The Trustworthy and Trusted Web

Full text available at: http://dx.doi.org/10.1561/1800000016

The Trustworthy and Trusted Web

Piotr Cofta

piotr@cofta.net

the essence of knowledge

Boston – Delft

Foundations and Trends® in Web Science

Published, sold and distributed by:
now Publishers Inc.
PO Box 1024
Hanover, MA 02339
USA
Tel. +1-781-985-4510
www.nowpublishers.com
sales@nowpublishers.com

Outside North America:
now Publishers Inc.
PO Box 179
2600 AD Delft
The Netherlands
Tel. +31-6-51115274

The preferred citation for this publication is P. Cofta, The Trustworthy and Trusted Web, Foundation and Trends® in Web Science, vol 2, no 4, pp 243–381, 2010

ISBN: 978-1-60198-492-0

Foundations and Trends® in Web Science
Volume 2 Issue 4, 2010

Editorial Board

Editorial Scope

Foundations and Trends® in Web Science will publish survey and tutorial articles in the following topics:

- Agents and the Semantic Web
- Content Management
- Databases on the Web
- Data Mining
- Dependability
- Emergent behaviour
- Human-Computer Interaction
- Hypertext/hypermedia
- Languages on the Web
- Mobile/pervasive
- Multimedia
- Network infrastructures
- Performance
- Scalability
- Security
- Semantic Web — metadata, ontologies
- Standards
- Trust and Provenance (Policy)
- Universal Usability
- User Interfaces
- Web Searching/Information Retrieval
- Web Services

Information for Librarians
Foundations and Trends® in Web Science, 2010, Volume 2, 4 issues. ISSN paper version 1555-077X. ISSN online version 1555-0788. Also available as a combined paper and online subscription.

Full text available at: http://dx.doi.org/10.1561/1800000016

Preface

'Think about your readers' — this is the first and the fundamental rule for every author. While writing those pages, I thought of those who might be reading them. The community interested in trustworthiness is a small and a dispersed one. They are united in the desire to understand trustworthiness but they are segregated into silos of their disciplines. They cannot agree even on the common definition, not to mention practical methods to achieve trustworthiness. I guess that I have met, read or heard of the majority of them.

There is also a much larger community that is interested in using trust, not in building trustworthiness. Their starting point is simple: 'there is trust — so what we can do with it?'. Such trust may reflect the trustworthiness or not. It may be unwarranted or — conversely — not granted where it is due. This particular approach may easily lead to the creation of the theatre of trust, where pretences of trustworthiness are mistaken for the actual one.

This situation is not inspiring, because the problem of a trustworthy ICT, and specifically trustworthy Web affects each and every one of us, whether we commute, work, chat or even just stroll in the park. The problem is inherently pervasive, interdisciplinary and acute. We are dependent on the ICT as never before, and we are becoming even more dependent on it with every passing hour. We literally 'live the Web' — or at least some of us do. If we cannot trust the warm technical cocoon that surrounds us, how can we trust anything (or anybody) else? Should we then trust knowing that we cannot tell the trustworthy infrastructure and trustworthy information from an untrustworthy one?

While the language of the following pages may be sometimes complex, the message is very simple: we can do better. In fact, we must do better. We have to improve on trustworthiness of the most critical of the ICT structures: the Web, and the way forward starts with understanding the trustworthiness. Once we understand, we can modify the way we develop the Web to make it more trustworthy. Yes, we can actually develop ICT (and consequently the Web) that is 'trustworthy

by design' — but the development process may not look like anything that we are familiar with. It is a challenge, and it is unlikely to happen any time soon, but hopefully it will happen before we make fools of ourselves by trusting what may be not worthy of our trust.

Foundations and Trends® in
Web Science
Vol. 2, No. 4 (2010) 243–381

DOI: 10.1561/1800000016

now
the essence of knowledge

The Trustworthy and Trusted Web

Piotr Cofta

piotr@cofta.net

Abstract

Considering the recognised importance of a trustworthy Web and trustworthy ICT infrastructure, it is surprising that there is not a single agreed approach to how to actually develop them, or what are the desired properties of it. We are not even certain whether an inanimate infrastructure can be considered trustworthy at all. If the truly trustworthy Web is ever going to happen, this deficiency has to be addressed. This monograph analyses the concept of 'trustworthy ICT' from the dual perspective of its technical architecture and from the sociological perspective of a systemic creation of social reality. It aims to determine whether a single notion of trustworthiness can be agreed upon and whether the disparate collection of existing views can be consolidated into useful design criteria.

Against this systemic background, this monograph reveals the structure behind conflicts and misunderstandings of our modern perception of the trustworthiness of ICT. It defines seven views on trustworthiness and demonstrates that six of them can be used to structure not only research but also market practices. The monograph then postulates that the shared future of truly trustworthy Web (and any

other trustworthy ICT infrastructure) is in the seventh view, in the systemic trustworthiness, and indicates required design properties of such a construct. This reasoning is then applied to the Web, with a specific focus on Semantic Web.

Contents

1

Introduction

The existence of large information and communication technology (ICT) structures, and its impact on our everyday lives is generally accepted as an unquestionable fact of modern life. The proliferation of the Web (known also less precisely as 'the Internet') has increased the everyday awareness of the existence of such large structures, even though the Web is not the only example of a global, pervasive ICT mega-structure. Other, somehow more autonomous structures include military networks, telecommunication networks, financial infrastructure, or large governmental systems.

Technology, and specifically ICT technology is an important (and ever-changing) component of our everyday experience. Directly or indirectly it affects lives of many people, with the Internet being used by every fourth person on the planet (http://data.worldbank.org/indicator/IT.NET.USER), Facebook having almost half a billion users (http://www.facebook.com, Nov. 2010), in par with large mobile phone operators such as China Mobile (http://www.chinamobileltd.com) or Vodafone (www.vodafone.co.uk).

The introduction of ICT systems is believed to deliver 40% of overall productivity growth for the last 15 years [2] and made several businesses dependent on such systems. The installation, operation, upgrade and

maintenance of these systems is a huge worldwide business where leading companies report revenues of hundreds of billion USD a year.

The reasonable level of operation of those ICT mega-infrastructures is usually taken for granted, for as long as there are no major breaches. Institutions, societies and individuals equally rely on them in pursuing their daily lives and investigating strategic options. It is uncommon to consider whether the Web deserves such a level of reliance, or to explore what and to what extent can be relied upon. Possibly it is due to the fact that even the simplest component of a modern Web (or any other modern ICT system), when investigated in depth, reveals the inconceivably complex network of technical and social dependencies of trust and control (see "The Case of A Humble Padlock").

