SpringerBriefs in Electrical and Computer Engineering

More information about this series at http://www.springer.com/series/10059

Michael G. Harvey

Wireless Next Generation Networks

A Virtue-Based Trust Model

Springer

Michael G. Harvey
Whiting School of Engineering
Johns Hopkins University
Pittsburgh, PA
USA

ISSN 2191-8112 ISSN 2191-8120 (electronic)
ISBN 978-3-319-11902-1 ISBN 978-3-319-11903-8 (eBook)
DOI 10.1007/978-3-319-11903-8

Library of Congress Control Number: 2014951722

Springer Cham Heidelberg New York Dordrecht London

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

For Missy and Kaija

Preface

The mobile Internet involves the ongoing convergence of fixed and mobile networks with other types of wireless next generation networks within an open and dynamic environment, where the lack of a central mediator forces entities to interact through collaboration and negotiation. Current computational approaches to trust, based on the iterative exchange of personal knowledge such as digital credentials and access control policies, are not feasible for wireless next generation networks due to the limited power, bandwidth, and computational capabilities of mobile devices. The lack of pre-authentication knowledge makes it difficult to establish initial trust between strangers. Use cases from secure routing and secure key management are used to illustrate the limitations of current computational trust models, and to motivate the need for a new trust model that reflects human social interaction and does not depend on personal knowledge of user identities.

A virtue-based trust model is proposed as an efficient and flexible version of trust without identity based on the actions of an entity rather than on personal knowledge of the actor. The trust model is influenced by recent contributions from virtue epistemology and the intuition that the actions of an entity should be more efficient to evaluate than the belief state of one entity regarding the intentions or future actions of another entity. From a theoretical point of view, a virtue-based trust model allows us to relate trust and rationality in a non-circular fashion by showing how trust and reason are complementary cognitive mechanisms that guide our rational conduct at an animal or instinctual level and at a reflective level respectively. From a practical point of view, in addition to protecting confidentiality, a virtue-based trust model can help ensure availability if used to support local information sharing schemes. Furthermore, given its emphasis on virtue and character as universal traits of trustworthiness and its moderating notion of achieving balance or harmony in the trust relation, a virtue-based trust model can be adapted to the intercultural context of the mobile Internet.

The trust model integrates the behavioral and cognitive dimensions of trust in a nomological framework which includes both objective and subjective decision structures. These decision structures correspond to a distinction between animal knowledge and reflective knowledge respectively. Initial trust in other entities is

established at the level of animal knowledge through innate competences called basic trust dispositions that are rational but not reason-based. Basic trust involves two pre-reflective and mutually dependent trust dispositions, self-trust and trust in other people. The trust relation involves the mutual adjustment, moderation, and self-control of one entity's basic trust dispositions or reactions in response to another entity's actions with the goal of achieving balance or harmony in the trust relation, whereby each entity accepts more or less the same degree of risk or vulnerability. For most interactions, the trust relation can be evaluated according to an objective decision structure using simple rules based on adapting actions and adjusting actions. Whereas adapting actions increase the level of trust and facilitate cooperation and collaboration through mutual adjustment, adjusting actions increase the level of distrust and lead to selfishness and conflict through the domination of one side by the other side. At the level of animal knowledge, the trust model reflects how humans do what they do naturally.

When there is a violation of initial trust, the trust relation needs to develop from basic trust toward full-fledged trust at the level of reflective knowledge. As the awareness of risk or vulnerability in the trust relation increases, an entity needs to justify its initial trust in another entity by establishing the reliability of the source. If the level of trust falls below a minimum acceptable threshold, where selfish behavior may lead to conflict, the trust relation needs to be evaluated according to a subjective decision structure using more complex rules based on acts of intellectual virtue that manifest the reliability or trustworthiness of an entity. At the level of reflective knowledge, the trust model reflects how humans can do a better job of what they do naturally by exercising reason-based competences such as intellectual virtues which help them avoid being either too trusting of other entities or not trusting enough of them.

A virtue-based trust model should be more efficient than identity-based, role-based, or attribute-based trust models that depend on computationally expensive methods. We need not evaluate the belief state of one entity regarding the intentions or future actions of another entity based on personal knowledge of the actor. Instead, we can evaluate the behavioral and cognitive performances of autonomous rational agents, whether human or artificial. An apt behavioral performance can be defined as an adapting action that enhances basic trust in other people and facilitates cooperation and collaboration. In contrast, an apt cognitive performance can be defined as an act of intellectual virtue that achieves balance or harmony in the trust relation by moderating the basic trust dispositions in the presence of the awareness of risk or vulnerability. Thus, we can evaluate the success of adapting actions in achieving balance or harmony in the trust relation so long as there is no violation of the trust relation. When a trust violation occurs, we can evaluate the success of acts of intellectual virtue manifested by one entity in moderating its own basic trust dispositions or reactions in response to the actions of another entity according to whether the acts achieve balance or harmony in the trust relation.

