Fine-grained Access Control & Photo-based Social Authentication for OSN

Foundation for Research and Technology – Hellas (FORTH)
Panagiotis Ilia

Problem of "Conflict of Interest"

Privacy settings of shared photos are set by the owner.

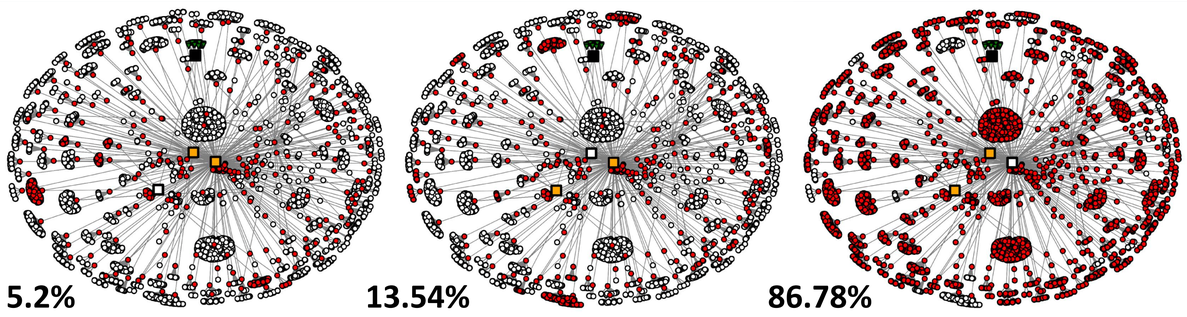
Related Users (tagged/depicted) not considered as co-owners.

→ not given any rights on controlling access on shared data

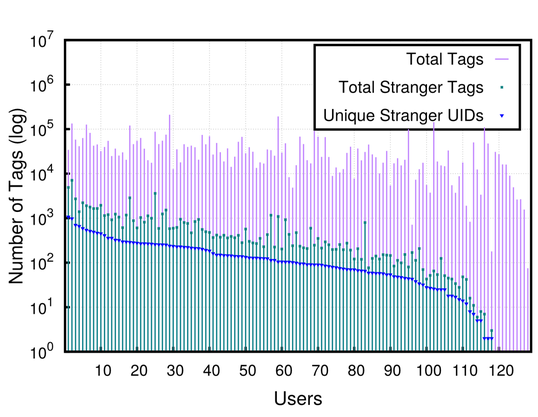
→ exposed to non-intentional risk (access given by others).

Privacy Risk Modelling and Analysis

$$PR(i) = \sum_{t=0}^{l} \beta_t \times Vis(i,t), \quad where \quad Vis(i,t) = \bigcup_{j=1}^{k-1} AL_{jp}, \quad U_i \notin k, \qquad \forall\ p \in \mathrm{t}$$

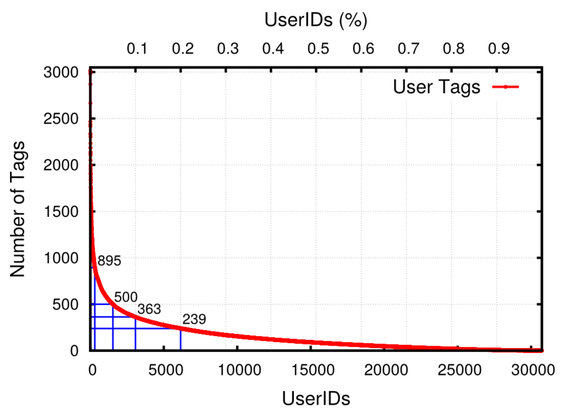


Progression of Risk for a photo accessible to "friends of a friend"



Number of tags per group of friends, number of tags belong to non-friends (strangers)

