Toward an Integrative Model of Trust for Digital Emergency Communication

Pouyan Fotouhi Tehrani*
Weizenbaum Institute
Fraunhofer FOKUS

Niklas von Kalckreuth
Weizenbaum Institute
Humboldt University Berlin

Selma Lamprecht
Weizenbaum Institute
Fraunhofer FOKUS

ABSTRACT

Digital technologies have become an integral enabler of communication during various phases of emergency management (EM). A crucial prerequisite of effective communication between authorities and the public during EM is the establishment of adequate mutual trust. Trust, however, is an elusive concept which is not easily translatable into technical settings. In this paper we propose an integrative model of trust in digital communication and show how such model can be advantageous in assessing and improving trust relations in context of EM. Our interdisciplinary model, which is based on findings from psychology, sociology and computer sciences provides an abstraction which not only seizes both subjective and objective as well as personal and non-personal, *e.g.,* institutional or cultural, aspects of trust but at the same time is concrete enough to be applicable to real-life scenarios.

Keywords

Trust, Emergency Management, Digital Communication, Modeling.

INTRODUCTION

The Munich rampage of 2016, leaving nine people dead and many injured, is a prominent example of how vulnerable our emergency communication infrastructure truly is: while the high amount of data traffic at that time rendered communication over the Internet practically impossible, online social media platforms, such as Twitter, were being flooded with false information regarding the nature of attacks and possible targets (Backes et al., 2016). Even for those at site, who were able to communicate through overloaded channels, it remained a nontrivial task to decide whom or what to trust.

The penetration of digital communication in nearly every aspect of our private and public life raises the question of how to integrate or realize trust over technical infrastructure. At the same time, the multi-faceted nature of trust poses a real challenge to its translation in its broader sense into technical context. Whatever factors may be influential in building trust, mediated communication, *e.g.,* digital communication, almost always leads to loss or at least inhibition of cues or signals that are crucial to the construction of trust relations (Riegelsberger, 2005). The interleaving of digital and real world aspects in emergence or suppression of trust in the context of digital communication highlights the necessity of an interdisciplinary study of the subject matter.

By combining different understandings of trust from psychology, sociology, and computer sciences, we propose an integrative model which can lead to a better understanding of trust in digital communication, specifically in context of emergency communication. We understand trust as both cause and effect which emerges within a given *context* and is based on presence of some *evidence*. Our main goal is to provide a concrete basis upon which emergency management practitioners can better comprehend their relationship with their audience, and to equip them with a framework that, in contrast to existing approaches, proves to be practical beyond experimental or research settings.

The rest of this paper is structured as follows: in **§2** an overview of trust among various disciplines are provided. Our integrative trust model is introduced in **§3**, and **§4** discusses how this model can be utilized for emergency communication. Finally, in **§5** we conclude our work and draw a brief outlook for future work.

*corresponding author

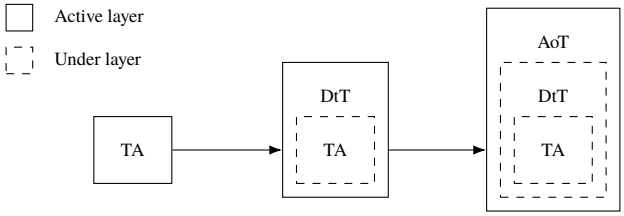

Figure 1. Trust stages and layers: Trust Attitude (TA), Decision to Trust (DtT), and Acting of Trusting (AoT)

TRUST AMONG VARIOUS DISCIPLINES

Trust is an elusive concept which has been subject of study in various disciplines (see Cho et al., 2015; Meyerowitz, 2013). In the following we give a brief overview of how trust is conceptualized in fields of psychology, sociology, and computer science.

Psychology

In psychology the most common and favored definition considers trust as "a psychological state of a trustor comprising the intention to accept vulnerability in a situation involving risk, based on positive expectations on the intentions or behavior of the trustee" (Rousseau et al., 1998). The emphasis here lies on the assumption that trust is a psychological condition which causes a certain behavior or choice and presupposes a) expectation of beneficial outcome and b) existence of risks and uncertainty (Schultz, 2006). This definition can be formalized as "X trusts Y in context C for performing task τ (with the action α and the result P), where τ corresponds to goal g of X" denoted as g_X (Castelfranchi and Falcone, 2010):

$$\textbf{Trust}(X, Y, C, \tau, g_X)$$

In this model the establishment of trust shows some parallels with cognitive skill acquisition processes, particularly by uniting dispositional and experiential determinants. The model postulates that the trust level of an individual in a certain situation emerges from situational context, experience of that individual, cognition state (attention, memory, decision-making processes, etc.), and social contact behavior, in which the context has the major influence (L. Tamilina and N. Tamilina, 2018). Castelfranchi and Falcone (2010) further elaborate this concept of trust using a three-layered model (Figure 1), which postulates that trust is a process of three steps:

- **Trust Attitude (TA)**: the mental attitude, *i.e.,* disposition, towards an entity.
- **Decision to Trust (DtT)**: the decision to rely on another entity, which makes the trustor 'vulnerable'.
- **Act of Trusting (AoT)**: the behavior, *i.e.,* the act of trusting.

