Community Based Identity Validation

Model & Opportunities for Collaboration

By: Leila Bahri

Supervised by: Prof. Elena Ferrai & Prof. Barbara Carminati

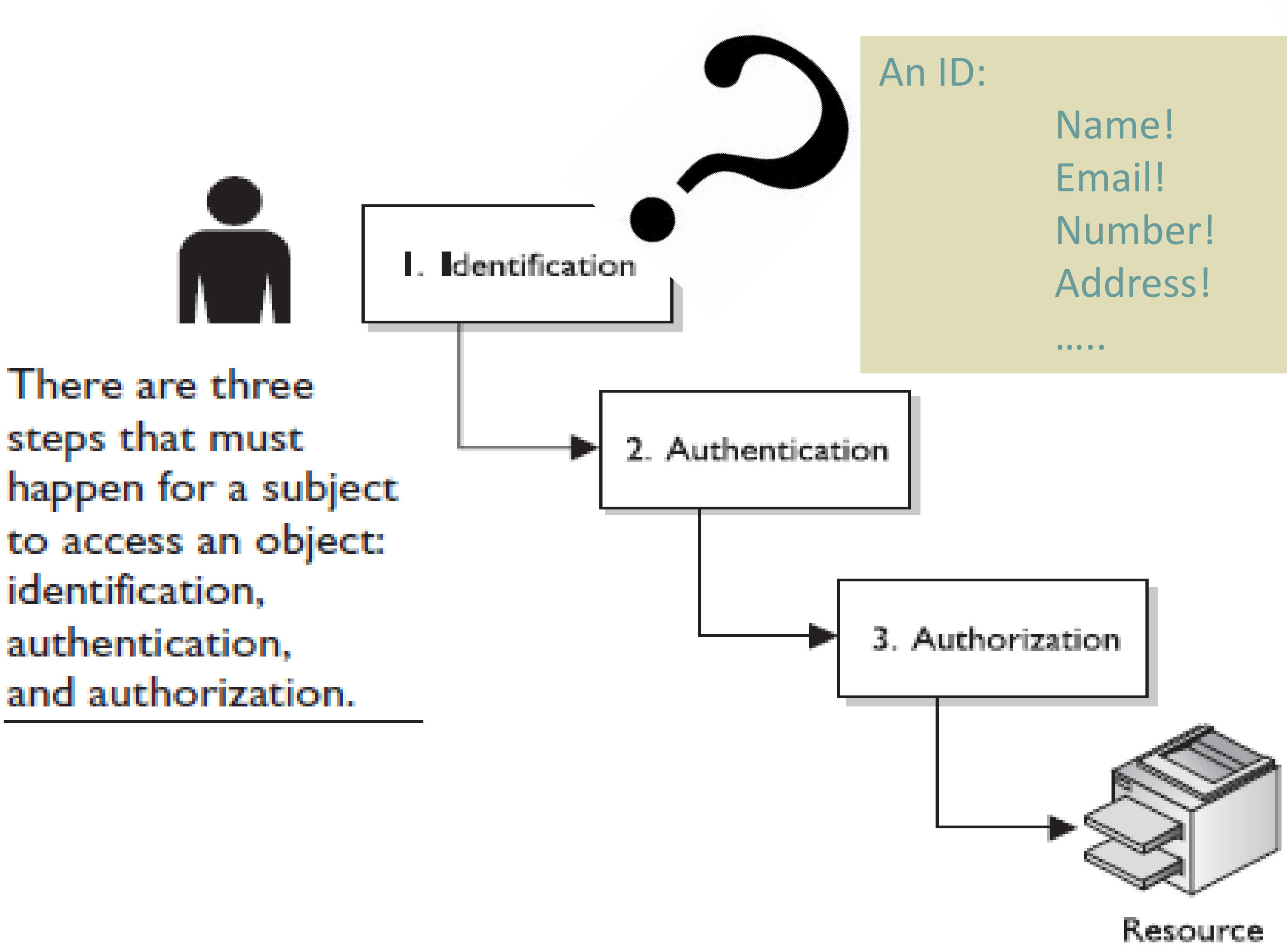
iSocial meeting

Stockholm, February 2014

Outline

- *Motivation*
  - *Identity within Access Control*
  - *Previous work*
  - *Research Question*
- *Observation, Hypothesis, Concerns*
- *The CBIV Model*
- *Preliminary Experiments and Results*
- *Future Work*
- *Opportunities for collaboration (KTH)*

Access Control in 3 steps



An ID:

- Name!
- Email!
- Number!
- Address!
- .....