This monograph is motivated by the need to convert the currently incidental trustworthiness of the ICT and the Web into the planned one, so that the trustworthy ICT and the trustworthy Web will be designed for. Therefore the outcome of the analysis presented here is not the analysis itself, but rather the creation of a set of design guidelines that will allow ICT to be 'designed for trustworthiness'.

1.1 Trustworthy Systems

Recently, there has been a growing interest in trustworthy Web, trustworthy information systems, trustworthy ICT, and trustworthy technology in general. One may cynically say that this is due to the amount of money EU decided to spend on research projects with 'trustworthy' in their titles [64, 186] or on an image repair that some large software companies decided to undertake [134]. However, the reason may be found also in an anticipation that trustworthiness will improve a rather dismay ICT adoption rate [113], thus justifying billions that governments and businesses spent on such systems. There are also some who honestly expect that technology has a power to improve our society, and that trustworthy infrastructure will make us more trustworthy (e.g., http://paradiso-fp7.eu/).

Trust is often listed as a near-magical solution to all the ills of our society (duly replicated on the Web), from illegal copying to pornography to disreputable retailers and misleading propaganda [165].

The Case of A Humble Padlock

Let us consider the most humble everyday experience of the (in)famous padlock on the Web browser. You navigate through the Web, you get to a page where your credit card number is required. As a savvy person you look for the locked padlock sign. Yes, it is here. You now feel confident that you are dealing with a trustworthy web site.

Not really. What you really see is a technical message saying that the communication between your browser and a certain remote server is secured. As for the rest — you have to trust. You have to trust 'the Internet', the highly complicated structure of millions of DNS servers around the world. You must trust your computer that it has set up the communication securely. You must trust (unknowingly) several parties that have designed, delivered and set up your browser and your computer. You must trust those who provide and operate the so-called key distribution infrastructure for the Internet.

Still, this is only about the technical communication channel between you and the remote server. The padlock does not guarantee that the party at the other end of the channel is trustworthy. They could be a front for a criminal organisation, they could have set-up this web site yesterday and could disappear by tomorrow, or they would simply be lazy with their security processes, leaking your credit card number through their back doors.

The real meaning of the padlock is beyond the comprehension of any user. It requires a real expert to conduct the complete analysis of whom, why and when you trust — but this of course requires you to trust the expert without being able to verify him. Either way, you end up trusting without knowing.

Trust is generally accepted as one of enablers of the proliferation of the Web, increase in e-commerce or e-government, improvement to the Internet-based economy [69], security and safety. Trust and trustworthiness have been explicitly listed as one of the important components of the Semantic Web [46] effectively making or breaking this important development.

Whatever is the reason of the current interest in trustworthiness, it fails to address one main problem: the fact that there is no agreement

what 'trustworthy' should really mean, and consequently how it can be designed, deployed and operated. There is no agreement even on whether technology can be attributed with trustworthiness at all. Those problems require a thorough discussion, otherwise the noble vision of trustworthy Web will be fragmented at the best, or misleading at the worst. Without trustworthiness, the Web can easily degrade into a theatre of trust, full of pretences and deception.

1.2 Definitions

This monograph distinguishes between the Information and Communication Technology (ICT) infrastructure, the Internet and the Web. While causal definitions of those terms are usually intuitionally well understood, it may be important to clarify them here.

- ICT infrastructure is the large-scale deployment of the information and communication technology, together with its immediate social environment of processes and operations. Thus, e.g., the mobile network is an ICT infrastructure that encompasses radio towers, back-haul links, mobile phones as well as customer support, frequency allocation and fraud detection processes. Other ICT infrastructures may include, e.g., the travel booking system, or the corporate payroll system.
- The Internet is a particular implementation of the public global packet-switching data network, together with its social environment. It contains such elements like the technical structure (cables, routers, modems), protocols (TCP/IP, etc.), supporting services (e.g., DNS), governance (e.g., ICANN), etc. There may be other global networks that are not public yet sharing similar technology, but this monograph is only interested in the public one.
- The Web is the information overlay on top of the Internet, again together with its social environment. The traditional fault line is demarcated by the HTTP/HTML protocol, but the proliferation of solutions 'above' the Internet may make

this differentiation misleading. For all practical purposes, the Web is dealing with information (with certain meaning assigned to it) while the Internet is dealing with data (possibly structured, yet with no meaning assigned).

1.3 Semantic Web

Semantic Web [77] is an ambitious attempt to standardise and automate the top technology layer of the Web that deals with the semantics of its content, and more generally with sense-making. The approach of the Semantic Web is through the application of formal logic, on the basis of the variety of meta-tags associated with the content.

There are potentially significant benefits that the Semantic Web may bring. Specifically, the ability to automate formal reasoning should allow for the automation of the sense-making well beyond current capabilities. This will affect all aspects of the usage of the Web, from a casual search to health diagnostics to algorithmic trading. The automation will be particularly important if and when the Web will encompass the 'Internet of things' [32], i.e., millions and billions of network-enabled sensors scatted around the world.

While certain areas of the Semantic Web experienced rapid development over recent years, the whole premise is still far on the horizon. Specifically, the adoption of Semantic Web tools and methods is slow, as they require expensive, rigorous re-development for the majority of the Web content. Currently, methods that are 'good enough' such as PageRank [141], augmented by social heuristics seem to satisfy the needs of our limited bounded rationality [170].

As there is a disparity between current social practices and the ones prescribed by the Semantic Web, there is a fundamental question that has to be explored. It is whether there is one and only one way of reasoning about the meaning of information that the Semantic Web understands and that the society has to follow (or ignore), or should the Semantic Web mimic what the society is doing even though it may lead to less than perfect results?

The same question applies when considering trust within Semantic Web. Is there a model of trust that the Semantic Web has in mind,

believes that it is to be a true one, and wants the society to accept it? Or is it possible to express within the Semantic Web the richness of different, partly conflicting and intuitional heuristics that the society is actually using?

Those questions essentially reflect the disparity between technological determinism [73] and social constructivism [146], and are discussed later in the monograph. Neither question is for the author to answer, but they are worth a separate discussion that goes beyond this monograph. As for the reader, it is worth bearing this question in mind while reading this monograph.

1.4 Propositions

The author believes that trustworthiness and trustworthy Web or ICT can be unambiguously defined, but that such a definition is subject to interpretations by different stakeholders, thus leading to different views on essentially the same phenomenon.