Besides trust, *trustworthiness* is being defined is an important part of the process of trust establishment, but is not equal to trust itself. While trust is a psychological state, which involves two entities (the trustor and the trustee, which can be individuals, groups or institutions), trustworthiness is just a characteristic of the trustee which is signaled to and interpret by the trustor (Schultz, 2006). This signal has the meaning that the trustee is worthy of being trusted (Solomon and Flores, 2003). In interpersonal trust there are three characteristics, which influence the perceived trustworthiness of an individual: ability, benevolence and integrity (Schultz, 2006). In a digital context, such characteristics are rather generic terms to describe the antecedents of the perceived trustworthiness, for example, there is evidence that in context of an online environment the structural design (usability), the content design (information quality), the social-cue design (indicators of social presence), and the reputation of the system influence the perceived trustworthiness (Frik and Mittone, 2016; Wang and Emurian, 2005; Yan et al., 2011). Usability plays an important role in this. So, participants are more dedicated to use applications, which are easy to use, well-suited to their purposes and well-designed. By aesthetics and a useful design, users can be convinced, that a lot of time and effort had been invested into producing the application. These investments are perceived as serious and trustworthy approach by the user (Haasteren et al., 2019).

Sociology

Sociological studies in the past decades have dealt with the concept of trust under a variety of terms such as *solidarity* (Durkheim, 2014), *social ties* (Simmel, 1950) or *reciprocity* (Gouldner, 1960). In contrast to psychology there is, however, no consensus to define and understand trust as an individual state of mind. In this context social trust often puts the emphasis on relational and situational aspects (Vallentin and Thygesen, 2017; Welch et al., 2005).

Luhmann recognizes trust as a mechanism of reducing complexity which keeps us capable to (inter)act even in situations of uncertainty (Luhmann, 1979). Only with uncertainty – as the end of rational predicition (Luhmann, 1979; Gambetta, 1988) – a window of opportunity opens and one can act in faith (Bradach and Eccles, 1989; Lewis and Weigert, 1985; Möllering, 2005; Simmel, 1950). Going one step further, Luhmann distinguishes between confidence and trust concluding that a situation of trust is based on the awareness of possible disappointment and the decision to trust anyway (Luhmann, 2014). Luhmann's definition of trust resonates some aspects widely agreed by others, namely the willingness to become vulnerable while having positive expectations (Bijlsma-Frankema and Costa, 2005; Rousseau et al., 1998).

An important notion that sociologists add is that quantification as well as a finite list of factors of trust stand contradictory to the idea of trust itself. Trust is not rational (Hartmann, 2011), rather it goes beyond mere economic rationality (Abdelhamid, 2018; Eikeland and Saevi, 2017; Zey, 1997), which is constrained to calculation and prediction of trust.

Computer Science

In computer sciences, trust and trustworthiness are often used interchangeably and generally formulated as a quantifiable value on a continuous or discrete scale based on some evidence either provided actively or collected passively. A piece of evidence asserts a claim either about an entity, *e.g.,* trustee, or an action or more specifically the correctness of an action. The most prominent examples are the public-key infrastructure (PKI) (see Tilborg and Jajodia, 2011), Web-of-trust (WOT) (Zimmermann, 1995), blockchains, and reputation systems (see Braga et al., 2018).

In PKI and WOT the notion of trust is based on binding identities to cryptographic keys through *digital certificates*. A digital certificate is provided by an entity as a proof of identity (see Boeyen et al., 2008). Such certificate is comparable to an identity document in the real world, such as a passport. The idea is to prove that behind a digital representation lies a real-world entity; if a trustor is provided with adequate proof of identity, then it can decide either to trust or not to trust that entity based on its preexisting trust relation in the real world. In PKI, trust anchors, *i.e.,* entities which are already identified and marked as trusted by a trustor, vouch for correctness of such real/virtual binding by cryptographically signing the respective certificate just a national government would vouch for correctness of a passport. As a generalization of the PKI concept, WOT resembles a social network where every entity can vouch for the identity of another. To decide if an unknown entity can be trusted or not, one checks how many of its already trusted or semi-trusted peers can vouch for that unknown entity. In contrast to PKI, where trust is a binary attribute, WOT introduces *marginal trust*, in addition to *complete trust* and *untrusted*; an enhancement that does not necessarily simplify the assessment of trust relations.

Trust in the context of blockchain technologies is reduced to verifiability of implemented protocols (see *proof of work* in Bitcoin protocol in Nakamoto, 2019). In this sense trust(worthiness) is not defined in relation to any specific entity, rather in regard to an action or process. Here, immutable transactions are bundled into blocks which are then chained together, while it is computationally possible to verify each and every transaction from the very first to the last one and ensure that none has been tampered with. Under the assumption that no involved entity in the distributed ecosystem of blockchain is inherently trustworthy, as long as all transactions and processes are verifiable, the overall system is considered to be trustworthy, *i.e.,* acting in an expected manner.