Identity related issues on OSNs

- Different types of attacks:
  - Sybil
  - Identity theft
    - Cloning
- Fake accounts for varying purposes: Facebook releases that 5% to 6% of registered accounts are fake

- → There is unreliability!
  - users do not have, or rarely do have, a mean to reliably identify the person behind the account

Identity validation in OSN – what for?

- OSNs = arena for creating and maintaining social ties
    - One of the main requirements for trust to occur is to be sure of the identity of each other!

- OSNs = environment for declaring and developing identities
    - Veracity is not verifiable:
        - privacy preservation
        - spoiled accounts
            - Identification misleads
            - Ineffective access control and privacy preservation mechanisms
    - Insecure environment

Previous works

- Most focus on **detecting** identity related frauds and attacks [14][15][16]
- Most **rely on the central system** to perform the detection and to take action
- **Few give users a mean to rate** the reliability/credibility of an account [17][18]
  - Mostly through relying on historical transactions or connections between participants
    - *Limitation 1:* Transaction scoped
    - *Limitation 2:* Connections' fraudulent - collusion

Research Question

- How can we validate identities of OSN users without relying on a central authority?
- Can we make use of the community to validate profile information?

Observation

- The more coherent an online profile is + the better this coherency is maintained over time, the more probable this profile is operated by a truthful identity [10]

Full name: Poe Pineapple
Gender: Male
Age: 31
Address: 12, Banana Street; Spring city; Fruits Land
Religious views: Citruism
Interested in: improving digestion, strengthening bones
Work place: Fun Juice factory
Education: Health and Nutrition University
Social status: married
Hobbies:
Sports:
Movies:
Music:
Country of origin: Fruits Land
Lives in: Fruits Land
Lived in: Fruits Land
Languages: Applian

Full name: Frya Straws
Gender: Female
Age: 18
Address:
Religious views: Complicated
Interested in: strength and body-building
Work place: Proteins production INC
Education: Aesthetics Professional School
Social status: single
Hobbies: sun-bathing
Sports:
Movies:
Music:
Country of origin: Veggies Land
Lives in: Flesh Land
Lived in: Veggies Land
Languages: Strawssian

Hypothesis & Concerns

- OSN community can collaborate to credibly rate the coherency of a target profile
- BUT
  - Profiles span multiple identity dimensions → where is coherency expected?
  - Quality of rates → who could rate what?
  - Collusions' risks
  - Privacy issues → sensitive information disclosure/leakage!

The CBIV Model - Overview

- What are the attributes for which the corresponding values can be rated for inter-coherency?
  - Correlated attribute groups identification
- How can these groups be identified?
  - A learning phase is needed
- Who is to rate what?
  - Raters' selection is a requirement
- How to rate a target profile based on the above
  - An evaluation phase emerges

Let's exemplify it…

Summary:

- ✓ We need to identify the correlated attributes
- ✓ We need to know the direction of the correlation

Resemblance:

- ❑ The problem sounds similar to Association Mining for Basket Analysis

Question:

- ➢ How can we detect the correlated attributes?
  - Can we count the frequency of occurrence of similar values?!
  - Can we mine people's knowledge/feedback?

The CBIV Model – Learning Phase 1/2

Correlated Attribute Groups: *a group of attributes for which the values can be rated as coherent to each other or not by an informed person.*

The CBIV Model – Learning Phase 1/2

<u>How to find correlated attribute groups?</u>

<u>Learn them from trusted users' feedback on learning profiles dataset</u>

- Do you think the following values can belong to a true identity altogether?
  - *Job = Fun fruits factory, project m*
  - *Education = Health and Nutrition* Σ *uate*
    - *Definitely YES*
    - *Definitely NO*
    - *Most Probably*
    - *Less Likely*
    - *Not meaningful to judge / I do not know*

1 Σ

0.5

0

Σ → **Support**

The CBIV Model – Learning Phase 2/2

Coherence Relation: *an implication between the elements of a correlated group based on which the coherence of their corresponding values is to be rated. Such an implication will define the raters selection on the given correlated group.*

Who is to better judge the coherency of this combination?

