A UNIFIED TRUST MODEL FOR PERVASIVE COMPUTING ENVIRONMENT

HAMED KHIABANI

UNIVERSITI TEKNOLOGI MALAYSIA

A UNIFIED TRUST MODEL FOR PERVASIVE COMPUTING ENVIRONMENT

HAMED KHIABANI

A thesis submitted in fulfilment of the
requirements for the award of the degree of
Doctor of Philosophy (Computer Science)

Faculty of Computing
Universiti Teknologi Malaysia

AUGUST 2013

To my dear parents

To my beloved wife *Sanaz*

To my sweet daughter *Bahareh*

ACKNOWLEDGEMENTS

First of all, I am grateful to Allah almighty for blessing me the courage, wisdom and strength to carry out my PhD studies. I would like to express my most sincere gratitude to my supervisors, Dato' Professor Dr. Norbik Bashah Idris and Dr. Jamalul-lail Ab Manan. Professor Norbik has had a convincing effect on me, and made me continue forward. In spite of his extraordinary workload, he always allocated time for helping me whenever I needed his guidance and support. I am indebted to Dr. Jamalul-lail, who has enthusiastically followed up the progress of my work once a week, and has contributed with discussions and advices. It has been a pleasure for me to work under his supervision. I also wish to express special gratitude to MIMOS Berhad for funding my studies and providing a good environment for research. I also want to thank Dr. Félix Gómez Mármol for his generous help throughout the simulation of my study, and my fellow researchers who have given me input and assistance during my work, particularly Mr. Hadi KhorasaniZadeh and Dr. Ali DehghanTanha.

I want to express my sincere appreciation and deepest gratitude to my companion along this journey, my beloved wife Sanaz, for morally supporting my studies. Without her patience, love and perpetual encouragement, it would not have been possible to achieve this dream and overcome the difficulties occurred during studying abroad. I thank my sweet daughter Bahareh, who is my source of everyday energy and encouraged me with her smiles. Thank you both for your understanding the worth of less time spent with you because of this research.

Finally, I would like to express my heartfelt thanks to my father for his endless support and sacrifices, and to my mother for her unconditional love and care throughout my life. Moreover, I would like to thank my brother, Saaed, for being available all the times and helping me in sorting out all my issues in home country. I thank my grandmother for her kindness and prayers, and my parents-in-law for their encouragement and keeping my wife’s spirits high. I also wish to thank my uncle, Mr. Jafar JafariTashan, who whetted my appetite for new knowledge during the school years, and all the teachers in my life who have influenced and inspired me.

P.S. The day I submitted my thesis for examination, my fate was unfortunate. My father passed away peacefully exactly the same date and I went back home only to visit his grave. It is needless to say that, this was truly the most difficult time of my life. I pray that Allah will shower his mercy on him and give me and my family patience in this tribulation.

ABSTRACT

Pervasive systems are weaving themselves in our daily life by making it possible for known and even unknown parties to collect user information invisibly and in an unobtrusive manner. The huge number of interactions between users and pervasive devices necessitate a comprehensive trust model which unifies different trust factors such as context, recommendation, and history that would be used to calculate precisely the trust level of each party. Therefore, developing a runtime and accurate trust computation would be a major issue in these environments. Measuring accurately the integrity of nodes willing to interact with each other can enhance the trust calculation process, particularly during the uncertainty state and initiation phase. Trusted computing enables effective solutions to verify the trustworthiness of computing platforms. This research aims to provide a unified and dynamic approach while considering several trust dimensions namely: history, recommendation, context, and attesting the communicating platforms to increase accuracy of trust computation mechanism. In this research, the Unified Trust Model (UTM) is proposed to calculate trustworthiness of entities based on history, recommendation, context, and platform integrity measurement (used in remote attestation). The accuracy and performance of UTM were evaluated using a simulation-based method in different experimental scenarios. A comparison of UTM with similar works showed that the accuracy of the model improved from 2% to 41.3% during an oscillating attack and from 7.4% to 26.8% during a collusion attack. The results obtained from the different simulated scenarios have demonstrated that the proposed UTM is highly accurate and can be used effectively in realistic as well as low interaction environments.