The motivation for this monograph originates from the interest in ICT design, and Web design in particular. Therefore, the key question investigated here is about our ability to design a trustworthy ICT infrastructure. This, in turn, leads to a question about design properties that make it trustworthy (as contrasted with the pretension of trustworthiness), about the role of a design (e.g., versus operation), etc.

Therefore the following is proposed, and will be discussed throughout this monograph.

1. Trustworthiness is not applicable directly to technical artefacts (such as the Web or an ICT infrastructure), but it is applicable to socio-technical structures that contain technical artefacts (such as the organisation that provides the infrastructure).
2. There is a framework for the analysis of trustworthy ICT that is applicable to the Web that allows for the complete analysis of the problem, including an explanation for the variety of existing views.
3. There may be aspects of systemic trustworthiness that are valuable yet not fully discovered, and that such systemic

aspects of the trustworthiness should drive developments in trustworthy ICT and trustworthy Web.

4. Practical design guidelines for trustworthy systems can be defined, but that such trustworthiness cannot be captured as a requirement or satisfied by the current development process, so that changes to the process are necessary.

All those postulates point to the fact that trustworthiness is likely to be a systemic issue, i.e., the issue of trust between different systems. Therefore it is necessary to establish a reference model of the society, together with the generative social reality, and its relationship to the physical reality. Within such a model, ICT infrastructure and the Web has to be positioned.

From there, it will be possible to understand who is actually supposed to trust the infrastructure, and what properties of the infrastructure make it trustworthy. Only after this rather long introduction, it will be possible to analyse different systems and their trust in the Web or any other ICT infrastructure, and to see what properties of such an infrastructure make it trustworthy for them. Eventually, means of improving trustworthiness can be discussed and conclusions drawn.

1.5 Structure

This monograph is structured as a discussion that gradually introduces relevant concepts, illustrating them, whenever possible, with case studies. It starts with a research overview that elaborates on several modern views on trustworthy ICT and the Web. Next, the systemic, socio-technical model is briefly introduced, followed by the discussion on trust. The analysis of the model leads to six views on trustworthiness, some of them compatible with modern views already identified earlier in this monograph. This is followed by the discussion of trust on the Web and on the Semantic Web. Finally, a systemic view on trustworthiness is then explored in details, followed by concluding remarks.

It is not necessary to read this monograph 'as is', from its first to its last page. An alternative method may be selected, depending on

reader's interest. In order to capture main proposition presented in this monograph, it is suggested to read:

> Introduction (Section 1).
> Literature review (Section 2, specifically 2.2).
> Introduction to systemic approach (Section 3).
> Re-visiting views on trustworthiness and trust (Section 6, specifically Section 6.1).
> Conclusions (Section 9).

Case studies, scatted throughout the text, and written in a slightly provocative manner, are for illustration only and can be safely ignored while reading the main body of the text.

References

[1] A. Abdul-Rahman, "A framework for decentralised trust reasoning," Ph.D. Thesis. Available at: http://www.cs.ucl.ac.uk/staff/F.AbdulRahman/docs/thesis-final.pdf, 2005.

[2] L. Abramovsky and R. Griffith, "ICT, corporate restructuring and productivity," IFS Working Paper W09/10, 2009.

[3] C. Adams and S. Lloyd, *Understanding PKI: Concepts, Standards, and Deployment Considerations*. Addison-Wesley Professional, 2010.

[4] G. Alonso, *Web Services: Concepts, Architectures and Applications*. Springer, 2004.

[5] R. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*. John Wiley & Sons Inc, 2001.

[6] R. Anderson, "Cryptography and competition policy. Issues with 'trusted computing'," in *Second Annual Workshop on Economics and Information Security*, pp. 29–30, University of Maryland, May 2003.

[7] S. Anderson et al., "Web services trust language (WS-Trust)," Available at: http://specs.xmlsoap.org/ws/2005/02/trust/WS-Trust.pdf, 2005.

[8] M. Arion, J. H. Numan, H. Pitariu, and R. Jorna, "Placing trust in human-computer interaction," in *Proceedings of 7th European Conference on Cognitive Ergonomics (ECCE 7)*, pp. 353–365, 1994.

[9] M. Armbrust et al., "A view of cloud computing," *Communications of the ACM*, vol. 53, no. 4, pp. 50–58, 2010.

[10] D. Artz and Y. Gil, "A survey of trust in computer science and the semantic web," *Journal of Web Semantics: Science, Services and Agents on the World Wide Web*, 2007.

[11] R. Ashri, T. Payne, D. Marvin, M. Surridge, and S. Taylor, "Towards a semantic web security infrastructure," in *Semantic Web Services (2004) Spring Symposium Series*, Stanford University, Stanford California, 22–26 March 2004.
[12] M. Bacharach, "How human trusters assess trustworthiness in quasi-virtual contexts," in *AAMAS2002 Workshop on Deception, Fraud and Trust in Agent Societies*, 2002.
[13] B. Barber, *The Logic and Limits of Trust*. Rutgerts University Press, 1983.
[14] K. Beck and C. Andres, *Extreme Programming Explained: Embrace Change*. Addison Wesley, 2004.
[15] M. Benantar, *Access Control Systems: Security, Identity Management and Trust Models*. Springer, 2006.
[16] P. Birks, *The Classification of Obligations*. Clarendon Press, 1997.
[17] M. Bishop, *Introduction to Computer Security*. Addison-Wesley, 2005.
[18] M. Blaze, J. Ioannidis, and A. D. Keromytis, "Experience with the keynote trust management system: Applications and future directions," in *Proceedings of International Conference on Trust Management iTrust 2003*, pp. 284–300, 2003.
[19] R. E. Bloomfield, "Resilient to the unexpected," *IEEE Security and Privacy*, vol. 9, no. 3, pp. 3–4, 2011.
[20] P. A. Bonatti and D. Olmedilla, "Driving and monitoring provisional trust negotiation with metapolicies," in *IEEE 6th International Workshop on Policies for Distributed Systems and Networks (POLICY)*, pp. 14–23, Stockholm, Sweden: IEEE Computer Society, June 2005.
[21] Books, *Computer Security Standards: Common Criteria*. Books Llc, 2010.
[22] M. Branchaud and S. Flinn, "xTrust: A scalable trust management infrastructure," in *Second Annual Conference on Privacy, Security and Trust (PST 2004)*, pp. 207–218, NRC 47411, Fredericton, New Brunswick, Canada, October 14–15 2004.
[23] M. Broersma, "NHS top culprit as UK data breaches exceed 1,000. ZDNet," Available at: http://www.zdnet.co.uk/news/compliance/2010/06/01/nhs-top-culprit-as-uk-data-breaches-exceed-1000-40089098/, 2010.
[24] D. Bunker, K. Kautz, and A. L. T. Nguyen, "The role of value compatibility in information technology adoption," in *The Transfer and Diffusion of Information Technology for Organizational Resilience*, vol. 206, (B. Donnellan, T. J. Larsen, L. Levine, and J. I. DeGross, eds.), pp. 53–70, Springer IFIP, 2006.
[25] A. Calder, *Implementing Information Security Based on ISO 27001/ISO 27002: A Management Guide*. Van Haren Publishing, 2009.
[26] L. J. Camp, *Trust and Risk in Internet Commerce*. The MIT Press, 2000.
[27] M. Carbone, M. Nielsen, and V. Sassone, "A formal model for trust in dynamic networks," BRICS Report Series RS-03-4, 2003.
[28] M. Casassa Mont and R. Thyne, "A systemic approach to automate privacy policy enforcement in enterprises," Privacy Enhancing Technologies. Lecture Notes in Computer Science, vol. 4258/2006, pp. 118–134, 2006.
[29] C. Castelfranchi and R. Falcone, "Trust is much more than subjective probability: Mental components and sources of trust," in *Proceedings of the 33rd Hawaii International Conference on System Sciences (HICSS2000)*,