- *Job = Fun fruits factory, project manager*
- *Education = Health and Nutrition Univ Graduate*

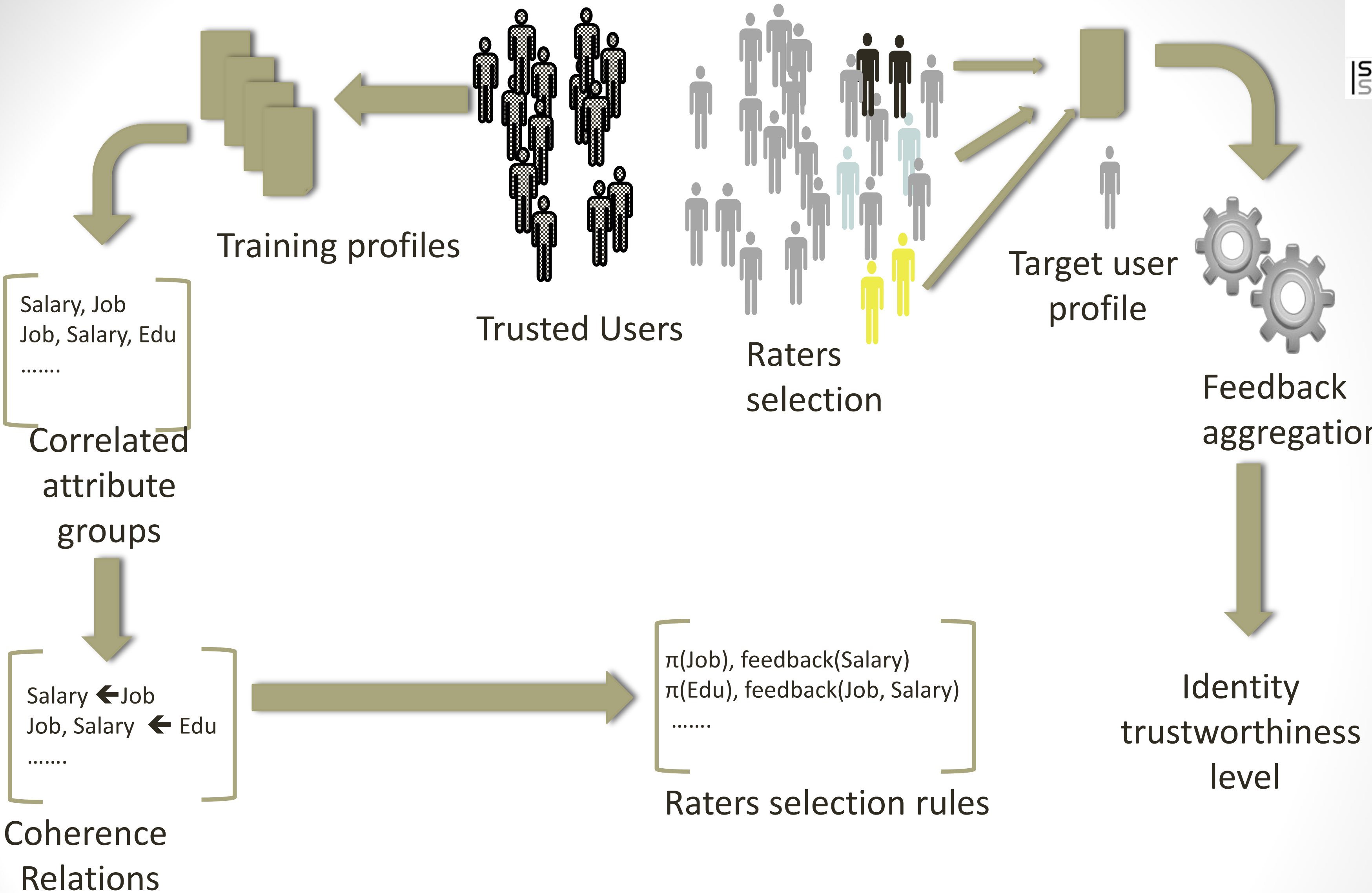
Support(Job/Education)
vs.
Support(Education/Job)

→ **Confidence**

The CBIV Model– The Evaluation Phase

- Goal: compute an **ITL** (Identity Trustworthiness Level) from user feedback for a target profile given a set of **correlated groups** and **coherence relations** on them

- Method:
  - For every correlated group
    - Perform raters' selection based on corresponding coherence relations
    - Gather selected raters' coherency feedback for the values on the target profile corresponding to the elements of the correlated group
  - Aggregate the feedback on all the correlated groups and make the **ITL**



Learning the correlated attributes

Evaluation of target user profile

Performed experiments - dataset

- Adults dataset from US Census Bureau
  - Contains 45222 records spanning 14 attributes
- 11 out of the original 14 attributes have been considered

