in circles that are not public on your profile.

View your email address

View your basic profile info

By clicking Allow, you allow this app and Google to use your information in accordance with their respective terms of service and privacy policies. You can change this and other Account Permissions at any time.

App rights example



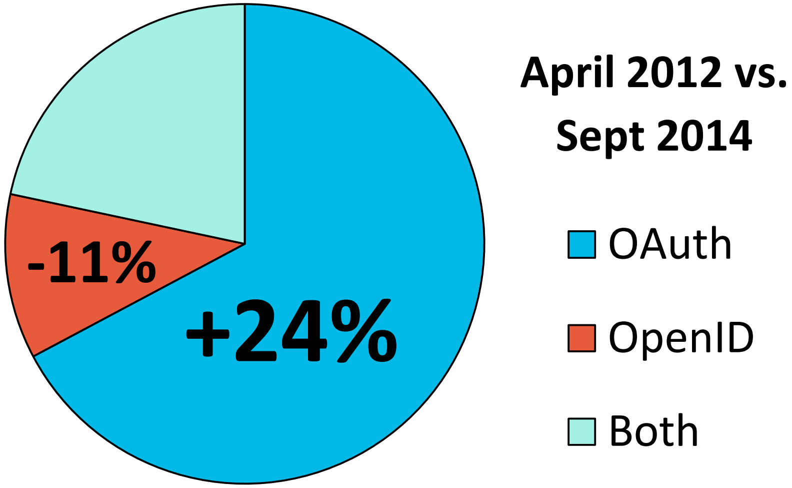
SEC’15, UEOP’16

Our Studies on Privacy Risks

- Categorization app-rights data
  - Manual study on the top 200 most popular websites
  - Longitudinal approach: three years
- Targeted login tests
- Privacy risk categorization
  - Data types in app rights
  - Combinations of types

Protocol Selection

- OpenID
  - Authentication protocol
  - Decreasing in popularity
- OAuth
  - RP may use actions on IDP
  - Rich user data is shared
  - Increasingly popular



IDP Selection

- Top 200 April 2012: 69 RPs and 180 relationships
- Same sites, April 2015: **+15** RPs and **+33** relationships
- **75%** of these RPs are selecting all their IDPs from the **top 5** most popular IDPs

Top IDPs: f 🐦 🐧 G Y!

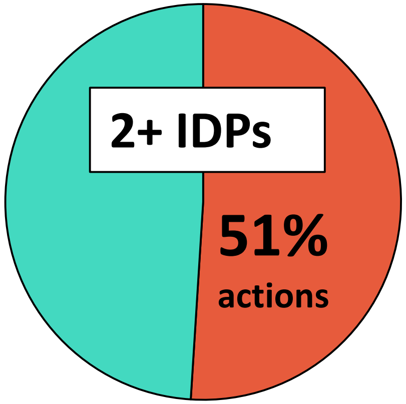
f + 🐦	37%
🐧 + sina	19%
f + G	12%

SEC'15, UEOP'16

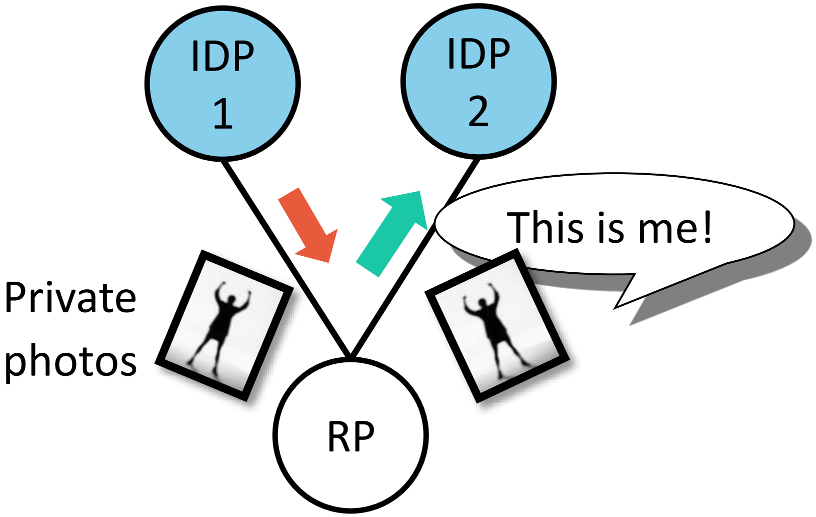
Risk Types

Facebook, Twitter and Google:

- Only a few relationships in the most privacy preserving category
- 2+ IDPs: More than half are using actions
  - Dangerous when having several IDPs
  - Potential multi-hop leakage