Finally, reputation systems bring temporal aspects of trust into account by collecting information about or observing the behavior of an entity in a given period: to estimate the trustworthiness of an unknown entity, one can either observe the behavior of that entity through time, or rely on statements from other trusted entities. The observation can either be on a local scale, e.g., watching neighboring nodes in an ad hoc network, or on a global scale, e.g., ranking of sellers on an e-commerce website. Whereas in general only a single factor is observed, introducing multiple factors can improve the precision and reliability of calculated trustworthiness (see Trapp et al., 2012; *cf.,* Granovetter, 1973).

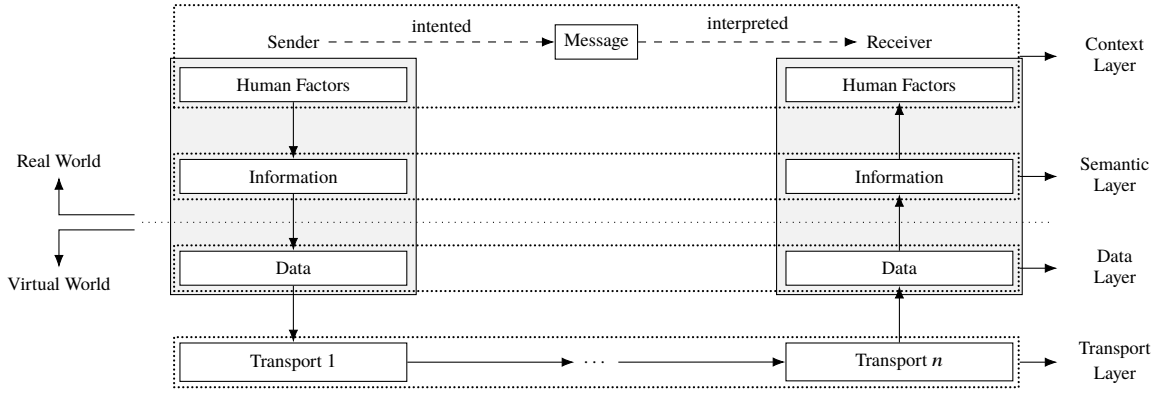

Figure 2. Digital Communication Model

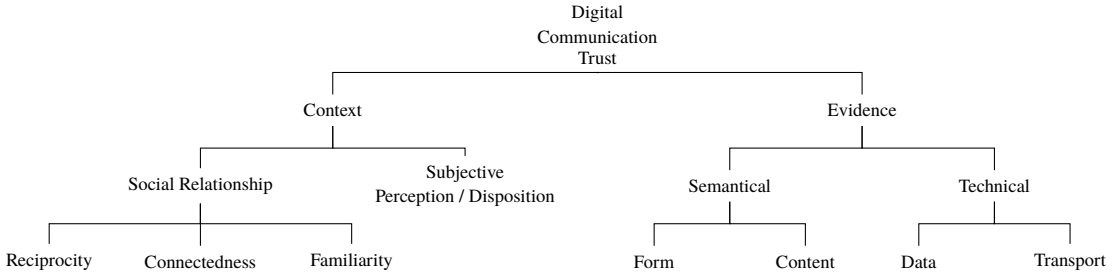

Figure 3. Taxonomy of Trust in Digital Communication

AN INTEGRATIVE TRUST MODEL

In contrast to vis-à-vis interaction, the biggest obstacle in establishing trust over digital communication is inhibition or at least distortion of signals necessary to evaluate a trust relation (cf., Riegelsberger, 2005). This effect is depicted in Figure 2 (*cf.,* Schultz, 2006): the sender formulates information which is then represented as data packets which subsequently are transmitted over a transport layer, reconstructed as data packets, interpreted as information and finally perceived by the receiver. The transition between each layer causes loss or transformation of signals that could be integral for evaluation of trust by the receiver, *i.e.,* the trustor. Additionally, there is a common context that influence the communication between the sender and the receiver. Adequately modelling trust, thus, entails adressing and understanding of processes occuring at each layer in both real and virtual spheres.

Based on the findings presented in the previous section, we consider trust to be a subjective experience which emerges in face of uncertainty under positive expectation regarding the qualities of an entity. In context of digital communication, trust relations are constrained and impacted by the digital medium, through which the interaction between trustor and trustee succeeds. In other words, the mediated communication between the entities is a decisive factor for establishment of trust[1]. Although there is no consensus as to which factors amount to experience of trust (see Braga et al., 2018 for an overview), we assume that the following holds: i) trust is context dependent, and ii) trust is evaluated based on available signals or cues which we henceforth refer to as *evidence*. Based on existing research and related works, we have developed a taxonomy (depicted in Figure 3) which summarizes our abstraction of trust relevant for digital communication. In the following we provide clarification for each point and give an overview of related works.