Attribute	Description
Age	Age
Work-class	Work Class
Education	Education Level
Educ-num	Number of years spent at school
Marital-status	Marital Status
Occupation	Job
Social-role	Social Role
Race	Race
Sex	Gender
hrsperweek	Number of hours worked per week
Country	Country of origin

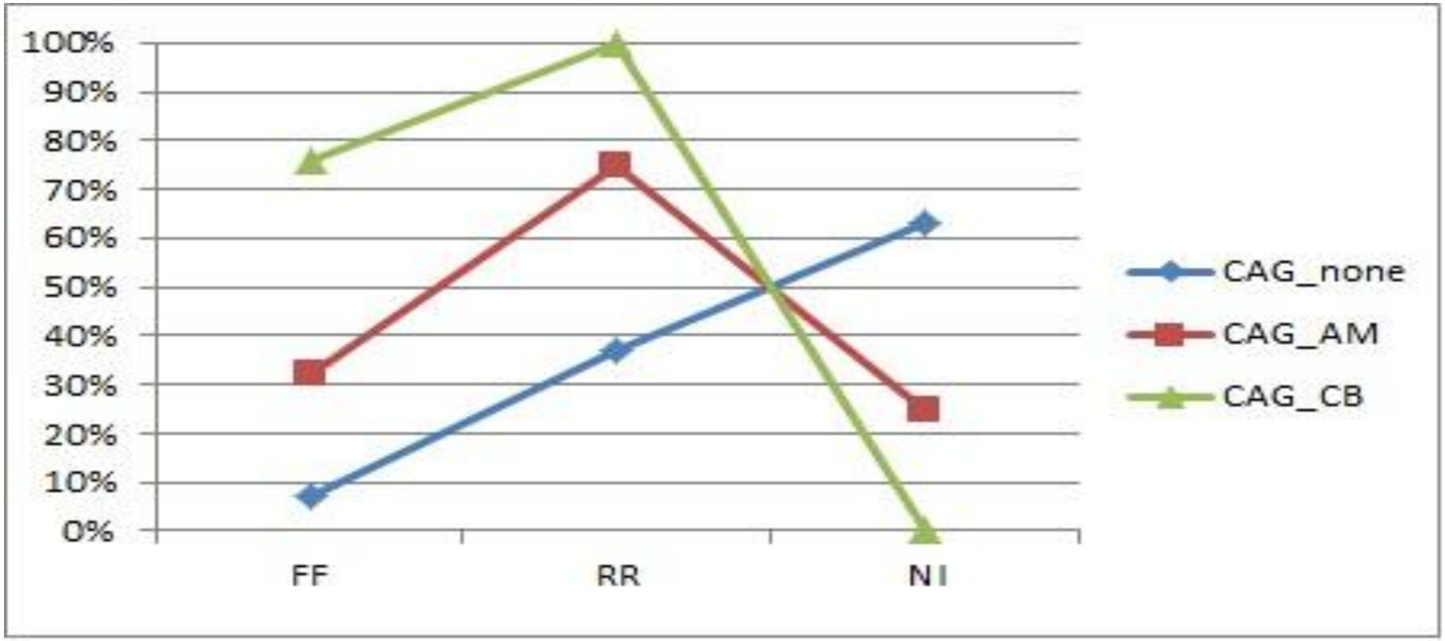
TABLE I : Attributes of the profile schema adopted in the experiments