vol. 6, Available at: http://www.istc.cnr.it/T3/download/Trust-more-than-probability.pdf, 2000.

[30] S. M. Chandran, K. Panyim, and J. B. D. Joshi, "A requirements-driven trust framework for secure interoperation in open environment," in *iTrust 2006, LNCS 3986*, (K. Stolen et al., eds.), Springer, 2006.

[31] E. Chang, T. Dillion, and F. K. Hussain, *Trust and Reputation for Service-Oriented Environments: Technologies for Building Business Intelligence and Consumer Confidence*. John Wiley & Sons, Ltd, 2006.

[32] H. Chaouchi, *The Internet of Things: Connecting Objects*. Wiley-Blackwell, 2010.

[33] K. Clarke, G. Hardstone, M. Rouncefield, and I. Sommerville, eds., *Trust in Technology: A Socio-Technical Perspective*. Springer, 2006.

[34] K. Clarke, J. Hughes, M. Rouncefield, and T. Hemmings, "When a bed is not a bed: Calculation and calculability in complex organisational settings," in *Trust in Technology: A Socio-Technical Perspective*, (K. Clarke, G. Hardstone, M. Rouncefield, and I. Sommerville, eds.), Springer, 2006.

[35] R. A. Cloran, *Trust on the Semantic Web*. MSc Dissertation, Rhodes University, 2006.

[36] P. Cofta, "Confidence creation framework of eBay," in *Proceedings of NAEC2006 Networking and Electronic Commerce Research Conference*, Italy, 2006.

[37] P. Cofta, "Distrust," in *Proceedings of International Conference on Electronic Commerce ICEC'06*, pp. 250–258, Fredericton, Canada, 2006.

[38] P. Cofta, "Confidence, trust and identity," *BT Technology Journal*, vol. 25, no. 2, April 2007.

[39] P. Cofta, *Trust, Complexity and Control: Confidence in a Convergent World*. J. Wiley & Sons, 2007.

[40] P. Cofta, "The Googleplex," in *Proceedings of the 10th International Conference on Electronic Commerce*, Innsbruck, Austria, vol. 342, ACM International Conference Proceeding Series, 2008.

[41] P. Cofta, "Towards a better citizen identification system," *Identity in the Information Society*, vol. 1, no. 1, pp. 39–53, 2009.

[42] P. Cofta et al., "Method for binding a program module," WO 01/48604, 1999.

[43] J. Coleman, *Foundations of Social Theory*. The Belknap Press of Harvard University Press, 1990.

[44] L. L. Cummings and P. Bromiley, "The organizational trust inventory (OTI): Development and validation," in *Trust in Organizations*, (R. M. Kramer and T. R. Tyler, eds.), Sage Publications, 1996.

[45] M. d'Aquin, S. Elahi, and E. Motta, "Semantic monitoring of personal Web activity to support the management of trust and privacy," in *Proceedings of the Second International Workshop on Trust and Privacy on the Social and Semantic Web (SPOT 2010) co-located with the 7thAnnual Extended Semantic Web Conference (ESWC 2010)*, (P. Karger et al., eds.), Heraklion, Crete, Greece. Published online as CEUR Workshop Proceedings, ISSN 1613-0073, Vol. 576, Available at http://CEUR-WS.org/Vol-576, May 31 2010.

[46] J. Davies, D. Fensel, and F. van Harmelen, *Towards the Semantic Web: Ontology-driven Knowledge Management*. Wiley-Blackwell, 2002.

[47] C. Dellarocas and P. Resnick, "Online reputation mechanisms: A roadmap for future research," Available at: http://ccs.mit.edu/dell/papers/symposiumreport03.pdf, 2003.
[48] E. Denham, "Report of findings into the complaint filed by the Canadian internet policy and public interest clinic (CIPPIC) against facebook inc. Under the personal information protection and electronic documents act," Available at: http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.pdf, 2009.
[49] D. C. Dennett, *The Intentional Stance*. Bradford Books, 1989.
[50] M. Deutsch, *The resolution of conflict: Constructive and destructive processes*. Yale University, USA, 1973.
[51] N. Dimmock, J. Bacon, D. Ingram, and K. Moody, "Risk models for trust-based access control (TBAC)," in *iTrust2005, LNCS 3477*, (P. Herrmann, ed.), pp. 364–371, 2005.
[52] DoD, "Department of defence," *Trusted Computer Evaluation Criteria*, 1983.
[53] M. D. Dorsher, "Hegemony online: The quiet convergence of power, culture, and computers," Ph.D. Dissertation, University of Maryland, USA. Available at: http://www.uwec.edu/mdorsher/ica2001, 2001.
[54] B. Dragovic, S. Hand, T. Harris, E. Kotsovinos, and A. Twigg, "Managing trust and reputation in the XenoServer open platform," in *Proceedings of iTrust 2003*, (P. Nixon and S. Terzis, eds.), pp. 59–74, Trust Management, LNCS 2692, 2003.
[55] N. Dwyer, T. Clark, D. Randall, and P. Cofta, "Where everyone knows your name: Trust in a localised media environment," in *Proceedings of 4th IFIP WG 11.11 International Conference on Trust Management*, Morioka, Iwate, Japan, June 14–18 2010.
[56] N. Dwyer and P. Cofta, Understanding the grounds to trust: Game as a cultural probe. Presented at Web 2.0 Trust (W2Trust), Trondheim, Norway in conjunction with IFIPTM, 2008.
[57] Economist, "Con of the century," *The Economist*, December 18 2008.
[58] Economist, "Serfing the web," *The Economist*, p. 77, 13-19. 11.2010 2010.
[59] J. Egan, *Rethinking Construction: Report of the Construction Task Force*. London: HMSO, 1998.
[60] F. Egger, "Consumer trust in E-commerce: From psychology to interaction design," in *Trust in Electronic Commerce*, (J. E. J. Prins, ed.), Kluwer, 2002.
[61] D. Elgesem, "Normative structures in trust management," in *iTrust 2006, LNCS 3986*, (K. Stolen et al., eds.), pp. 48–61, 2006.
[62] C. Ellison et al., "SPKI certificate theory — IETF RFC 2693," Technical Report, The Internet Society, September 1999.
[63] T. Erl, *Service-Oriented Architecture: Concepts, Technology, and Design*. Prentice-Hall, 2005.
[64] European Union, "Work Programme 2011-12. ICT — Information and Communication Technologies," Available at: ftp://ftp.cordis.europa.eu/pub/fp7/ict/docs/ict-wp-2011-12_en.pdf, 2009.
[65] D. Fensel, J. Hendler, H. Lieberman, and W. Wahlster, eds., *Spinning the Semantic Web: Bringing the World Wide Web to Its Full Potential*. MIT Press, 2005.

