Trust and trustworthiness in online profile-based social networks

David Zejda david@zejda.net

University of Hradec Králové

Faculty of Informatics and Management

Abstract

As popularity of online social networking sites such as Facebook grows, more users are joining and further activities within the sites are becoming quite natural extension of their social life, the overall dynamics of the sites gets to higher levels. With recent incidents on mind, importance of better trust solutions in the systems is increasingly apparent. What are possible sources of trust, how can be the trust captured into systems and how can be processed? Could we infer a level of indirect trust between users who do not know each other yet? We also describe trustworthiness as a per-community relevant or system-wide metric of reliability of certain user. In the conclusion we point out some current challenges related to trust matters and also we recommend publications worth of reader's further attention.

Key words

trust, trustfulness, trustworthiness, social networks, social networking, inferred trust

Trust and social networks

Trust may be defined as “the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party.” [MAYER95] In the real life we deal differently with trusted people than with strangers. A level of trust which we feel towards someone helps us to decide how thoroughly check his proclamations or promises. We rely on trusted people. Trust emerges from our experiences with the person and also from recommendation or guarantee from those, who we trust already.

We all belong to a global-world village with a small world phenomenon, where everyone is connected with anyone else through only several steps of relations [PAVL09]. New social strategies are necessary to cope with a social and information overload [WALT07]. Web becomes not only bigger every year, but also semantically richer and more and more driven by a community. Besides milieu for implicit socialization [WENN06], it provides dating sites, community portals and social networking sites, such as Friendster or Facebook, where people not only specify their friends, but they also maintain an explicit profile of interests and passions [LIU05].

In a virtual space we actually miss many relevant non-verbal indices which usually help us in the process of trust formation. We do not see the person in real, sometimes we even do not see him at all. It is also more likely that there are no other trustful people around who could share their opinions based on direct personal experiences. Dozens of people have joined social networking sites so far, whereas reputation of the sites has been affected by many incidents. Is it possible to join a site with millions of users and trust all of them? Of course not. Though there are risks and we may say well known risks, many people are still being attracted to not only join, but also communicate carelessly, and even reveal quite personal information [DWYE07]. To avoid further disillusion, incidents, frauds we are really in need of a good trust management. Trust has a key role in a social exchange theory [ROLO81]. Once captured, it may be utilized in many ways. For example [GOLD09] points out application in recommender systems, website access control systems and message filtering. Trust is also pivotal for successful online interactions [COPP04] and of course in social relationships [FUKU95].

Explicit trust

Trust is being gained, lowered or even lost. In general, trust grows slowly, but falls sharply [WALT07]. It may take months or years before you trust someone. A single act of betrayal destroys the trust to the roots. Algorithms used by social networking sites should reflect this behaviour. Besides positive trust expressions users should be granted with means to both withdraw the trust expressed already and express loss of confidence, distrust instead. Explicit distrust may be utilized by site maintainers to reveal malicious users, such as scammers or other betrayals. For further examination of the case it may be useful to allow or even require to provide reasons for the distrust expression.

What are common sources of trust among users within social networking systems? Online transactions are only technically flavoured variants of similar transactions usually performed as off-line in real world, without the technical support. [DWYE07] Existing trust may be captured from a real social background by technical means and mapped into the system [WALT07]. If you personally invite someone to join a networking site, you probably know him and trust him, at least at certain level.

Besides this, new trusted friendships may arise out of vital interactions within the site, usually during some period and based on certain level of interaction. Zheng et al. [ZHEN04] redefine trust as “trustor A trusts trustee B for purpose P under condition C based on root trust R”. The main difference is in the element C, condition to trust. Trustor should be informed about any distrustful behaviour of the trustee according to the conditions and a trust is considered as something dependant on the conditions. Level of trust considered sufficient for certain purpose differs. [ZHOU08] Trustors may have different personal preferences and requirements on a time and deepness of communication before falling into trust. The preferences may depend on many factors – on type of relationship or transaction, on previous history of the possible-trustee within community, and so. Last to mention, similarity is not equal to trust, of course, but correlation between similarity and trust evolves quite often [WALT07], thus some matching functions may help users to find prospective trustees.

Trust, both explicitly expressed and revealed by inference, one captured may be represented as binary value (do trust – do not trust), as discrete scale (levels of trust), real scale, usually normalized into certain interval.