ABSTRAK

Sistem Pervasif semakin mempengaruhi hidupan harian kita, membenarkan individu untuk memungut maklumat pengguna secara sembunyi, menggunakan kaedah yang tidak menggangu sama ada melalui pihak–pihak yang dikenali atau tidak. Interaksi tidak terhingga diantara pengguna dan alat pervasive memerlukan sebuah model komprehensif yang menggambungkan pelbagai faktor amanah contohnya, konteks, rekomendasi dan latar sejarah untuk mengira tahap amanah setiap pihak secara jitu. Oleh yang demikian, suatu komputasi secara masalarian dan jitu adalah menjadi masalah besar dalam persekitaran sedemikian. Pengukuran jitu terhadap integriti nod nod yang berinteraksi dapat merangsang proses evolusi tersebut; khasnya dalam keadaan ketidaktentuan dan fasa permulaan. Trusted computing membolehkan penyelesaian efektif untuk membuktikan keamanahan (trustworthiness) sesuatu platform pengkomputeran. Penyelidikan ini adalah bertujuan untuk memberikan suatu pendekatan persatuan (unified) dan dinamik sementara mengambilkira beberapa dimensi amanah, seperti latar sejarah, rekomendasi, konteks,dan pembuktian (attesting) platfom yang berkomunikasi untuk meningkatkan kejituan mekanisma komputasi. Dalam penyelidikan ini kami mencadangkan dan membentangkan Unified Trust Model (UTM) yang mengira keamanahan entiti berdasarkan kepada latar sejarah, rekomendasi, konteks, dan pengukuran integriti platform (digunakan semasa keamanahan jarak jauh). Kejituan dan Persembahan model kami dinilai dengan menggunakan kaedah simulasi dalam pelbagai sinario ujikaji. Perbandingan diantara UTM dengan penyelidikan yang serupa, kami mendapati kejituannya dapat diperbaiki dari 2% ke 41.3% dalam suasana serangan berayun (oscillating attack), dan dari 7.4% ke 26.8% dalam serangan kolusi (collusion attack). Keputusan yang diperolehi daripada pelbagai senario simulasi menunjukkan kejituan yang tinggi daripada model yang dipersembahkan dan mempamerkan bahawa UTM dapat digunakan secara efektif dalam keadaan realistic dan juga persekitaran yang mempunyai interaksi rendah.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AIK	–	Attestation Identity Key
APT	–	Advanced Persistent Threats
CPS	–	Cyber Physical Systems
DAA	–	Direct Anonymous Attestation
EK	–	Endorsement Key
ICE	–	Indisputable Code Execution
IMA	–	Integrity Measurement Architecture
IoT	–	Internet of Things
MBA	–	Model-based Behaviour Attestation
ML	–	Measurement List
MLTM	–	Mobile Local-owner Trusted Module
MRTM	–	Mobile Remote-owner Trusted Module
MTM	–	Mobile Trusted Module
OpenTC	–	Open Trusted Computing
PBA	–	Property-based Attestation
PCR	–	Platform Configuration Registers
PIV	–	Program-Integrity Verification
PKI	–	Public Key Infrastructure
PRIMA	–	Policy-Reduced Integrity Measurement Architecture
QoS	–	Quality of Service
RA	–	Remote Attestation
SML	–	Stored Measurement Log

SRK	–	Storage Root Key
TC	–	Trusted Computing
TCB	–	Trusted Computing Base
TCG	–	Trusted Computing Group
TCPA	–	Trusted Computing Platform Alliance
TPM	–	Trusted Platform Module
TRMSim-WSN	–	Trust and Reputation Models Simulator for Wireless Sensor
TTP	–	Trusted Third Party
UTM	–	Unified Trust Model
WSN	–	Wireless sensor network

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Background of the Problem

Pervasive computing coined by Mark Weiser (1991) is an emerging research field that initiates innovative concepts and ideas into computer science. It provides ambient services and applications that allow users, devices, and applications in different physical locations to communicate unobtrusively. In a pervasive computing environment, the devices are interconnected and embedded in physical objects to collect, process, and transport information with the least human participation.

Trust has diverse definitions within different research disciplines. In computer science, trust is related to reliability and behaviour of a system according to design and policy. In a decentralized environment such as pervasive computing, security, trust and privacy are important issues since devices need to autonomously distinguish peers and then interact amongst them, without any human intervention.

In pervasive computing environments, devices encounter some security issues when communicating with each other. These security issues, that are most trust-related problems, can be summarized as follows (Ranganathan, 2004):

(a) Device authentication: It is difficult to establish a connection between devices, among many, within pervasive environments in which their interaction nature is temporary and ad-hoc. So during establishing a secure communication channel between two devices, each device must know which physical device it is communicating with, hence device authentication is crucial.

(b) Trust management and device assurance: In pervasive systems, even if a device knows which devices it is communicating with, the device must be able to assess whether its peer can be trusted, and whether it can share sensitive information or not. Meanwhile, the devices in pervasive systems must take in some high level security assurance properties.

(c) Recourse: Because of its inherent decentralized administrative ownership model in pervasive systems, it is more difficult to manage the risk in these systems than traditional ones. So the availability of recourse increases the psychological acceptability and reduces the risk.

(d) Availability: Due to the high amount of interconnections and decentralized nature of pervasive systems, we face larger attack surface with many points of failure in comparison to traditional computing environments, so pervasive systems are extremely vulnerable to the attacks that decrease the availability of system i.e. denial of service attacks.

(e) Privacy: In pervasive systems, autonomous interaction of devices with little awareness of the human entities can cause compromising of privacy of personal data or sensed information.

Since pervasive systems do not have any central control and the users are not predetermined, conventional access control mechanisms like authentication and authorization are not suitable for pervasive environments. Such environments require a security architecture based on *trust* to handle security and privacy problems (Kagal *et al.*, 2001; Sun and Denko, 2008). “The more sensitive the interaction in terms of security, privacy, or safety, the more trust there must be” (Trcek, 2011).