[66] E. Ferrari and B. M. Thuraisingham, eds., *Web and Information Security*. Idea Group Inc, 2006.

[67] M. Fishbein and I. Ajzen, *Beliefs, Attitude, Intentions and Behaviour: An Introduction to Theory and Research*. Addison-Wesley, Reading, MA, USA, 1975.

[68] K. Fogel, *Producing Open Source Software: How to Run a Successful Free Software Project*. O'Reilly Media, 2005.

[69] F. Fukuyama, *Trust: The Social Virtues and the Creation of Prosperity*. Touchstone Books, 1996.

[70] K. Fullam, T. B. Klos, G. Muller, J. Sabater, A. Schlosser, Z. Topol, K. S. Barber, J. S. Rosenschein, L. Vercouter, and M. Voss, "A specification of the agent reputation and trust (ART) testbed: Experimentation and competition for trust in agent societies," in *AAMAS*, pp. 512–518, 2005.

[71] D. Gambetta, "Can we trust?," in *Trust: Making and Breaking Cooperative Relations*, electronic edition, Department of Sociology, University of Oxford, chapter 13, (D. Gambetta, ed.), pp. 213–237, 2000. Available at: http://www.sociology.ox.ac.uk/papers/gambetta213-237.

[72] P. Ganley and B. Allgrove, "Net neutrality: A user's guide," *Computer Law & Security Report*, vol. 22, no. 6, pp. 454–463, 2006.

[73] A. Gehlen, *Man in the Age of Technology, Trans. Patricia Lipscomb*. New York: Columbia University Press, 1980.

[74] A. Giddens, *The Constitution of Society: Outline of the Theory of Structuration*. Cambridge: Polity Press, 1984.

[75] A. Giddens, *Modernity and Self-identity: Self and Society in the Late Modern Age*. Polity Press, 1991.

[76] I. M. Goklany, *The Improving State of the World: Why We're Living Longer, Healthier, More Comfortable Lives On a Cleaner Planet*. Cato Institute, 2007.

[77] J. Golbeck, *Trust on the World Wide Web: A Survey. Foundations and Trends in Web Science 1:2*. now Publishers Inc, 2006.

[78] J. Golbeck, *Computing with Social Trust*. Springer, 2008.

[79] J. Golbeck and J. Hendler, "Reputation network analysis for email filtering," in *Proceedings of the First Conference on Email and Anti-Spam*, Mountain View, California, July 30-31 2004.

[80] J. Golbeck, B. Parsia, and J. Hendler, "Trust Networks on the Semantic Web," in *Cooperative Information Agents VII: Seventh International Workshop on Cooperative Information Agents*, (M. Klusch et al., eds.), Helsinki, Finland: Springer-Verlag, Berlin Heidelberg, 2003.

[81] J. Gorski, A. Jarzebowicz, and J. Miler, "Arguing trustworthiness of e-health services with the Trust-IT framework," in *Proceedings of 25th Healthcare Computing conference*, Harrogate, UK, 21-23 April 2008.

[82] T. Grandison, "Trust management for internet applications," PhD thesis, University of London, UK, 2003.

[83] N. Gujral et al., "Modelling multi-dimensional trust," in *Proceedings of Fifth International Conference on Autonomous Agents and Multiagent Systems AAMAS-06*, Hakodate, Japan, 2006.

[84] Z. Gyongyi, H. Garcia-Molina, and J. Pedersen, "Combating web spam with trustrank," in *Proceedings of the 30th VLDB Conference*, Toronto, Canada, 2004.

[85] R. Hardin, ed., *Trust and Trustworthiness*. Russell Sage Foundation, 2002.

[86] G. Hardstone, d'Adderio, and R. Williams, "Standardisation, trust and dependability," in *Trust in Technology: A Socio-Technical Perspective*, (K. Clarke, G. Hardstone, M. Rouncefield, and I. Sommerville, eds.), Springer, 2006.

[87] O. Hartig, "Towards a data-centric notion of trust in the Semantic Web (a position statement)," in *Proceedings of the Second International Workshop on Trust and Privacy on the Social and Semantic Web (SPOT 2010) co-located with the 7thAnnual Extended Semantic Web Conference (ESWC 2010)*, vol. 576, (P. Karger et al., eds.), Heraklion, Crete, Greece. Published online as CEUR Workshop Proceedings, ISSN 1613-0073, May 31 2010. Available at: http://CEUR-WS.org/Vol-576.

[88] P. Himanen, *The Hacker Ethic*. Random House, 2001.

[89] P. Hodgson and P. Cofta, "Society As An Information Network," *International Journal of Technology, Knowledge and Society*, vol. 4, no. 1, pp. 1–10, 2008.

[90] ICO, 2010, Information Commissioner's Office: USB containing sensitive patient data lost on train, Press Release, 20 September.

[91] D. Ingram, "An evidence based architecture for efficient, attack-resistant computational trust dissemination in peer-to-peer networks," in *iTrust 2005, LNCS 3477*, (P. Herrmann et al., eds.), pp. 273–288, 2005.