From explicit to inferred trust

How to find out, how trustful is certain user from a perspective of other user, when they are not related yet? E.g. in recommender system – how relevant and trustful are recommendations of others to the one who is in search for an advice? If we are asking a such question we are indeed in need of some metric of indirect trust.

Social network forms a graph with users as nodes and relationships between them as edges. For easier further complementary computations Walter et al. [WALT09] recommend to use the same range 0..1 for all trust-related variables including individual expressed trust, individual inferred trust or community-relevant trustworthiness or system-wide trustworthiness discussed later, so the values probably need some normalizations. Assuming the trust is transitive, the basic idea of indirect trust inference is to multiply trust values along the path between users. The multiplication effectively discounts the resulting value, thus those whom the user trusts already are being taken more seriously as a source of recommendations whom else to trust.

Walter et al. [WALT09] present fairly tuned metric. The algorithm does not reduce cycles in a graph before computation as most other algorithms do. In recommender system the algorithm gives best results when used to find recommendation for a different category of media than in which the user recommended already, such as when user who posted comments to cartoon movies asks for recommendation on drama. Hales at al. [HALE05] used similar algorithm to find cooperative routes among selfish agents acting as players in prisoner's dilemma in an environment with no central authority.

From individual trust to system-wide trustworthiness

Besides a personalized trust metric (individual trust either expressed or inferred), we may be in need of more general, either per-community related [PAVL09] or system-wide trustworthiness. Whereas trust is something between two people, with trustworthiness we mean overall reliability of the user, his credit, site-wide reputation. As a source of trustworthiness we may take activity of users within the system in the past, such as how many times the user failed to deliver goods ordered in auction or how often has been his wiki contribution re-edited. User's activity together with individual explicit trusts constitute a basis for trustworthiness inference. Apparently, more incoming trust increase the overall trustworthiness of certain user. We may either simply sum individual trusts or apply an eigenvector-type[1] algorithm [GOLD09] to weigh the individual values according to trustor's own trustworthiness. The trustor's trustworthiness may be viewed as a confidence of his own trust expressions [ZHEN07]. In result, trustworthiness of certain user is dependent on trustworthiness of his neighbours in the graph of trust [WALT09]. Not-yet-much-trustworthy users may be allowed to express their trust towards others, though these expressions are not treated as much relevant, until the trustors themselves gain enough trustworthiness. Eigenvector algorithms also take count of outgoing trust expressions into account. If user with certain trustworthiness expresses his trust towards a single user, the single expression is being considered as of greater value than if he trusts dozens of other users. Pavlovic [PAVL09] further recommends to take differences in user's attitudes towards trust into account also in normalization of their own trust expressions.

Trustworthiness may undergo transitions, such as from 'unknown' or 'not-yet-trustworthy' to 'trustworthy' when user reaches a threshold, defined either per-community or for the whole site. As a final step in systems with central authority an approval by site maintainers may be required. On the other end of it's life-cycle, the trustworthiness may be 'disputed' when the user loses confidence and the case is under consideration by site maintainers. Value of the withdrawal may be weighted by impeacher's current trustworthiness in comparison with trustworthiness of the user whose reliability has been disputed. Trustworthy users may be granted with more privileges, whereas users who are losing trustworthiness and becoming 'untrustworthy' lose the privileges in parallel. Further, if someone loses the trustworthiness, it automatically affects trustworthiness of those, who received his trust. These trust relations of the disputed user may be examined by maintainers to find either other victims (and maybe warn them or provide other assistance) or complices on the other hand.

Besides trust among users, also trust to media within system (the trust probably inferred from a trust to the owner of the media or his trustworthiness), trust to site maintainers [DWYE07], services provided by the system or to the system as a whole may be examined.

[1] One of well-known eigenvector-type algorithms is PageRank by Google.

Conclusions and challenges

There had been impressive visions of trustworthy Internet, such as Augmented Social Network [JORD03], where internet-wide persistent online identity across systems would facilitate reliable interactions of so called 'citizens of the Net'. A lot of work has been done to make Internet more trusty space already. We have security and trust authorities, security certificates, great algorithms, trust-related ontologies, whole area of trust management, some great systems. But seven years passed since ASN vision and Internet in general is not more reliable than before. The advancement is being effectively outweighed by more sophisticated efforts of deceivers.