Context

Context comprises both subjective and objective aspects of trust. Despite existing efforts on formalizing trust using mathematical tools and notation[2], we tend to believe that such formalisms, *e.g.,* trust as a quantity between -1 and 1, fail to grasp and reflect the concept of trust in its totality, thus, limiting our scope to qualitative factors of trust.

Disposition to Trust

Trust is fundamental to building social bonds, thus, risks and uncertainties in social interaction appear more acceptable through trust (Erikson, 1993). These uncertainties are rooted in the fact that in the fewest decisions,

[1]see Riegelsberger (2005) for an exhaustive investigation and Bos et al. (2002) for concrete examples.
[2]See Marsh (1994) as one of the very first pioneering works in formalizing trust.

complete knowledge or complete information is available (Cho et al., 2015). Trust can be viewed from two different perspectives of the disposition and experience (Dinesen, 2012), which are not clearly distinguishable from one another. The former sees trust as a deeply rooted disposition, which is conveyed from generation to generation in the context of early childhood socialization and which can be seen as a cultural feature of a society (Dinesen, 2012; Dinesen and Bekkers, 2017; Stolle and Nishikawa, 2011). The latter, *i.e.,* the perspective of experience, sees trust as a result of formative experiences such as active participation in society by means of social interactions, upbringing and education, as well as an institutional context as a possible 'safety net' (Dinesen and Bekkers, 2017; L. Tamilina and N. Tamilina, 2018). These approaches are difficult to distinguish from one another, since early childhood socialization is also an experience. In fact, the relationship between disposition and experience is reciprocal, as formative childhood experiences and following education are of utmost importance for the disposition to trust.

Social Relationship

Multiple aspects and characteristics of social relationships are emphasized to influence trust: many studies distinguish between different levels of society (micro, meso, macro) and specialize on certain types with respect to this differentiation. For example, in organizational sociology much attention is given to trust between individuals, between individuals and organizations (Vanneste, 2016), and among organizations (Dodgson, 2016; Powell, 1996). Fewer but still a wealth of approaches are concerned with trust between state actors and organizations and/or individuals (Fukuyama, 1995; Putnam, 2000). Even though most studies focus on one layer and aspect, there is an agreement that these levels intervene with each other and can not be separated in practicee (Dietz, 2011) while certain variables influencing trust levels can be found on every layer. Due to the focus on digital communication we highlight three of these relational aspects for building trust, which are addressed as influential in psychological, sociological and computational research: reciprocity, familiarity and connectedness.

Reciprocity is understood as an aspect of the power structure between trustor and trustee that evolves around the issue of who is (able to) send and recive impulses: the trust received by an institution from individuals is not necessary reciprocated, for example, Tapia et al. (2011) studies how various NGOs initially leveraged Twitter to disseminate information but did not use it to collect back data as they did not perceive senders (presumably recipients of their messages) as trustworthy. Nevertheless, reciprocity is commonly seen as an important factor and basis of trust (Creed and Miles, 1996; Zucker, 1986; as organic solidarity, based on 'exchanging' even found by Durkheim, 2014).

Familiarity is understood as the historical and temporal dimension of trust which denotes the commonly expressed expectation that trust evolves over time. Concepts like *trust dynamics* try to grasp this general understanding and to bring it in line with observations and practical experiences (Faems et al., 2008; Fukuyama, 1995; Rousseau et al., 1998). This, however, fails to be an eligible case of compelling causality: familiarity is rather a variable for the trustor to calculate the risk of disappointment due to previous experiences with the trustee (Luhmann, 1988; Meyer and Ward, 2009). This understanding includes the difficulties to rebuild broken trust (Slovic, 1999).

Connectedness captures the relationship of entities within their social networks. The premise of connectedness is the fact that just like any kind of other of information being exchanged within ones social network, information about trust relations, *i.e.,* trustworthiness, credibility or reputation (*cf.,* Mui et al., 2002), are also passed on from one entity to another and can be integral to building own trust relations.

Evidence

Evidence is the signal or cue that amounts to establishment of trust relations. Here, we investigate two type of evidence that can be transmitted over digital infrastructure: semantical and technical.

Semantical

Content and form are qualitative types of evidence that can influence the trustworthiness perception of a message and its sender. Content, ranging from textual body to seals of approval and third-party certificates (Frik and Mittone, 2016; Wang and Emurian, 2005), has a major influence on the perceived trustworthiness of a technical system, *i.e.,* its reliability and correctness of provided information (Corritore et al., 2003; Lee and Chung, 2009; Yan et al., 2011). Whereas precise and well-formulated content can enforce trustworthiness, other factors, such as advertisement on a website or impolite and non-constructive messages have a negative influence on the perceived trustworthiness (Corritore et al., 2003; Haasteren et al., 2019).