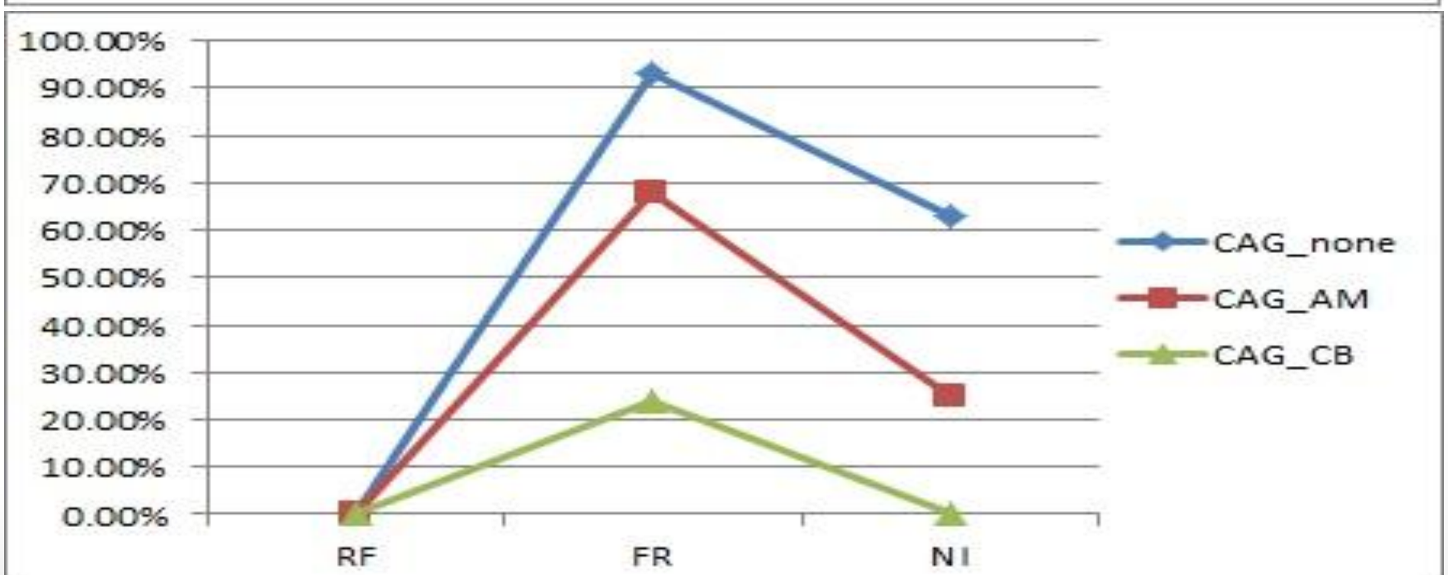
Identified correlated groups– CB vs. AM

Candidate Group	Supports AM	Supports CB
educ-num, gender	0.36	insig
hrsperweek, gender	0.66	insig
educ-num, race	0.34	insig
hrsperweek, race	0.36	insig
gender, race	0.44	insig
educ-num, social-role	0.29	insig
hrsperweek, social-role	0.30	insig
gender, social-role	0.38	insig
educ-num, marital-status	0.27	insig
hrsperweek, marital-status	0.26	insig
gender, marital-status	0.36	insig
gender, education	0.25	insig
educ-num, work-class	0.29	insig
hrsperweek, work-class	0.30	insig
gender, work-class	0.37	insig
race, work-class	0.21	insig
educ-num, age	0.28	insig
race, age	0.21	insig
gender, age	0.37	insig
hrsperweek, age	0.35	0.56
social-role, marital-status	0.21	0.56
educ-num, education	0.37	0.52
education, hrsperweek	insig	0.66
age, marital-status	insig	0.58
education, occupation	insig	0.59
occupation, hrsperweek	insig	0.67
occupation, educ-num	insig	0.63
occupation, work-class	insig	0.63
country, race	insig	0.56
work-class, educ-num	insig	0.57

TABLE II : Candidate groups considered as correlated attributes either by CB or by AM method

Performance results





The CBIV Model – Privacy issues

- Exclude the quasi-identifier attributes from all the reasoning of the model
- … not enough
- K-anonymity shall be ensured…
  - Is it enough?!

The CBIV Model – Future Works

- More experiments on real environment
- Address privacy issues
- Weighted / multi-dimensional **ITL**
- Revise the model to fit the requirements of a decentralized architecture

The CBIV Model – Collaborations

- CBIV on a decentralized architecture using Gossip learning

Amira has addressed that…

This model has been formalized and submitted for a paper review to the **International Conference on Distributed Computing Systems-ICDCC 2014**

http://lsd.ls.fi.upm.es/icdcs2014

References...