[92] J. Isham, "The effect of social capital on technology adoption: Evidence from rural Tanzania," Opportunities in Africa: Micro-evidence on Firms and Households. (Retrieved 18 October, 2007), Available at: http://www.csae.ox.ac.uk/conferences/2000-OiA/pdfpapers/isham.PDF, 2000.

[93] ITU, 1994, International Communication Union Recommendation X.200: Information Technology — Open System Interconnection — Basic Reference Model: The Basic Model.

[94] M. Jakobsson and S. Myers, eds., *Phishing and Counter-Measures: Understanding the Increasing Problem of Electronic Identity Theft*. Wiley-Blackwell, 2007.

[95] B. K. Jayaswal and P. C. Patton, *Design for Trustworthy Software: Tools, Techniques, and Methodology of Developing Robust Software*. Prentice Hall, 2006.

[96] C. D. Jensen and P. O'Connell, "Trust-based route selection in dynamic source routing," in *iTrust 2006, LNCS 3986*, (K. Stolen et al., eds.), pp. 150–163, 2006.

[97] A. J. I. Jones and B. S. Firozabadi, "On the characterisation of a trusting agent — aspects of a formal approach," in *Trust and Deception in Virtual Societies*, (C. Castelfranchi and Y.-H. Tan, eds.), pp. 157–168, Kluwer Academic Publishers, 2001.

[98] A. Josang, "A logic for uncertain probabilities," *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, vol. 9, pp. 279–311, 2001.

[99] A. Josang, C. Keser, and T. Dimitrakos, "Can we manage trust?," in *Proceedings of the 3rd International Conference on Trust Management, (iTrust)*, Paris, May 2005.
[100] A. Josang, S. Marsh, and S. Pope, "Exploring Different Types of Trust Propagation," in *iTrust 2006, LNCS 3986*, (K. Stolen at al., eds.), pp. 179–192, Springer-Verlag, 2006.
[101] A. Josang and D. McAnally, "Multiplication and Comultiplication of Beliefs," *International Journal of Approximate Reasoning*, vol. 38, no. 1, pp. 19–55, 2004.
[102] C. Keser, "Experimental games for the design of reputation management systems," *IBM Systems Journal*, vol. 42, no. 3, 2003.
[103] J. Kong, X. Hong, and M. Gerla, "An identity-free and on-demand routing scheme against anonymity threats in mobile ad hoc networks," *IEEE Transactions on Mobile Computing*, vol. 6, no. 8, pp. 888–902, 2007.
[104] H. Lacohée, P. Cofta, A. Phippen, and S. Furnell, "Understanding public perceptions: Trust and engagement in ICT mediated services," *International Engineering Consortium*, 2008.
[105] W. Lassar, B. Mittal, and A. Sharma, "Measuring customer-based brand equity," *Journal of Consumer Marketing*, vol. 12, no. 4, pp. 11–19, 1995.
[106] J. K. Lee et al., "Secure knowledge management and the semantic Web," *Communications of the ACM — The semantic e-business vision*, vol. 48, no. 12, December 2005.
[107] A. Leon, *Software Configuration Management Handbook*. Artech House, 2004.
[108] V. Lepetit and M.-O. Berger, "An intuitive tool for outlining objects in video sequences: Applications to augmented and diminished reality," in *Proceedings of the International Symposium on Mixed Reality*, Yokohama, Japan, 2001.
[109] L. Lessig, *Code and Other Laws of Cyberspace*. Basic Books, 1999.
[110] B. Leuf, *The Semantic Web: Crafting Infrastructure for Agency*. Wiley-Blackwell, 2005.
[111] R. L. Levien, "Attack resistant trust metrics," Ph.D. Thesis, University of Berkeley, Available at: http://www.levien.com/thesis/thesis.pdf, 2002.
[112] R. J. Lewicki and B. B. Bunker, "Developing and maintaining trust in work relationships," in *Trust in Organisations: Frontiers of theory and Research*, 1996.
[113] S. K. Lippert and M. Davis, "A conceptual model integrating trust into planned change activities to enhance technology adoption," *Journal of Information Science*, vol. 32, 2006.
[114] P. Lucas and L. Van Der Gaal, *Principles of Expert Systems*. Addison-Wesley Publishing, 1991.
[115] M. Luck et al., *Agent Technology: Computing as Interaction. A Roadmap for Agent based Computing*. AgentLink, 2005.
[116] N. Luhmann, *Trust and Power*. John Wiley & Sons, 1979.
[117] N. Luhmann, *Social Systems*. Stanford University Press, 1995.
[118] N. Luhmann, *Risk: A Sociological Theory*. AldineTransaction, 2005.
[119] S. Maleki, "Trust and reputation on the semantic Web," Report COMP6028, University of Southampton, 2010.

[120] M. Manion and W. M. Evan, "Technological catastrophes: Their causes and prevention," *Technology in Society*, vol. 24, no. 3, pp. 207–224, August 2002.
[121] S. P. Marsh, "Formalising trust as a computational concept," University of Stirling PhD thesis, Available at: http://www.nr.no/∼abie/Papers/TR133.pdf, 1994.
[122] S. Marti et al., "Mitigating routing misbehavior in mobile ad hoc networks," in *Proceedings MobiCom '00 Proceedings of the 6th Annual International Conference on Mobile Computing and Networking*, 2000.
[123] R. C. Mayer, J. H. Davis, and F. D. Schoorman, "An integrative model of organizational trust," *Academy of Management Review*, vol. 20, no. 3, pp. 709–734, 1995.
[124] J. C. McCroskey, "Scales for the measurement of ethos," *Speech Monographs*, vol. 33, pp. 65–72, 1966. Available at: http://www.jamescmccroskey.com/publications/22.htm.
[125] D. H. McKnight and N. L. Chervany, "The meanings of trust," University of Minnesota, Available at: http://www.misrc.umn.edu/wpaper/wp96-04.htm, 1996.
[126] D. H. McKnight, V. Choudhury, and C. Kacmar, "Developing and validating trust measures for e-commerce: An integrative typology," *Information Systems Research*, vol. 13, no. 3, pp. 334–359, 2002.
[127] I. Menken and G. Blokdijk, *Virtualization: The Complete Cornerstone Guide to Virtualization Best Practices*. Emereo Publishing, 2008.
[128] R. R. Moeller, *IT Audit, Control and Security*. John Wiley & Sons, 2010.
[129] G. Mollering, "The trust/control duality: An integrative perspective on positive expectations of others," *Int. Sociology*, vol. 20, no. 3, pp. 283–305, September 2005.
[130] G. Mollering, *Trust: Reason, Routine, Reflexivity*. Elsevier, 2006.
[131] T. Moreton and A. Twigg, "Enforcing collaboration in peer-to-peer routing services," in *Trust Management First International Conference on Trust Management iTrust*, (P. Nixon and S. Terzis, eds.), Springer-Verlag, LNCS 2692, 2003.
[132] L. Mui and M. Mohtashemi, "Rational decision making using social information," Submission to Rationality and Society, March 12 2002.
[133] L. Mui, M. Mohtashemi, and A. Halberstadt, "A computational model of trust and reputation," in *35th Hawaii International Conference on System Science (HICSS)*, 2002.
[134] C. Mundie et al., "Trustworthy computing," Microsoft White Paper, Available at: http://download.microsoft.com/download/a/f/2/af22fd56-7f19-47aa-8167-4b1d73cd3c57/twc_mundie.doc, 2002.
[135] J. Nair, "User driven product innovation," Thesis, S. M., Massachusetts Institute of Technology, System Design and Management Program, 2007.
[136] J. Nielsen, *Usability Engineering*. Academic Press Inc, 1993.
[137] M. Nielsen and K. Krukow, "On the formal modelling of trust in reputation-based systems," in *Theory Is Forever, Essays Dedicated to Arto Salomaa on the Occasion of His 70th Birthday, Lecture Notes in Computer Science 3113*, (J. Karhumäki et al., eds.), Springer, 2004.