Graphical attributes also have influence on the perceived trustworthiness of a technical system. For example, Miran et al. (2017) studies the effect of color usage in combination with background maps "on users' perception, interpretation, and reaction to threat information" in context of probabilistic hazard information. Similarly, the

effect of form on trustworthiness has also been studied on the world wide web: while the impact of the choice of colors to achieve a high trustworthiness (postulated by Wang and Emurian, 2005) is negligible (Frik and Mittone, 2016), the general aesthetics of the website have a big influence on the perceived trustworthiness. Professionalism and usability of a website are associated with the perceived aesthetics (Fogg et al., 2001; Bansal et al., 2015).

Technical

Under technical evidence, we subsume information security measures, such as confidentiality, integrity, authentication and alike (cf., CIA triangle in Whitman and Mattord, 2009). Such measures can either be applied directly on data or on transport layer, for example, data can be encrypted and transmitted over insecure transport channels or the channel itself can be secured and plain data is transmitted securely. The decision whether to secure data, transport layer or both depends on the given situation. Protocols, such as SSL/TLS, which depend on an end-to-end connectivity between communication partners, are not applicable where networks are fragmented and data is transmitted using data mules. On the other hand, if the communication succeeds over multiple transport protocols, or over insecure channels, protocols such as OSCORE (Selander et al., 2019), can be leveraged to secure data directly regardless of the transport layer capabilities.

Technical evidence can either be self-sufficient or third-party-dependent. Measures to secure data integrity, such as checksums, for example, are self-sufficient as the trustor can verify that the data has not been tampered without reliance on any external party. Other measures, such as X.509 certificates (Boeyen et al., 2008) which bind names to cryptographic keys and are used for authentication, depend on trusted third parties (TTP) to vouch for the binding by signing a digital certificate. Integral aspect in verification of evidence of the latter type is a bootstrapping phase to mark which TTP is trustworthy.

SHAPING TRUST IN EMERGENCY COMMUNICATION

Emergency management is an enterprise encompassing policies, activities, and measures with the aim of preparing for, mitigating, responding to and recovering from emergency situations (cf. Blanchard, 2008). In every phase of EM, communication (between and among) authorities and the public, plays an integral role (Reynolds and Seeger, 2005), not just as a functional necessity, but as "the most important and least understood role for policy makers" amounting to reinforcement of social resilience (Longstaff and Yang, 2008).

Effective communication relies on presence of trust among communication partners, however, depending on involved actors and each phase of EM, factors introduced in the previous section (see Figure 3) may have a stronger or lighter impact on trust relations: for example, whereas trust in technology in virtual emergency response teams may have a higher priority (*cf.,* Büscher et al., 2009), trusting crowdsourced data over social media may rely heavily on semantic evidence and connectedness of actors within the network (*cf.,* Mehta et al., 2017). Specially during response and recovery phases, dynamics of trust relations are changed: whereas on the one hand the time pressure to act and react does not leave enough development room for temporal aspects of trust building, network infrastructure may also be fragmented, isolated or overloaded so that technical trust mechanisms are not applicable anymore. In short, during response and recovery "sharing and dissemination of information is both critical and problematic, beginning with whom to trust in unfamiliar settings." (Manoj and Baker, 2007).

According to our proposed model, both context and evidence are integral in maintaining trust relations. There is, however, a reciprocal excretion of influence between these factors: one can imagine how context is decisive for choosing proper evidence and how evidence shapes the context in a persisting cycle of trust formation. For the sake of simplicity, we limit ourselves here to response and recovery phases where the context is given and cannot easily be changed but the evidence needs to selected accordingly. To show how our proposed model can be advantageous for strengthening trust in emergency communication, we appeal to example of *emergency alerting applications* such as FEMA's app[3] in the U.S. or KATWARN[4] (Meissen et al., 2018) in Germany. The point of departure is the systematic analysis of the context between trustees, *i.e.,* alerting authorities, and possible trustors, *i.e.,* citizens receiving alerts: in this case the relationship is not reciprocal so that the communication succeeds from alerting authority to citizens; the recipients might be in a vulnerable emotional and psychological state, and may have not yet familiarized themselves with responsible authorities. Considering the communication context and the constraints of given situation, an alerting authority can then choose proper evidence modalities to enforce the establishment of a trust relation: the better the understanding of authorities regarding the context, the more appropriate evidence can be chosen. Proper language, form, and content needs to be chosen to invoke the maximum perception of trustworthiness in recipients. Finally, the decision on technical evidence is highly dependent on

[3] https://www.fema.gov/mobile-app
[4] https://katwarn.de/

the state of communication infrastructure: authorities should be aware that in case of disaster or catastrophes communication networks may be fragmented, ad hoc networks emerge as alternatives, data is relayed from producers to consumers over (possibly malicious) third party nodes, *e.g.,* data mules, and that common security measures are not applicable anymore. Since no assumptions can be made about the available transport layer, technical evidence should be limited to the data itself: on the one hand the data must be *self-certifying*, *i.e.,* provide evidence that it hasn't been tampered with, and on the other hand it should be *self-authenticating*, *i.e.,* carry a digital signature to authenticate its origin. It should be noted that self-authentication presupposes a *trust bootstrapping phase* in which the certificate of origin is retrieved and marked as trusted by the trustee, *i.e.,* alert recipient.