- [1] Vandell, Deborah. L, *Parents, peer groups, and other socializing influences.* Development Psychology, Vol 36(6). 2000.
- [2] Pascal. S, Joachim. G, *Organizational Virtualness.* Proc. of the VoNet - Workshop. 1998.
- [3] C. L. Corritoire, B. Kracher, S. Wiedenbeck, *On-line trust: concepts, evolving themes, a model.* International Journal of Human- Computer Studies, Vol. 58, no. 6, pp. 737 - 758. 2003.
- [4] Nikolaos Volakis, *Trust in Online Social Networks.* University of Eidenberg. 2011.
- [5] H. Nissennbaum, *Securing trust online: Wisdom or Oxymoron.* BUL Rev, Vol. 81. 2001.
- [6] Squicciarini. A. C, Griffin. C, Sundareswaran. S, *Towards a Game Theoretical Model for Identity Validation in Social Network Sites.* IEEE International Conference on Privacy, Security, Risk, and Trust. 2011.
- [7] E. Martinez, *Alexis Pilkington brutally cyber bullied even after her suicide.* http://www.cbsnews.com/8301-504083-162-20001181-504083.html. 2010.
- [8] H. Bray, Griffin. C, Sundareswaran. S, *Privacy still a nagging concern on Facebook.*
- http://www.boston.com/business/technology/articles//2010/02/04/privacy still a nagging concern on facebook/. 2010.
- [9] S. Barnes, Griffin. C, Sundareswaran. S, *Social networking in the united states. First Monday. A privacy paradox* [Online], 11(9). 2006.
- [10] Ljung, A and Wahlforss, E, Griffin. C, Sundareswaran. S, *People Profiles and Trust On Interpersonal Trust in Web-mediated Social Spaces.* [Online], available at: http://trustmojo.com. 2008.
- [11] Michael J. A. Berry, Gordon S. Linoff, *Data Mining Techniques.* Copyright 1997 by John Wiley and Sons. ISBN 0-471-47064-3. 2007.
- [12] S. de Capitani di Vimercati, S. Foresti, *Quasi-Identifier.* Encyclopedia of Cryptography and Security: SpringerReference. [Online].
- [13] R. Agrawal, R. Srikant, *Fast Algorithms for Mining Association Rules.* IBM Almaden Research Center. Proc. of the 20th VLDB Conference Santiago, Chile. 1994.
- [14] B. Viswanath, M. Mondal, A. Clement, P. Druschel, K O. Gummadi, A. Mislove, A. Post, *Exploring the design space of social network-based Sybil defenses.* IEEE Fourth International Conference on Communication Systems and Networks (COSNETS). 2012.
- [15] G. Guette, B. Ducourthial, *On the Sybil attack detection in VANET.* IEEE International Conference on Mobile Adhoc and Sensor Systems (MASS). 2007.
- [16] L. Jin, H. Takabi, J B.D. Joshi, *Towards Active Detection of Identity Clone Attacks on Online Social Networks.* Proc. of the first ACM conference on Data and Application Security and Privacy (CODAPSY). 2011.

References…

- [17] X. Cai, M. Bain, A. Krzywicki, W. Wobcke, Y. S. kim, P. Compton, A. Mahidadia, *Collaborative Filtering for People to People Recommendation in Social Networks.* Advances in Artificial Intelligence: Lecture Notes in Computer SCience Vol, 6464. SpringerLink. 2011.
- [18] M. Sirivianos, K. Kim, J. W. Gan, Yang, *Assessing the veracity of identity assertions via OSNs.* IEEE 4th International Conference on Communication Systems and Networks (COMSNETS). 2012.
- [19] Roffo, Giorgio, Segalin, Cristina, Vinciarelli, Alessandro, Murino, Vittorio, al. *Reading between the turns: Statistical modeling for identit recognition and verification in chats.* IEEE 10th International Conference on Advanced Video and Signal Based Surveillance (AVSS). 2013.

- [20] L. Dehache, L. Souici-Meslati, *A multibiometric system for identity verification based on fingerprints and signatures.* IEEE International Conference on Complex Systems (ICCS). 2012.
- [21] P. Chairunnanda, D. R. Cheriton, N. Pham, U. Hengartner, *Privacy: Gone with the Typing! Identifyin Web Users by Their Typing Patterns.* IEEE 3rd International Conference on Social Computing. 2011.
- [22] A. S. Bozkir, S. G. Mazman, E. A. Sezer, *identification of User Patterns in Social Networks by Data Mining Techniques: Facebook Case.* Technological Convergence and Social Networks in Information Management, Vol, 96. 2010.
- [23] Y. Yang, E. Lewis, J. Newmarch, *Profile-based digital identity management - a better way to combat fraud.* IEEE International Symposium on Technology and Society (ISTAS). 2010.
- [24] TOGAF, *TOGAF version 9.1.* [Online] available at: www.togaf.org. 2013.
- [25] M. Kosinski, D. Stillwell, T. Graepel, *Private traits and attributes are predictable from digital records of human behavior.* Proc. of the National Academy of Sciences of the USA. [online]. 2012.
- [26] S. Vijayarani, A. Tamilarasi, M. Sampoorna, *Analysis of privacy preserving k-anonymity methods and techniques.* IEEE International Conference on Communication and Computationa

Thank you for your attention…