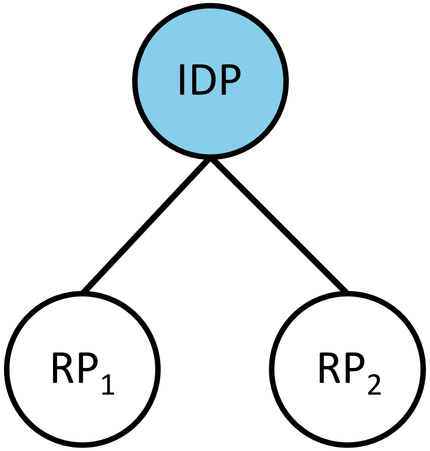
Multi-account Information Risks



Connecting several IDPs to an RP

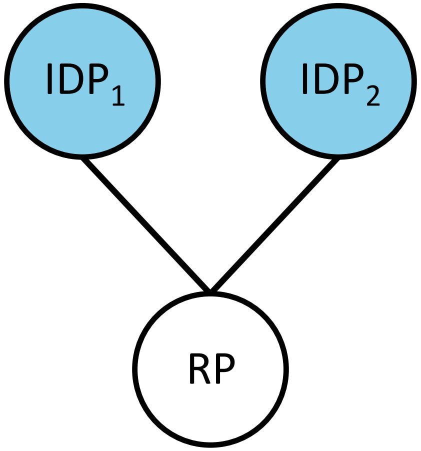
- Cross account leakage
- Unwanted combinations of conflicting information
- RPs handle multi-IDP usage badly

Structures in the RP-IDP Landscape



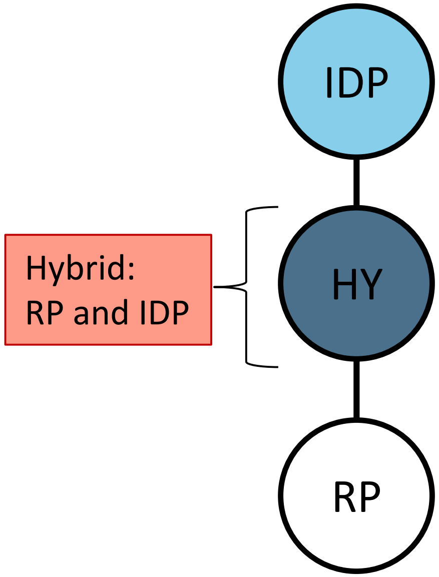
High-degree IDP case

- IDP having many RPs
- Top IDPs



High-degree RP case

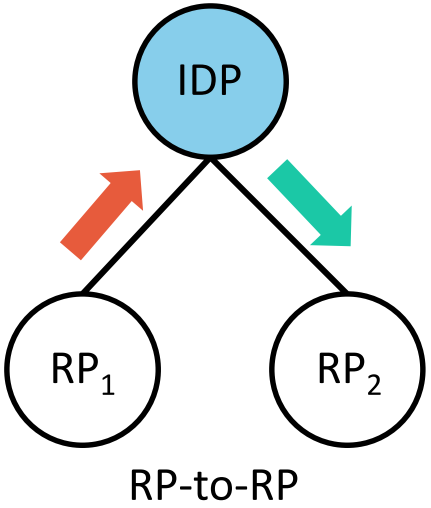
- RP having many IDPs
- Specialized IDPs



Hybrid case

- Hybrids are both RP and IDP

RP-to-RP Leakage Example



RP-to-RP leaks	February 2014		April 2015	
IDP	**All**	**Severe**	**All**	**Severe**
Facebook	645	150	473	66
Twitter	110	110	110	110
Google	91	0	91	0

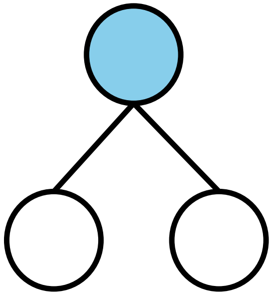
Dataset with 44 RPs using Facebook, 14 using Twitter and 12 using Google

- Potential RP-to-RP leaks
  - Data posted to IDP from RP1
  - Data read from IDP to RP2

Contributions

Contributions

- Design and evaluation method
- Large-scale RP-IDP measurements
  - Novel measurement method
  - Categorization of RP-IDP relationships
- Privacy risks and information sharing
  - Protocol analysis
  - Structural properties



Web Authentication using Third-parties in Untrusted Environments

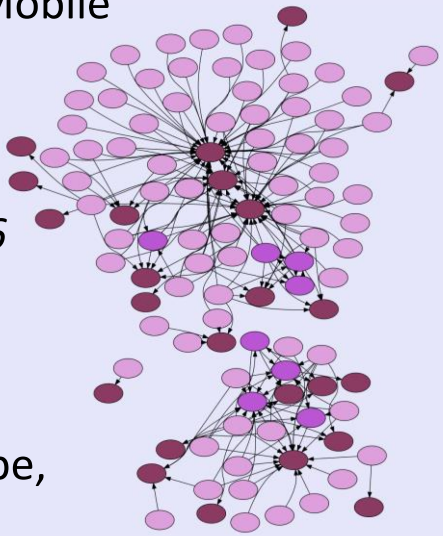
Anna Vapen

Papers included in this thesis:

- Security Levels for Web Authentication using Mobile Phones, *PrimeLife'11*
- 2-clickAuth - Optical Challenge-Response Authentication using Mobile Handsets, *IJMCMC'11*

- Third-party Identity Management Usage on the Web, *PAM'14*
- A Look at the Third-Party Identity Management Landscape, *IC'16*

- Information Sharing and User Privacy in the Third-party Identity Management Landscape, *SEC'15*
- Longitudinal Analysis of the Third-party Authentication Landscape, *UEOP'16*



LINKÖPING UNIVERSITY

ELLIIT