The most relevant sources of information to calculate trustworthiness of an entity are experiences of its peers based on the interactions; they had with that entity in the past. This is inspired from human society, from the way we evaluate and predict behaviour of the others before relying on them. Reliability of results depends on the complexity of the trust models in calculating the trustworthiness and the choices of parameters taken into account.

By calculating the trustworthiness, a pervasive device can estimate as accurate as possible its peer's "honesty" before interaction occurs. In general, trust management through trustworthiness calculations, enhances security and privacy for devices in pervasive computing environments, and hence improves the efficiency and quality of communications among devices.

1.2 Problem Statement

In pervasive computing environments, devices tend to interact without prior knowledge of each other and meanwhile need to distinguish each other autonomously without human intervention. The most noticeable properties of pervasive environments compared to other computer science domains are Ubiquity, Invisibility, Intimate data gathering and sharing (Lahlou *et al.*, 2005; Langheinrich, 2001). As it is clear, the pervasive computing properties raised several trust issues, i.e. invisible sensing of communication between two devices might happen even without user trusting any of these communication endpoints as well as the endpoints themselves. In such a decentralized environment, unprecedented data sharing could possibly allow unwanted information flow between heterogeneous entities. Therefore, providing automatic (and invisible) determination of user oriented trust calculation system is a must for any pervasive environment.

Since pervasive entities are constantly changing, trust determination is not simply a static and simple process. To overcome this problem, several trust models (Jøsang *et al.*, 2007; Gómez Mármol and Martínez Pérez, 2010b) have been proposed, each of which focusing on one of following trust dimensions:

(a) History: experience of an entity about its past interaction with its peer.

(b) Recommendation: experience of other entities.

(c) Context: situation that interaction happens.

Based on our study, the recent trust models migrate from single-dimension trust calculation models to multi-dimension trust calculation models. They are merging the above mentioned dimensions to achieve more accurate trustworthiness (Liu *et al.*, 2004; Wang and Varadharajan, 2005; Holtmanns and Yan, 2006; Sarkio and Holtmanns, 2007; Nguyen *et al.*, 2007; Sun and Denko, 2008; Yan and Holtmanns, 2008; Nguyen and Camp, 2008; Gómez Mármol and Martínez Pérez, 2010a).

In pervasive computing environments, because of the ad-hoc nature of interactions between devices and large number of possible devices willing to communicate, while development of trust-negotiation protocols are critically required, attesting trustworthiness of the devices could be useful (Ranganathan, 2004; Yan and Holtmanns, 2008). Combining trust management with the security mechanisms would be a significant contribution to the computing community, if it reduces the drawbacks and preserves its advantages (Trcek, 2011).

There are many suitable hardware and software properties that can be remotely attested using Trusted Computing (TCG, 2011b) technology. Trusted Computing defines the standards and specifications for multiple computing platforms to use an intelligent hardware to vouch for trustworthiness of the platform, its firmware and software components. This technique, which is called *attestation*, ensures the health of system, not only against software and hardware modification and tampering but even against the user.

The above discussion motivates the need for a trust calculation mechanism to effectively identify the most trustworthy node that helps in making any decision whether to do any interaction or activities. The trust calculation will also help us detect and later revoke any suspicious nodes by employing trusted computing techniques.

This research aims to provide a unified and dynamic approach while considering several trust dimensions (history, recommendation and context), and attesting the communicating devices. A dynamic model of trust will provide the ability to autonomously detect alteration in behaviour of the neighbouring nodes and dynamically update their trust levels accordingly.

1.3 Research Objectives

Based on the problem statement the research objectives of this research are as follows:

(a) To design a unified multi-dimensional trust model to increase accuracy of trust computation mechanism.

(b) To design a trust evaluation method to improve trustworthiness of the new nodes.

In order to achieve the above objectives, we need to formulate components of the proposed trust model and describe them mathematically and then develop a trust evaluation mechanism to measure accuracy of the proposed trust model in pervasive computing.

1.4 Scope of the Study

This research focuses solely on trust models and other security functions such as privacy and availability are out of the research scope. This research assumes that all context information has been extracted before, thus context information gathering techniques are not within the scope of this study. Also, network limitations like bandwidth or network transmitting quality are not considered in this work.

1.5 Significance of the Study

Because of following visions in pervasive computing, trust has an outstanding role as compared to traditional computing (Langheinrich, 2003; Trcek, 2011):

(c) Highly decentralized networks communicating on shared channels,

(d) Expected to operate in a non-intrusive way, freeing the user from such dull things as usernames and passwords.

Trust is used in pervasive computing as a prerequisite to automate cooperation and transferring information between the pervasive entities. The vision of pervasive computing will not become reality if the security issues are not addressed. So pervasive computing environments require security architecture based on trust rather than just user authentication and access control.

1.6 Thesis Organization

The thesis discusses the design and evaluation of a trust model for pervasive computing environment by leveraging trusted computing technology. The main aim is to present the theoretical background for understanding the area of trust and trusted computing and at the same time to provide all the necessary details for designing and evaluating a novel model for tackling the current limitations and weaknesses.