CONCLUSION AND OUTLOOK

Trust remains an attractive subject of study among various disciplines. In this paper we balance abstract notions of trust and practicability by introducing an integrative model of trust, which comprises both quantitative and qualitative aspects of trust in digital communication. Our model serves organizations and individuals involved in emergency communication as a point of departure to asses their policies, procedures, and technical infrastructure with the aim of improving trust with their audience.

Although in our use case scenario, the focus lies on response and recovery phases and trust is understood as effect of available evidence, in future work we will investigate trust not just as cause but also as a cause which can be attended to during preparedness and mitigation phases. In other words, trust will be integrated into the perpetual cycle of emergency management; partly as a cause and partly as effect.

REFERENCES

Abdelhamid, M. I. (2018). *Die Ökonomisierung des Vertrauens: Eine Kritik gegenwärtiger Vertrauensbegriffe [The Economization of Trust: A Critique of Current Concepts of Trust]*. Bielefeld: transcript.

Backes, T., Jaschensky, W., Langhans, K., Munzinger, H., Witzenberger, B., and Wormer, V. (Oct. 1, 2016). *Timeline der Panik*. URL: https://sz.de/panik.

Bansal, G., Zahedi, F. M., and Gefen, D. (Nov. 2015). "The role of privacy assurance mechanisms in building trust and the moderating role of privacy concern". In: *European Journal of Information Systems* 24.6, pp. 624–644.

Bijlsma-Frankema, K. and Costa, A. C. (2005). "Understanding the Trust-Control Nexus". In: *International Sociology* 20.3, pp. 259–282.

Blanchard, B. W. (Oct. 2008). *Guide to Emergency Management and related Terms, Definitions, Concepts, Acronyms, Organizations, Programs, Guidance, Executive Orders & Legislation*.

Boeyen, S., Santesson, S., Polk, T., Housley, R., Farrell, S., and Cooper, D. (May 2008). *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. RFC 5280.

Bos, N., Olson, J., Gergle, D., Olson, G., and Wright, Z. (2002). "Effects of four computer-mediated communications channels on trust development". In: *Proceedings of the SIGCHI conference on Human factors in computing systems Changing our world, changing ourselves - CHI '02*. 4. New York, New York, USA: ACM Press, p. 135.

Bradach, J. L. and Eccles, R. G. (1989). "Price, Authority, and Trust: From Ideal Types to Plural Forms". In: *Annual Review of Sociology* 15.1, pp. 97–118.

Braga, D. D. S., Niemann, M., Hellingrath, B., and Neto, F. B. D. L. (Nov. 2018). "Survey on Computational Trust and Reputation Models". In: *ACM Computing Surveys* 51.5, pp. 1–40.

Büscher, M., Holst Mogensen, P., and Kristensen, M. (Apr. 2009). "When and How (Not) to Trust It? Supporting Virtual Emergency Teamwork". In: *International Journal of Information Systems for Crisis Response and Management* 1.2, pp. 1–15.

Castelfranchi, C. and Falcone, R. (2010). *Trust Theory: A Socio-Cognitive and Computational Model*. Wiley Series in Agent Technology. Chichester: Wiley.

Cho, J.-H., Chan, K., and Adali, S. (Oct. 2015). "A Survey on Trust Modeling". In: *ACM Computing Surveys* 48.2, pp. 1–40.

Corritore, C. L., Kracher, B., and Wiedenbeck, S. (June 2003). "On-line trust: concepts, evolving themes, a model". In: *International Journal of Human-Computer Studies* 58.6, pp. 737–758.

Creed, W. E. D. and Miles, R. E. (1996). "Trust in Organizations: A Conceptual Framework Linking Organizational Forms, Managerial Philosophies, and the Opportunity Costs of Controls". In: *Trust in Organizations: Frontiers of Theory and Research*. Thousand Oaks, CA, US: Sage Publications, Inc, pp. 16–38.

Dietz, G. (2011). "Going Back to the Source: Why Do People Trust Each Other?" In: *Journal of Trust Research* 1.2, pp. 215–222.

Dinesen, P. T. (May 2012). "Does Generalized (Dis)Trust Travel? Examining the Impact of Cultural Heritage and Destination-Country Environment on Trust of Immigrants". In: *Political Psychology* 33.4, pp. 495–511.

Dinesen, P. T. and Bekkers, R. (July 2017). "The Foundations of Individuals' Generalized Social Trust". In: *Trust in Social Dilemmas*. Ed. by P. A. V. Lange, B. Rockenbach, and T. Yamagishi. Oxford University Press.