- Scammers are increasingly more proficient, with both technical and social skills. You would probably never give money based on poorly written e-mail from Nigerian prince. But what if you are being contacted by your friend or relative, who has been coincidentally trapped somewhere without a coin? One of trends is impersonating or hijacking user profiles for scamming purposes.
- Social networks give good ground for cyberstalking or cyberbullying.
- Trust authorities are greatly vulnerable. [PAVL09]
- Power-law distribution where rich becomes even richer works in trust systems similarly – trusted nodes tend to receive even more trust. It leads to constitution of so called 'trust hub' [PAVL09], which is not necessarily bad, but it intensifies impact when a trust hub is being compromised.
- More work is needed to provide sufficient means for establishing trusty relationships where existing trusted social network is not present in the background. [HALE05]
- We have to deal with matters of trust in systems with steadily increasing dynamics, where millions of users are joining the networks, performing their activities there and leaving.
- We also have search for ways how to keep a network useful and sufficiently safe and trusty, despite activities of defective peers [HALE05] and agents with random, selfish or even malicious behaviour [WALT07].
- It will be furthermore a long path from system-wide trustworthiness to global trust identity.

Further reading

Zheng et al. [ZHEN07] has brought good state-of-the-art overview about characteristics of trust (p. 7), trust modelling (p. 4), classification of trustor/trustee/context properties (p. 7), or taxonomy of whole trust models (p. 10). To get even deeper into how trust emerges from its sources, dynamics of trust, profile-level or item-level per-community or system-wide relevant trustworthiness, delegation of trust and decision to trust, algorithms and methods for computing trust in social context with either group or eigenvector trust metrics, systems for trust management and other applications of trust, virtual identities, privacy questions, attack resistance of trust systems, redundant certification paths, failures of trust (distrust, mistrust, untrust, ignorance, lack of trust, regret, forgiveness) and feedback on acts such as eliciting effort and deterring frauds, I would recommend newly released book „*Computing with Social Trust*“ edited by Jennifer Golbeck [GOLD09].

References

COPP04: Coppola N., Hiltz S. R., Rotter N. - *Building Trust in Virtual Teams*, 2004 IEEE Transactions on Professional Communication 95-104

DWYE07: Dwyer C., Hiltz R. S., Passerini K. - *Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace*, 2007 Proceedings of the Thirteenth Americas Conference on Information Systems

FUKU95: Fukuyama F. - *Trust: The Social Virtues and the Creation of Prosperity*, 1995

GOLD09: Golbeck, J. (Ed.) - *Computing with Social Trust*, 2009 338 Springer

HALE05: Hales D., Arteconi S. - *Friends for Free: Self-Organizing Artificial Social Networks for Trust and Cooperation*, 2005

ZHOU08: Chunying Zhou, Huajun Chen, Tong Yu - *Social network mashup: Ontology-based social network integration for statistic learning*, 2008

JORD03: Jordan K., Hauser J., Foster S. - *The Augmented Social Network: Building Identity and Trust into the Next Generation Internet*, 2003 Networking A Sustainable Future conference

LIU05: Liu Hugo, Maes Pattie - *InterestMap: Harvesting Social Network Profiles for Recommendations*, 2005

MAYER95: Mayer R. C., Davis J. H., Schoorman F. D. - *An Integrative Model of Organizational Trust*, 1995 TheAcademy of Management Review 709-734

PAVL09: Pavlovic, D. - *Dynamics, Robustness and Fragility of Trust*, 2009 Formal Aspects in Security and Trust: 5th International Workshop 97-113 Springer-Verlag

ROLO81: Roloff M. E. - *Interpersonal communication: The social exchange approach.*, 1981

WALT09: Walter F. E., Battiston S., Schweitzer F. - *Personalised and Dynamic Trust in Social Networks*, 2009 Recommender Systems

WALT07: Walter F. E., Battiston S., Schweitzer F. - *A Model of a Trust-based Recommendation System on a Social Network*, 2007 Autonomous Agents and Multi-Agent Systems 16/1 57-74 Springer Netherlands

WENN06: Wennerberg P. O., Oellinger T. - *Ontology Based Modelling and Visualization of Social Networks for the Web*, 2006

ZHEN04: Zheng Y., Cofta P. - *A Mechanism for Trust Sustainability among Trusted Computing Platforms*, 2004 In Proceedings of the 1st International Conference on Trust and Privacy in Digital Business (TrustBus2004) 11-19 Springer Science + Business Media

ZHEN07: Zheng Y., Holtmanns S. - *Trust Modeling and Management: from Social Trust to Digital Trust*, 2007 book chapter of Computer Security, Privacy and Politics: Current Issues, Challenges and Solutions IGI Global