Chapter 1 demarcates the reason and aim of the study besides introducing the research topic and touching on the concepts. Furthermore, it describes the scope of this study and its significance. Chapter 2 covers the extensive literature review and discusses background information and related work on trust models and trusted computing to-date. It deepens the understanding of the concepts introduced in Chapter 1 and describes additional notions that are used throughout the thesis. The philosophical perspective of the research and view of the methods that are applied in this research are provided in Chapter 3. Chapter 4 explains the research approach and introduces the proposed solution to the research problem and define the model parameters and properties. It also defines the proposed model, called Unified Trust Model in details and provides the model formula and calculation mechanism. Chapter 5 presents a simulation-based analysis and evaluation of the trust model proposed in the preceding chapter. In particular, we investigate which conditions affect the trust calculation mechanism and how much the model is able to deal with different scenarios. Chapter 6 presents a case study. It describes the application of Unified Trust Model to Wireless Sensor Networks, and discusses the simulation scenarios and presents the results. Chapter 7 concludes the thesis and reflects the results in summary and suggests directions for future research.

REFERENCES

Akyildiz, I.F., Su, W., Sankarasubramaniam, Y., Cayirci, E. (2002). Wireless sensor networks: a survey. *Computer Networks*. 38(4), 393–422.

Alam, M., Zhang, X., Nauman, M., Ali, T., Seifert, J.-P. (2008). Model-based behavioral attestation. In *Proceedings of the 13th ACM symposium on Access control models and technologies*. SACMAT ’08. New York, NY, USA: ACM, 175–184.

Anon (2001). *NSF-01-160, NSF:CISE-Trusted Computing*. National Science Foundation.

Anon (2009). TCG Mobile Phone Work Group Selected Use Case Analyses – v 1.0.

Anon (2005). TCG Mobile Phone Work Group Use Case Scenarios – v 2.7.

Anon (2008a). TCG Mobile Reference Architecture - version 1.0 - Revision 5.

Anon (2008b). TCG Mobile Trusted Module Specification - version 1.0 - Revision 6.

Anon (2007). TCG Mobile Trusted Module Specification FAQ - Technical Overview.

Becher, A., Benenson, Z., Dornseif, M. (2006). Tampering with Motes: Real-World Physical Attacks on Wireless Sensor Networks. In J. Clark, R. Paige, F. Polack, & P. Brooke, eds. *Security in Pervasive Computing*. Lecture Notes in Computer Science. Springer Berlin / Heidelberg, 104–118.

Bella, G., Librizzi, F., Riccobene, S. (2008). A privacy paradigm that tradeoffs anonymity and trust. In *16th International Conference on Software, Telecommunications and Computer Networks (SoftCOM 2008)*. 16th International Conference on Software, Telecommunications and Computer Networks (SoftCOM 2008). 384–388.

Biancalana, C., Profiti, F. (2008). Security and privacy preserving data in eGovernment integration. In *Proceedings of the Second European Summit on Interoperability in the iGovernment.* ESIIG2. Rome, 31-38.

Blaze, M., Feigenbaum, J., Lacy, J. (1996). Decentralized Trust Management. In *Proceedings of the IEEE Symposium on Security and Privacy*. IEEE Symposium on Security and Privacy. 164–173.

Böttcher, A., Kauer, B., Härtig, H. (2008). Trusted Computing Serving an Anonymity Service. In *Trusted Computing - Challenges and Applications*. 143–154.

Brickell, E., Camenisch, J., Chen, L. (2004). Direct anonymous attestation. In *Proceedings of the 11th ACM conference on Computer and communications security*. CCS ’04. New York, NY, USA: ACM, 132–145.

Brickell, E., Chen, L., Li, J. (2008). A New Direct Anonymous Attestation Scheme from Bilinear Maps. In *Proceedings of the 1st international conference on Trusted Computing and Trust in Information Technologies: Trusted Computing - Challenges and Applications*. Trust ’08. Berlin, Heidelberg: Springer-Verlag, 166–178.

Brumitt, B., Meyers, B., Krumm, J., Kern, A., Shafer, S. (2000). EasyLiving: Technologies for Intelligent Environments. In *Handheld and Ubiquitous Computing*. 97–119.

Campbell, R., Al-Muhtadi, J., Naldurg, P., Sampemane, G., Dennis Mickunas, M. (2003). Towards Security and Privacy for Pervasive Computing. In *Software Security — Theories and Systems (LNCS 2609)*. Lecture Notes in Computer Science. Springer Berlin / Heidelberg, 77–82.

Carminati, B., Ferrari, E. (2005). Trusted Privacy Manager: A System for Privacy Enforcement. In *Proceedings of the 21st International Conference on Data Engineering Workshops*. IEEE Computer Society, 1195-1195.

Carnegie Mellon University (2000). Project Aura. [online]. Available from: http://www.cs.cmu.edu/~aura/ [Accessed July 28, 2009].

Castelluccia, C., Francillon, A., Perito, D., Soriente, C. (2009). On the Difficulty of Software-Based Attestation of Embedded Devices. In *Proceedings of the 16th ACM conference on Computer and communications security*. CCS ’09. New York, NY, USA: ACM, 400–409.