Dodgson, M. (2016). "Learning, Trust, and Technological Collaboration:" in: *Human Relations* 46.1, pp. 77–95.

Durkheim, E. (2014). *The Division of Labor in Society*. New York, London, Toronto, Sydney, New Delhi: Free Press.

Eikeland, T. B. and Saevi, T. (2017). "Beyond Rational Order: Shifting the Meaning of Trust in Organizational Research". In: *Human Studies* 40.4, pp. 603–636.

Erikson, E. (1993). *Childhood and Society*. New York: W. W. Norton.

Faems, D., Janssens, M., Madhok, A., and Looy, B. V. (2008). "Toward an Integrative Perspective on Alliance Governance: Connecting Contract Design, Trust Dynamics, and Contract Application". In: *The Academy of Management Journal* 51.6, pp. 1053–1078.

Fogg, B. J., Swani, P., Treinen, M., Marshall, J., Laraki, O., Osipovich, A., Varma, C., Fang, N., Paul, J., Rangnekar, A., et al. (2001). "What makes Web sites credible?" In: *Proceedings of the SIGCHI conference on Human factors in computing systems - CHI '01*. ACM Press.

Frik, A. and Mittone, L. (2016). *Factors Influencing the Perceived Websites' Privacy Trustworthiness and Users' Purchase Intentions*. CEEL Working Papers 1609. Cognitive and Experimental Economics Laboratory, Department of Economics, University of Trento, Italia.

Fukuyama, F. (1995). *Trust: The Social Virtues and the Creation of Prosperity*. New York: Free press.

Gambetta, D. (1988). "Can We Trust Trust?" In: *Trust: Making and Breaking Cooperative Relations*. Cambridge: B. Blackwell, pp. 213–239.

Gouldner, A. W. (1960). "The Norm of Reciprocity: A Preliminary Statement". In: *American Sociological Review* 25.2.

Granovetter, M. S. (May 1973). "The Strength of Weak Ties". In: *American Journal of Sociology* 78.6, pp. 1360–1380.

Haasteren, A. van, Gille, F., Fadda, M., and Vayena, E. (Jan. 2019). "Development of the mHealth App Trustworthiness checklist". In: *DIGITAL HEALTH* 5, pp. 1–21.

Hartmann, M. (2011). *Die Praxis des Vertrauens [The practice of Trust]*. Deutsch. Berlin: Suhrkamp Verlag.

Lee, K. C. and Chung, N. (Dec. 2009). "Understanding factors affecting trust in and satisfaction with mobile banking in Korea: A modified DeLone and McLean's model perspective". In: *Interacting with Computers* 21.5-6, pp. 385–392.

Lewis, J. D. and Weigert, A. (1985). "Trust as a Social Reality". In: *Social Forces* 63.4, pp. 967–985.

Longstaff, P. H. and Yang, S.-U. (2008). "Communication Management and Trust: Their Role in Building Resilience to "Surprises" Such As Natural Disasters, Pandemic Flu, and Terrorism". In: *Ecology and Society* 13.1, pp. 1–14.

Luhmann, N. (1979). *Trust and Power*. Chichester: Wiley.

Luhmann, N. (1988). "Familiarity, Confidence, Trust: Problems and Alternatives." In: *Trust: Making and Breaking Cooperative Relations*. Ed. by D. Gambetta. B. Blackwell, pp. 94–107.

Luhmann, N. (2014). *Vertrauen*. Konstanz: UTB.

Manoj, B. and Baker, A. H. (Mar. 2007). "Communication challenges in emergency response". In: *Communications of the ACM* 50.3, p. 51.

Marsh, S. P. (Apr. 1994). "Formalising Trust as a Computational Concept". PhD thesis.

Mehta, A. M., Bruns, A., and Newton, J. (July 2017). "Trust, but verify: social media models for disaster management". In: *Disasters* 41.3, pp. 549–565.

Meissen, U., Pfennigschmidt, S., Hardt, M., and Faust, D. (2018). "KATWARN – A Microservice-Based Architecture for Distributed, Flexible and Robust Warning Systems". In: *Progress in IS*. Springer International Publishing, pp. 213–225.

Meyer, S. and Ward, P. R. (2009). "Reworking the Sociology of Trust: Making a Semantic Distinction between Trust and Dependence". In: *Proceedings of the Australian Sociological Association Conference*. The Future of Sociology. TASA Annual Conference. Australian National University, Canberra: The Australian Sociological Association, pp. 1–16.

Meyerowitz, S. A. (Nov. 2013). "Trust Management". In: *Intrusion Detection Networks*. Vol. 125. 5. Auerbach Publications, pp. 51–72.

Miran, S. M., Ling, C., James, J. J., Gerard, A., and Rothfusz, L. (Nov. 2017). "User perception and interpretation of tornado probabilistic hazard information: Comparison of four graphical designs". In: *Applied Ergonomics* 65, pp. 277–285.