[138] B. Nooteboom, "Framing, attribution and scripts in the development of trust," in *Proceedings of Symposium on 'Risk, Trust and Civility'*, Victoria College, University of Toronto, 6–8 May 2005.

[139] K. O'Hara, H. Alani, Y. Kalfoglou, and N. Shadbolt, "Trust strategies for the semantic Web," in *Workshop on Trust, Security, and Reputation on the Semantic Web, 3rd International (ISWC'04)*, Hiroshima, Japan, 7–11 November 2004.

[140] K. O'Hara and N. Shadboldt, "Knowledge technologies and the semantic Web," in *Trust and Crime in Information Societies*, (R. Mansell and B. S. Collins, eds.), Edward Elgar Publishing, 2005.

[141] L. Page, S. Brin, R. Motwani, and T. Winograd, *The PageRank Citation Ranking: Bringing Order to the Web*. Stanford Digital Library Technologies Project, 1998.

[142] S. Pearson et al., *Trusted Computing Platforms: TCPA Technology in Context*. Prentice Hall, 2002.

[143] D. Peled, *Software Reliability Methods*. Springer, 2010.

[144] H. Peng and L. Niu, "Two-way exchange of virtual currency: Future tendency and inherent risks," in *International Conference on Future Networks*, pp. 220–224, Bangkok, 7–9 March 2009.

[145] S. Pentland and T. Heibeck, "Understanding 'honest signals' in business," *MIT Sloan Management Review*, vol. 50, no. 1, pp. 70–75, Fall 2008.

[146] T. Pinch and W. Bijker, *The Social Construction of Facts and Artefacts: Or How the Sociology of Science and the Sociology of Technology Might Benefit Each Other*. Bijker, Pinch, and Hughes, 1987.

[147] N. Pissinou, T. Ghosh, and K. Makki, "Collaborative trust-based secure routing in multihop ad hoc networks," in *NETWORKING 2004, Networking Technologies, Services, and Protocols; Performance of Computer and Communication Networks; Mobile and Wireless Communications. Lecture Notes in Computer Science*, vol. 3042/2004, (M. Nikolas et al., eds.), pp. 1446–1451, Springer, 2004.

[148] N. N. Potter, *How Can I Be Trusted?: A Virtue Theory Of Trustworthiness*. Rowman & Littlefield Publishers, 2002.

[149] D. Powell and R. Stroud, eds., Conceptual Model and Architecture of MAFTIA. Project IST-1999-11583: Malicious- and Accidental-Fault Tolerance for Internet Applications. MAFTIA deliverable D21, 2003.

[150] R. D. Putnam, *Bowling Alone. The Collapse and Revival of American Community*. Simon & Schuster, 2000.

[151] W. Rankl and W. Effing, *Smart Card Handbook*. Wiley-Blackwell, 2010.

[152] J. Rao and X. Su, "A survey of automated Web service composition methods," in *Semantic Web Services and Web Process Composition. Lecture Notes in Computer Science*, vol. 3387/2005, (J. Cardoso and S. Amit, eds.), pp. 43–54, Springer, 2005.

[153] M. Raza, F. K. Hussain, and E. Chang, "A methodology for quality-based mashup of data sources," in *iiWAS '08 Proceedings of the 10th International Conference on Information Integration and Web-based Applications & Services*, 2008.

[154] J. K. Rempel, J. G. Holmes, and M. P. Zanna, "Trust in close relationships," *Journal of Personality and Social Psychology*, vol. 49, no. 1, pp. 95–112, 1985.
[155] P. Resnick, "The value of reputation on eBay: a controlled experiment," *Experimental Economics*, vol. 9, no. 2, pp. 79–101, June 2006. Available at: http://www.si.umich.edu/~presnick/papers/postcards/PostcardsFinalPrePub.pdf.
[156] P. Resnick et al., "GroupLens: An open architecture for collaborative filtering of netnews," in *Proceedings of the 1994 ACM Conference on Computer Supported Cooperative Work*, pp. 175–186, Chapel Hill, North Carolina, United States, 1994. Available at: http://delivery.acm.org/10.1145/200000/192905/p175-resnick.pdf?key1=192905&key2=8948234411&coll=portal&dl=ACM&CFID=68878040& CFTOKEN=74261221.
[157] M. Richardson, R. Agrawal, and P. Domingos, "Trust management for the semantic Web," in *ICWS 2003. LNCS 2870*, (D. Fensel et al., eds.), pp. 351–368, Springer-Verlag Berlin Heidelberg, 2003.
[158] J. Riegelsberger, M. A. Sasse, and J. D. McCarthy, "The mechanics of trust: A framework of research and design," *International Journal of Human-Computer Studies*, vol. 62, no. 3, pp. 381–422, March 2005.
[159] J. B. Rotter, "Generalized expectancies for interpersonal trust," *American Psychologist*, vol. 26, no. 5, pp. 443–452, 1971.
[160] M. N. K. Saunders and A. Thornhill, "Organisational justice, trust and the management of change: An exploration," *Personnel Review*, vol. 32, no. 3, pp. 360–375, 2003.
[161] S. C. Saunders, *Reliability, Life Testing and the Prediction of Service Lives: For Engineers and Scientists*. Springer, 2007.
[162] A. Schlosser, M. Voss, and L. Bruckner, "Comparing and evaluating metrics for reputation systems by simulation," in *Proceedings of the IEEE Workshop on Reputation in Agent Societies*, 2004.
[163] J. R. Searle, *The Construction of Social Reality*. The Free Press, 1995.
[164] K. Sentz and S. Ferson, *Combination of Evidence in Dempster-Shafer Theory*. SAND 2002-0835. Binghamton University, 2002.
[165] C. Shirky, *Here Comes Everybody: How Change Happens when People Come Together*. Penguin Books, 2009.
[166] B. Shneiderman, "Designing trust into online experiences," *Communications of the ACM*, vol. 43, no. 12, pp. 57–59, 2000.
[167] J. Shore and S. Warden, *The Art of Agile Development*. O'Reilly Media, 2007.
[168] G. Shroff, *Enterprise Cloud Computing: Technology, Architecture, Applications*. Cambridge University Press, 2010.
[169] G. C. Silaghi, A. E. Arenas, and L. M. Silva, "Reputation-based trust management systems and their applicability to grids," CoreGRID Technical Report, Number TR-0064, February 23 2007.
[170] H. Simon, "A behavioral model of rational choice," *Models of Man*, 1957.
[171] M. P. Singh, "Trustworthy service composition: Challenges and research questions," in *Trust, Reputation, and Security: Theories and Practice, AAMAS 2002 Int. Workshop*, (R. Falcone et al., eds.), Bologna, Italy, July 15 2002. Selected and Invited Papers. Lecture Notes in Computer Science 2631 Springer.