Challener, D., Yoder, K., Catherman, R., Safford, D., Doorn, L.V. (2008). *A Practical Guide to Trusted Computing*. 1st ed. IBM Press.

Chen, L., Landfermann, R., Löhr, H., Rohe, M., Sadeghi, A.-R., Stüble, C. (2006). A protocol for property-based attestation. In *Proceedings of the first ACM* *workshop on Scalable trusted computing*. STC ’06. New York, NY, USA: ACM, 7–16.

Chen, L., Löhr, H., Manulis, M., Sadeghi, A.-R. (2008). Property-Based Attestation without a Trusted Third Party. In T.-C. Wu, C.-L. Lei, V. Rijmen, & D.-T. Lee, eds. *Information Security*. Berlin, Heidelberg: Springer Berlin Heidelberg, 31–46.

Chen, X., Makki, K., Yen, K., Pissinou, N. (2009). Sensor Network Security: A Survey. *IEEE Communications Surveys & Tutorials*. 11(2), 52 –73.

Choi, Y.-G., Kang, J., Nyang, D. (2007). Proactive Code Verification Protocol in Wireless Sensor Network. In *Proceedings of the 2007 international conference on Computational science and Its applications*. ICCSA’07. Berlin, Heidelberg: Springer-Verlag, 1085–1096.

Demeyer, S. (2011). Research Methods in Computer Science. In *27th IEEE International Conference on Software Maintenance (ICSM)*. 27th IEEE International Conference on Software Maintenance (ICSM). 600-600.

Dietrich, K. (2007). An integrated architecture for trusted computing for java enabled embedded devices. In *Proceedings of the 2007 ACM workshop on Scalable trusted computing*. Alexandria, Virginia, USA: ACM, 2–6.

Dooley, K. (2005). Simulation Research Methods. In J. Baum, ed. *Companion to Organizations*. London: Wiley-Blackwell, 829–848.

Ducatel, K., Bogdanowicz, M., Scapolo, F., Leijten, J., Burgelman, J. (2001). *Scenarios for Ambient Intelligence in 2010*. IPTS-Seville.

Ekberg, J.E., Kylanpaa, M. (2007). *Mobile Trusted Module (MTM) - an introduction*. Helsinki, Finland: Nokia Research Center.

El Defrawy, K., Francillon, A., Perito, D., Tsudik, G. (2012). SMART: Secure and Minimal Architecture for (Establishing a Dynamic) Root of Trust. In *Proceedings of the Network and Distributed System Security Symposium, NDSS 2012, San Diego*.

Erika McCallister, Tim Grance, Karen Scarfone (2010). NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information.

Feller, T., Malipatlolla, S., Meister, D., Huss, S.A. (2011). TinyTPM: A lightweight module aimed to IP protection and trusted embedded platforms. In *Proceedings of the IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*. 6 –11.

Ganeriwal, S., Balzano, L.K., Srivastava, M.B. (2008). Reputation-Based Framework for High Integrity Sensor Networks. *ACM Transactions on Sensor Networks*. 4(3), 15:1–15:37.

Ge, H., Tate, S.R. (2007). A Direct Anonymous Attestation Scheme for Embedded Devices. In *Proceedings of the 10th international conference on Practice and theory in public-key cryptography*. PKC'07. Berlin, Heidelberg: Springer-Verlag, 16–30.

Giang, P.D., Hung, L.X., Shaikh, R.A., Zhung, Y., Lee, S. (2007). A Trust-Based Approach to Control Privacy Exposure in Ubiquitous Computing Environments. In *Proceedings of IEEE International Conference on Pervasive Services*. IEEE International Conference on Pervasive Services. 149–152.

Glass, R.L., Ramesh, V., Vessey, I. (2004). An analysis of research in computing disciplines. *Communications of the ACM*. 47(6), 89–94.

Gómez Mármol, F. (2012a). *TRMSim-WSN*.

Gómez Mármol, F. (2012b). TRMSim-WSN - Trust and Reputation Models Simulator for Wireless Sensor Networks. [online]. Available from: http://ants.dif.um.es/~felixgm/research/trmsim-wsn/ [Accessed January 21, 2012].

Gómez Mármol, F., Martínez Pérez, G. (2010a). Providing trust in wireless sensor networks using a bio-inspired technique. *Telecommunication Systems*. 46(2), 163–180.

Gómez Mármol, F., Martínez Pérez, G. (2010b). Towards pre-standardization of trust and reputation models for distributed and heterogeneous systems. *Computer Standards & Interfaces*. 32(4), 185–196.

Gómez Mármol, F., Martínez Pérez, G. (2009). TRMSim-WSN, Trust and Reputation Models Simulator for Wireless Sensor Networks. In *IEEE International Conference on Communications (ICC '09)*. IEEE International Conference on Communications (ICC '09). IEEE, 1–5.