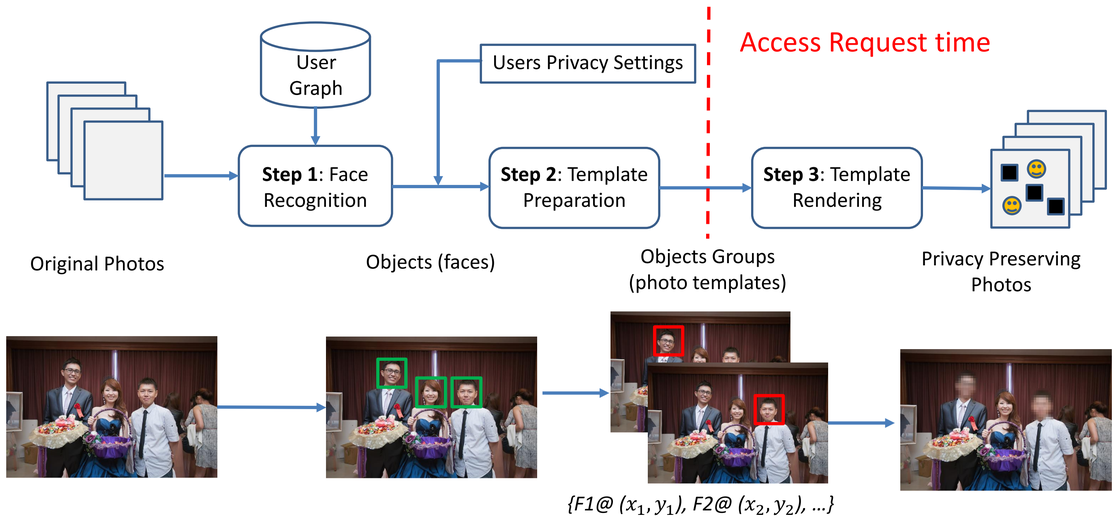
Tagged Strangers gain access to these photos



Number of tags individual users have, in friend's photos they do not own.

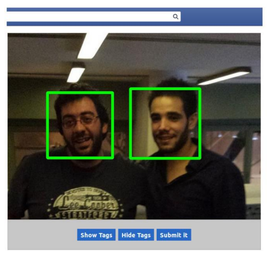
Cannot restrict access to these photos

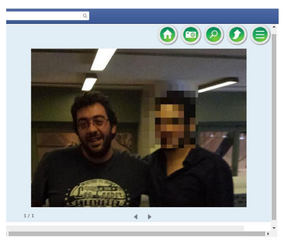
Fine-grained Access Control Model



Performance Evaluation

- Fine grained access control mechanism.
- Can be easily implemented on top of the existing access control mechanisms (no dependencies).
- Template preparation once, in the background
- Process a copy of the original photo "on the fly".
- Average time for tag processing 0.0023 second
- Average time for populating a photo 0.052 second.





Social Authentication

An alternative two-factor authentication mechanism.

Users should correctly identify their friends to log-in.
(7 pages, 3 photos per page & 6 name suggestions)

→ An attacker collects all the photos of a user and of his friends, for being able to break social authentication.

Contribution

- Demonstrate two efficient attacks on social authentication
- User study to verify users ability to identify their friends.
- Design a secure and usable social authentication system.
- Assess performance and verify usability of the system.

User study

Simple (98.89%)

Medium (99.14%)

Difficult (82.09%)

Users identify their friends even when their faces are not clearly visible, based on secondary features, associative information or memory retrieval

Attacking SA mechanism

Simplistic pixel-based image comparison attack

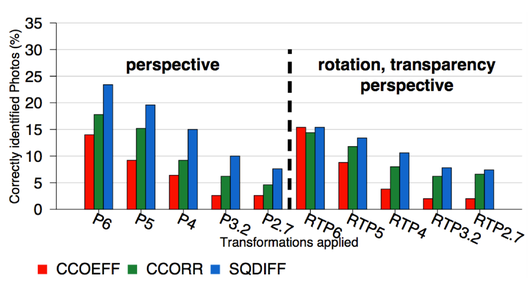
- Collections of up to 40k photos, 100 SA challenges (21 photos).
- **98.4%** photos identified (worst case 18/21), **0.06 sec** per photo.

Tag-based template matching attack

- CCOEFF, CCORR, SQDIFF template matching algorithms
- 500 challenges, 100% correct, **6.89 sec** per photo

Secure Social Authentication

- Random background photo
- Tag transformations
  (rotation and transparency)
- Photo transformation
  (change photo perspective)



Tags	alpha	CCOEFF	CCORR	SQDIFF	Time (sec)
2	0.8	0.0%	2.1%	1.8%	397.7
	0.7	0.0%	1.9%	1.6%	400.6
	0.6	0.2%	1.5%	1.0%	401.5
3	0.8	0.0%	0.0%	0.0%	663.6
	0.7	0.0%	0.0%	0.4%	675.0
	0.6	0.0%	0.4%	0.0%	695.9

Photo contains 2 and 3 tags

- Success rate for **2 tags ~ 2.1%,** for **3 tags ~ 0.4%**
- Requires four orders of magnitude more processing effort for the attack
- Usability: Users identification rate ~ 94%

FORTH Foundation for Research & Technology - Hellas

pilia@ics.forth.gr