Möllering, G. (2005). "The Trust/Control Duality: An Integrative Perspective on Positive Expectations of Others". In: *International Sociology* 20.3, pp. 283–305.

Mui, L., Mohtashemi, M., and Halberstadt, A. (Jan. 2002). "A computational model of trust and reputation". In: *Proceedings of the 35th Annual Hawaii International Conference on System Sciences*, pp. 2431–2439.

Nakamoto, S. (2019). *Bitcoin: A peer-to-peer electronic cash system*. Tech. rep. Bitcoin.

Powell, W. W. (1996). "Trust-Based Forms of Governance". In: *Trust in Organizations: Frontiers of Theory and Research*. Thousand Oaks: SAGE Publications, Inc., pp. 51–67.

Putnam, R. D. (2000). "Bowling Alone: America's Declining Social Capital". In: *Culture and Politics: A Reader*. Ed. by L. Crothers and C. Lockhart. New York: Palgrave Macmillan US, pp. 223–234.

Reynolds, B. and Seeger, M. W. (2005). "Crisis and emergency risk communication as an integrative model". In: *Journal of Health Communication* 10.1, pp. 43–55.

Riegelsberger, J. (June 2005). "Trust in Mediated Interactions". PhD thesis. University of London.

Rousseau, D. M., Sitkin, S. B., Burt, R. S., and Camerer, C. (July 1998). "Not So Different After All: A Cross-Discipline View Of Trust". In: *Academy of Management Review* 23.3, pp. 393–404.

Schultz, C. D. (2006). "A trust framework model for situational contexts". In: *Proceedings of the 2006 International Conference on Privacy, Security and Trust Bridge the Gap Between PST Technologies and Business Services - PST '06*. c. New York, New York, USA: ACM Press, p. 1.

Selander, G., Mattsson, J., Palombini, F., and Seitz, L. (July 2019). *Object Security for Constrained RESTful Environments (OSCORE)*. RFC 8613.

Simmel, G. (1950). *The Sociology of Georg Simmel*. Glencoe: Free Press.

Slovic, P. (1999). "Trust, Emotion, Sex, Politics, and Science: Surveying the Risk-Assessment Battlefield". In: *Risk Analysis* 19.4, pp. 689–701.

Solomon, R. and Flores, F. (2003). *Building Trust: In Business, Politics, Relationships, and Life*. Oxford: Oxford University Press.

Stolle, D. and Nishikawa, L. (2011). "Trusting Others - How Parents Shape the Generalized Trust of Their Children". In: *Comparative Sociology* 10.2, pp. 281–314.

Tamilina, L. and Tamilina, N. (Feb. 2018). "Trust as a Skill". In: *Psychology and Developing Societies* 30.1, pp. 44–80.

Tapia, A. H., Bajpai, K., Jansen, J., Yen, J., and Giles, L. (2011). "Seeking the Trustworthy Tweet: Can Microblogged Data Fit the Information Needs of Disaster Response and Humanitarian Relief Organizations". In:

Tilborg, H. van and Jajodia, S. (2011). *Encyclopedia of Cryptography and Security*. Encyclopedia of Cryptography and Security. Springer US.

Trapp, S., Wählisch, M., and Schiller, J. (May 2012). "Bridge the Gap: Measuring and Analyzing Technical Data for Social Trust between Smartphones". In: eprint: 1205.3068.

Vallentin, S. and Thygesen, N. (2017). "Trust and Control in Public Sector Reform: Complementarity and Beyond". In: *Journal of Trust Research* 7.2, pp. 150–169.

Vanneste, B. S. (2016). "From Interpersonal to Interorganisational Trust: The Role of Indirect Reciprocity". In: *Journal of Trust Research* 6.1, pp. 7–36.

Wang, Y. D. and Emurian, H. H. (Jan. 2005). "An overview of online trust: Concepts, elements, and implications". In: *Computers in Human Behavior* 21.1, pp. 105–125.

Welch, M. R., Rivera, R. E. N., Conway, B. P., Yonkoski, J., Lupton, P. M., and Giancola, R. (2005). "Determinants and Consequences of Social Trust*". In: *Sociological Inquiry* 75.4, pp. 453–473.

Whitman, M. and Mattord, H. (2009). *Principles of Information Security*. Boston: Course Technology.

Yan, Z., Kantola, R., and Zhang, P. (Nov. 2011). "A Research Model for Human-Computer Trust Interaction". In: *2011IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications*. IEEE.

Zey, M. (1997). *Rational Choice Theory and Organizational Theory: A Critique*. London: SAGE Publications.

Zimmermann, P. R. (1995). *The Official PGP User's Guide*. Cambridge, MA, USA: MIT Press.

Zucker, L. G. (1986). "Production of Trust : Institutional Sources of Economic Structure, 1840 - 1920". In: *Research in organizational behavior : an annual series of analytical essays and critical reviews*. Research in Organizational Behavior : An Annual Series of Analytical Essays and Critical Reviews. 8, pp. 53–111.