Gu, L., Ding, X., Deng, R.H., Xie, B., Mei, H. (2008). Remote attestation on program execution. In *Proceedings of the 3rd ACM workshop on Scalable trusted computing*. STC '08. New York, NY, USA: ACM, 11–20.

Haldar, V., Chandra, D., Franz, M. (2004). Semantic remote attestation: a virtual machine directed approach to trusted computing. In *Proceedings of the 3rd* *conference on Virtual Machine Research And Technology Symposium - Volume 3*. Berkeley, CA, USA: USENIX Association, 3–3.

Haque, M., Ahamed, S.I. (2006). Security in Pervasive Computing: Current Status and Open Issues. *International Journal of Network Security*. 3(3), 203–214.

Haque, M.M., Ahamed, S.I. (2007). An Omnipresent Formal Trust Model (FTM) for Pervasive Computing Environment. In *Proceedings of the 31st Annual International Computer Software and Applications Conference*. COMPSAC 2007. IEEE Computer Society, 49–56.

Hengartner, U. (2008). Location privacy based on trusted computing and secure logging. In *Proceedings of the 4th international conference on Security and privacy in communication netowrks*. Istanbul, Turkey: ACM, 1–8.

Holtmanns, S., Yan, Z. (2006). Context-Aware Adaptive Trust. In *Developing Ambient Intelligence*. Springer Paris, 137–146.

Hu, W., Tan, H., Corke, P., Shih, W.C., Jha, S. (2010). Toward Trusted Wireless Sensor Networks. *ACM Transactions on Sensor Networks*. 7(1), 5:1–5:25.

Hutter, D., Stephan, W., Ullmann, M. (2004). Security and Privacy in Pervasive Computing State of the Art and Future Directions. In *Security in Pervasive Computing (LNCS 2802)*. Lecture Notes in Computer Science. Springer Berlin / Heidelberg, 285–289.

Jaeger, T., Sailer, R., Shankar, U. (2006). PRIMA: policy-reduced integrity measurement architecture. In *Proceedings of the eleventh ACM symposium on Access control models and technologies*. SACMAT ’06. New York, NY, USA: ACM, 19–28.

Jøsang, A. (1999). An Algebra for Assessing Trust in Certification Chains. In *Proceedings of the Network and Distributed Systems Security Symposium NDSS’99*. Network and Distributed Systems Security Symposium NDSS’99.

Jøsang, A., Ismail, R., Boyd, C. (2007). A survey of trust and reputation systems for online service provision. *Decision Support Systems*. 43(2), 618–644.

Kagal, L., Finin, T., Joshi, A. (2001). Trust-Based Security in Pervasive Computing Environments. *Computer*. 34(12), 154–157.

Kamat, P., Zhang, Y., Trappe, W., Ozturk, C. (2005). Enhancing Source-Location Privacy in Sensor Network Routing. In *Proceedings of the 25th IEEE International Conference on Distributed Computing Systems*. ICDCS ’05. Washington, DC, USA: IEEE Computer Society, 599–608.

Kamvar, S.D., Schlosser, M.T., Garcia-Molina, H. (2003). The EigenTrust Algorithm for Reputation Management in P2P Networks. In *Proceedings of the 12th international conference on World Wide Web*. WWW '03. New York, NY, USA: ACM, 640–651.

Krauß, C., Stumpf, F., Eckert, C. (2007). Detecting node compromise in hybrid wireless sensor networks using attestation techniques. In *Proceedings of the 4th European conference on Security and privacy in ad-hoc and sensor networks*. ESAS'07. Berlin, Heidelberg: Springer-Verlag, 203–217.

Lahlou, S., Langheinrich, M., Röcker, C. (2005). Privacy and trust issues with invisible computers. *Communications of the ACM*. 48(3), 59–60.

Langheinrich, M. (2001). Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems. In *Proceedings of the 3rd international conference on Ubiquitous Computing*. Atlanta, Georgia, USA: Springer-Verlag, 273–291.

Langheinrich, M. (2003). When Trust Does Not Compute - The Role of Trust in Ubiquitous Computing. In *Proceedings of Privacy Workshops of Ubicomp'03*. Ubicomp'03. 1-8.

Lázaro, M., Marcos, E. (2005). Research in Software Engineering: Paradigms and Methods. In *Proceedings of the 17th International Conference on Advanced Information Systems Engineering (CAiSE 2005)*. CAiSE'05. Porto, Portugal, 517–522.

Liu, Z., Joy, A.W., Thompson, R.A. (2004). A Dynamic Trust Model for Mobile Ad Hoc Networks. In *Proceedings of the 10th IEEE International Workshop on Future Trends of Distributed Computing Systems FTDCS 2004*. 10th IEEE International Workshop on Future Trends of Distributed Computing Systems FTDCS 2004. 80–85.

Maria, A. (1997). Introduction to Modeling and Simulation. In *Proceedings of the 29th conference on Winter simulation*. WSC '97. Washington, DC, USA: IEEE Computer Society, 7–13.

Mármol, F.G., Pérez, G.M. (2011). Trust and Reputation Models Comparison. *Internet Research*. 21(2), 138–153.

Martin, A. (2008). The ten-page introduction to Trusted Computing.