Whereas the present work aims to develop a theory of trust that reflects human social interaction, future work will need to define the methods of the theory and illustrate their application in different areas of network security such as secure

routing and secure key management. An ontology needs to be defined for organizing adapting actions and acts of intellectual virtue in a nomological framework. Simple rules need to be formulated for distinguishing adapting actions from adjusting actions in accordance with how successful they are in achieving the socially valuable ends of cooperation and collaboration, while avoiding the socially undesirable ends of selfishness and conflict. More complex rules need to be formulated for determining whether an entity has manifested a certain intellectual virtue or reason-based competence that is conducive to increasing the level of trust in a given interaction. Finally, potential defeaters of the methods need to be considered. In particular, acts of intellectual virtue may not be sufficient for distinguishing atypical interaction scenarios such as malicious hacking versus ethical hacking, since both actions involve the exercise of similar intellectual virtues and we have to take into account the intention of the action.

The interdisciplinary nature of a virtue-based trust model should appeal to at least two different groups of researchers. As the problem of developing more efficient and flexible trust models for wireless next generation networks has become more pressing in computer science, the nature of trust and its role in society have emerged as topics of widespread interest in philosophy and the social sciences. Thus, on one hand, computer scientists may benefit from the normative, sociological, and cultural analyses of trust provided by philosophers and social scientists in developing more efficient and flexible trust models that reflect the way humans interact in social environments. Philosophers and social scientists, on the other hand, may benefit from the empirical application of trust models in computer science in understanding the practical limitations of their own theories and models of trust. Consequently, a virtue-based trust model may best be seen as an example of experimental philosophy that aims to make a small theoretical contribution to computer science.

Pittsburgh, PA Michael G. Harvey

Acknowledgments

The author would like to thank Dr. Harold J. Podell, Assistant Director of IT Security in the Center for Science, Technology and Engineering at the Government Accountability Office, for directing his attention to key management issues in wireless next generation networks. These issues, among others, have motivated the need for a more efficient and flexible trust model. The author would also like to thank Dr. Ernest Sosa, Board of Governors Professor of Philosophy at Rutgers University, for introducing him to epistemology as a doctoral student at Brown University. With respect to both influences, however, the author bears full responsibility for the proposal of a virtue-based trust model, and for his interpretation of Sosa's virtue perspectivism which provides the theoretical anchor for the trust model.

Most importantly, the author would like to thank his spouse, Melissa J. Harvey, for her research assistance in verifying the references, obtaining copyright permissions for material used in the book, and for encouraging him to think outside the box and perhaps even against the grain.

The author would like to thank the publishers for copyright permissions to reproduce material from the following papers:

©2009 Elsevier. Fig. 1.1 is reprinted with permission from TalebiFard P et al. (2010) Access and service convergence over the mobile internet–A survey. Computer Networks 54(4):545–557.

©2012 CRC Press. Fig. 2.2 is reprinted with permission from Chen L, Gong G (2012) Wireless security: Security for mobility. In: Communication system security. CRC Press, New York.

©2008 ACM Press. Figs. 2.3–2.5 are reprinted with permission from Hoeper K et al. (2008) Security challenges in seamless mobility–How to 'handover' the keys? In: 4th international ACM wireless internet conference (WICON '08), Maui, HI, 17–19 November 2008, pp 2–3.

©2013 IEEE. Figs. 2.6–2.7 are reprinted with permission from Kishiyama Y et al. (2013) Future steps of LTE-A: Evolution toward integration of local area and wide area systems. IEEE Wireless Communications 20(1):12–18.

©2013 NTT DOCOMO, Inc. Figs. 2.8–2.9 are reprinted with permission from Zugenmaier A, Aono H (2013) Security technology for SAE/LTE (system architecture evolution 2/LTE). NTT DOCOMO Technical Journal 11(3):28–30, 2013.

©2011 Emerald Group Publishing. Fig. 6.6 is reprinted with modifications and permission from Du R et al. (2011) Integrating Taoist yin-yang thinking with western nomology: A moderating model of trust in conflict management. Chinese Management Studies 5(1):55–67.

Contents

Figures

Tables

About the Author

Michael G. Harvey holds an undergraduate degree magna cum laude in Physics and Astronomy from the University of Pittsburgh. He holds master's degrees from Yale University, Brown University, and Carnegie Mellon University, where he studied a variety of disciplines, including epistemology, theory of religion, cognitive psychology, and computer science. He is currently studying cybersecurity at Johns Hopkins University. His most recent publication on privacy and security issues for mobile health platforms, co-authored with his spouse Melissa J. Harvey of the National Network of Libraries of Medicine, Middle Atlantic Region, appeared as the lead article in the July 2014 issue of *Journal of the Association for Information Science and Technology (JASIST)*.