[172] R. C. Solomon and F. Flores, *Building Trust in Business, Politics, Relationships and Life*. Oxford University Press, 2001.
[173] I. Sommerville, G. Dewsbury, K. Clarke, and M. Rouncefield, "Dependability and trust in organisational and domestic computer systems," in *Trust in technology: A socio-technical perspective*, (K. Clarke, G. Hardstone, M. Rouncefield, and I. Sommerville, eds.), Springer, 2006.
[174] I. Sommerville and P. Sawyer, *Requirements Engineering: A Good Practice Guide*. John Wiley & Sons, 1997.
[175] R. K. Stamper, "Organisational semiotics: Informatics without the computer?," in *Information, organisation and technology: Studies in organisational semiotics*, (K. Liu, R. J. Clarke, P. Bøgh Andersen, and R. K. Stamper, eds.), pp. 115–171, Boston, MA: Kluwer Academic Publishers, 2001.
[176] B. J. Steele, *Ontological Security in International Relations: Self-Identity and the IR State*. Routledge, 2008.
[177] B. Stone, *Amazon Erases Orwell Books From Kindle*. New York Times, July 17 2009.
[178] L. M. Surhone, M. T. Tennoe, and S. F. Henssonow, eds., *ITSEC. DoD Information Assurance Certification and Accreditation Program, Information Technology Security Assessment, AAA Protocol*. Betascript Publishing, 2010.
[179] P. Sztompka, *The Sociology of Social Change*. Blackwell Publishers, 1994.
[180] Y. B. Tang, H. M. Wang, and W. Dou, "Trust based incentive in P2P network," in *Proceedings of IEEE International Conference on E-Commerce Technology for Dynamic E-Business (CEC-East'04)*, Beijing, China, 2004.
[181] S. Turkle, *The Second Self: Computers and the Human Spirit*. Simon & Schuster, 1984.
[182] S. Turkle, *Alone Together: Why We Expect More From Technology and Less From Each Other*. Basic Books, 2011.
[183] A. Twigg, "A subjective approach to routing in P2P and ad hoc networks," in *Proceedings of First International Conference on Trust Management iTrust 2003*, pp. 225–238, Springer-Verlag LNCS 2692, 2003.
[184] J. Urquhart, "The biggest cloud-computing issue of 2009 is trust," *CNet News*, January 7 2009.
[185] E. M. Uslaner, *The Moral Foundations of Trust*. Cambridge University Press, 2002.
[186] D. van Rooy and J. Bus, "Trust and privacy in the future internet — a research perspective," *Identity in the Information Society*, vol. 3, no. 2, pp. 397–404, 2010.
[187] A. Ward and J. Smith, *Trust and Mistrust. Radical Risk Strategies in Business Relationships*. John Wiley and Sons Ltd, 2003.
[188] C. Weifang, L. Xiangke, S. Changxiang, L. Shanshan, and P. Shaoliang, "A trust-based routing framework in energy-constrained wireless sensor networks," in *Wireless Algorithms, Systems, and Applications. Lecture Notes in Computer Science*, vol. 4138/2006, (C. Xiuzhen et al., eds.), pp. 478–489, 2006.
[189] M. Wilbur, *A Decade of the DMCA*. lulu.com, 2009.
[190] F. Wilder, *A Guide to the TCP/IP Protocol Suite*. Artech House, 1998.

[191] L. P. Willcocks and S. Cullen, "The outsourcing enterprise: The power of relationships," Available at: http://www.logicacmg.com/pSecured/admin/countries/assets/serve_asset.asp?id=3252, 2006.
[192] M. A. Willson, *Technically Together. Rethinking Community within Techno-Society*. Peter Lang Publishing, 2006.
[193] P. J. Windley, *Digital Identity*. O'Reilly Media, 2005.
[194] W. H. Winsborough, K. E. Seamons, and V. E. Jones, "Automated trust negotiation," in *Proceedings of the DARPA Information Survivability Conference and Exposition*, pp. 88–102, IEEE, Los Alamitos, CA, 2000.
[195] A. M. Wyglinski, M. Nekovee, and T. Hou, eds., *Cognitive Radio Communications and Networks: Principles and Practice*. Academic Press, 2010.
[196] J. Yang and F.-B. Sun, "A comprehensive review of hard-disk drive reliability," in *Proceedings of Reliability and Maintainability Symposium*, Washington, DC, USA, 18–21 January 1999.
[197] E. Yourdon, *Managing the System Life Cycle: Software Development Methodology Overview*. Yourdon Press, 1983.
[198] P. J. Zak, "The neuroeconomics of trust," in *Renaissance in Behavioral Economics*, (R. Frantz, ed.), Routledge, 2009.
[199] C.-N. Ziegler, "Scalable Trust propagation Models," *Information Security Bulletin*, vol. 10, July 2005.
[200] P. Zimmermann, ed., *PGP User's Guide*. MIT Press, Cambridge, 1994.