Mateus, P., Vaudenay, S. (2009). On Privacy Losses in the Trusted Agent Model. In *Workshop on Cryptographic Hardware and Embedded Systems (CHES'09)*. Workshop on Cryptographic Hardware and Embedded Systems (CHES'09).

MathWorks (2011). *MATLAB®*. The MathWorks, Inc.

Maurer, U.M. (1996). Modelling a Public-Key Infrastructure. In *Proceedings of the 4th European Symposium on Research in Computer Security: Computer Security*. Springer-Verlag, 325–350.

Mhatre, V., Rosenberg, C. (2004). Homogeneous vs Heterogeneous Clustered Sensor Networks: A Comparative Study. In *2004 IEEE International Conference on Communications*. 2004 IEEE International Conference on Communications. 3646–3651 Vol.6.

MIT Computer Science and Artificial Intelligence Laboratory (1999). Project Oxygen. [online]. Available from: http://www.oxygen.lcs.mit.edu/ [Accessed July 22, 2009].

Moteiv Corporation (2006). Tmote Sky Datasheet: Ultra Low Power IEEE 802.15.4 Compliant Wireless Sensor Module.

Nguyen, C.T., Camp, O. (2008). Using Context Information to Improve Computation of Trust in Ad Hoc Networks. In *Proceedings of the 2008 IEEE International Conference on Wireless & Mobile Computing, Networking & Communication*. WIMOB '08. 619–624.

Nguyen, C.T., Camp, O., Loiseau, S. (2007). A Bayesian network based trust model for improving collaboration in mobile ad hoc networks. In *Proceedings of the 2007 IEEE International Conference on Research, Innovation and Vision for the Future*. 2007 IEEE International Conference on Research, Innovation and Vision for the Future. 144–151.

OpenTC (2011). Open Trusted Computing. [online]. Available from: http://www.opentc.net.

Oracle (2012). *NetBeans IDE*. Oracle Corporation.

Park, T., Shin, K.G. (2005). Soft Tamper-Proofing via Program Integrity Verification in Wireless Sensor Networks. *IEEE Transactions on Mobile Computing*. 4(3), 297–309.

Pearson, S. (2005a). How Trusted Computers can Enhance for Privacy Preserving Mobile Applications. In *Proceedings of the First International IEEE WoWMoM Workshop on Trust, Security and Privacy for Ubiquitous Computing*. IEEE Computer Society, 609–613.

Pearson, S. (2005b). Trusted Computing: Strengths, Weaknesses and Further Opportunities for Enhancing Privacy. In *Trust Management*. 305–320.

Pearson, S., Casassa-Mont, M. (2006). A System for Privacy-Aware Resource Allocation and Data Processing in Dynamic Environments. In *Security and Privacy in Dynamic Environments*. 471–482.

Perrig, A., Stankovic, J., Wagner, D. (2004). Security in Wireless Sensor Networks. *Communications of the ACM*. 47(6), 53–57.

Polastre, J., Szewczyk, R., Culler, D. (2005). Telos: Enabling Ultra-Low Power Wireless Research. In *Proceedings of the 4th international symposium on Information processing in sensor networks*. IPSN ’05. Piscataway, NJ, USA: IEEE Press.

Poritz, J.A. (2006). Trust[ed , in] computing, signed code and the heat death of the internet. In *Proceedings of the 2006 ACM symposium on Applied computing*. SAC ’06. New York, NY, USA: ACM, 1855–1859.

Ranganathan, K. (2004). Trustworthy Pervasive Computing: The Hard Security Problems. In *Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops*. Second IEEE Annual Conference on Pervasive Computing and Communications Workshops. IEEE Computer Society, 117–121.

Raymond Pearl (1924). The Curve of Population Growth. In *Proceedings of the American Philosophical Society*. American Philosophical Society, 10–17.

Reiter, M.K., Stubblebine, S.G. (1998). Resilient Authentication Using Path Independence. *IEEE Transactions on Computers*. 47(12), 1351–1362.

Sabater, J., Sierra, C. (2005). Review on Computational Trust and Reputation Models. *Artificial Intelligence Review*. 24(1), 33–60.

Sadeghi, A.-R. (2008). Trusted Computing — Special Aspects and Challenges. In *SOFSEM 2008: Theory and Practice of Computer Science (LNCS 4910)*. Lecture Notes in Computer Science. Springer Berlin / Heidelberg, 98–117.

Sadeghi, A.-R., Stüble, C. (2004). Property-based attestation for computing platforms: caring about properties, not mechanisms. In *Proceedings of the 2004 workshop on New security paradigms*. NSPW ’04. New York, NY, USA: ACM, 67–77.

Saha, D., Mukherjee, A. (2003). Pervasive Computing: A Paradigm for the 21st Century. *IEEE Computer*. 36(3), 25–31.

Sailer, R., Zhang, X., Jaeger, T., van Doorn, L. (2004). Design and implementation of a TCG-based integrity measurement architecture. In *Proceedings of the 13th* *conference on USENIX Security Symposium - Volume 13*. SSYM’04. Berkeley, CA, USA: USENIX Association, 16–16.

Sarkio, K., Holtmanns, S. (2007). Tailored trustworthiness estimations in Peer-to-Peer networks. *International Journal of Internet Technology and Secured Transactions*. 1(1/2), 95 – 107.

Satyanarayanan, M. (2001). Pervasive computing: vision and challenges. *Personal Communications, IEEE*. 8(4), 10–17.

Schunter, M., Waidner, M. (2007). Simplified Privacy Controls for Aggregated Services — Suspend and Resume of Personal Data. In *Privacy Enhancing Technologies*. 218–232.

Seshadri, A., Luk, M., Perrig, A. (2008). SAKE: Software Attestation for Key Establishment in Sensor Networks. In *Proceedings of the 4th IEEE international conference on Distributed Computing in Sensor Systems*. DCOSS ’08. Berlin, Heidelberg: Springer-Verlag, 372–385.

Seshadri, A., Luk, M., Perrig, A., van Doorn, L., Khosla, P. (2006). SCUBA: Secure Code Update By Attestation in sensor networks. In *Proceedings of the 5th ACM workshop on Wireless security*. WiSe ’06. New York, NY, USA: ACM, 85–94.

Seshadri, A., Perrig, A., van Doorn, L., Khosla, P. (2004). SWATT: SoftWare-based ATTestation for Embedded Devices. In *Proceedings of the 2004 IEEE Symposium on Security and Privacy*. 2004 IEEE Symposium on Security and Privacy. IEEE, 272– 282.

Shaneck, M., Mahadevan, K., Kher, V., Kim, Y. (2005). Remote Software-based Attestation for Wireless Sensors. In *Proceedings of the Second European conference on Security and Privacy in Ad-Hoc and Sensor Networks*. ESAS’05. Berlin, Heidelberg: Springer-Verlag, 27–41.

Shirey, R. (2000). RFC2828 - Internet Security Glossary.

Sikka, P., Corke, P., Overs, L. (2004). Wireless Sensor Devices for Animal Tracking and Control. In *Proceedings of the 29th Annual IEEE International Conference on Local Computer Networks*. LCN ’04. Washington, DC, USA: IEEE Computer Society, 446–454.

Stajano, F. (2002). *Security for Ubiquitous Computing*. West Sussex, England: J. Wiley & Sons.

Sun, T., Denko, M.K. (2008). Performance Evaluation of Trust Management in Pervasive Computing. In *Proceedings of the 22nd International Conference on*

Advanced Information Networking and Applications. Advanced Information Networking and Applications, 2008. AINA 2008. IEEE Computer Society, 386–394.

Sun, Y.L., Han, Z., Yu, W., Liu, K.J.R. (2006). A Trust Evaluation Framework in Distributed Networks: Vulnerability Analysis and Defense Against Attacks. In *Proceedings of 25th IEEE International Conference on Computer Communications INFOCOM 2006*. INFOCOM 2006. Barcelona, Spain, 1–13.

Sun, Y.L., Yu, W., Han, Z., Liu, K.J.R. (2006). Information theoretic framework of trust modeling and evaluation for ad hoc networks. *IEEE Journal on Selected Areas in Communications*. 24(2), 305–317.

Suriadi, S., Ouyang, C., Smith, J., Foo, E. (2009). Modeling and verification of privacy enhancing security protocols. [online]. Available from: http://eprints.qut.edu.au/20088/ [Accessed September 30, 2009].

Tan, H., Hu, W., Jha, S. (2011). A TPM-enabled remote attestation protocol (TRAP) in wireless sensor networks. In *Proceedings of the 6th ACM workshop on Performance monitoring and measurement of heterogeneous wireless and wired networks*. PM2HW2N ’11. New York, NY, USA: ACM, 9–16.

Tan, Y.-H., Thoen, W. (2000). Toward a Generic Model of Trust for Electronic Commerce. *International Journal of Electronic Commerce*. 5(2), 61–74.

TCG (2011a). *TPM Main - Part 1 Design Principles, Version 1.2, Revision 116*. Trusted Computing Group.

TCG (2011b). Trusted Computing Group. [online]. Available from: http://www.trustedcomputinggroup.org/ [Accessed December 7, 2011].

TCG (2011c). Trusted Computing Group - Developers - Glossary. [online]. Available from: http://www.trustedcomputinggroup.org/developers/glossary/ [Accessed December 2, 2011].

TCG (2011d). Trusted Computing Group - Trusted Platform Module. [online]. Available from: http://www.trustedcomputinggroup.org/developers/trusted_platform_module [Accessed December 7, 2011].

Theodorakopoulos, G., Baras, J.S. (2006). On Trust Models and Trust Evaluation Metrics for Ad Hoc Networks. *IEEE Journal on Selected Areas in Communications*. 24(2), 318–328.

Toahchoodee, M., Abdunabi, R., Ray, Indrakshi, Ray, Indrajit (2009). A Trust-Based Access Control Model for Pervasive Computing Applications. In *Proceedings of the 23rd Annual IFIP WG 11.3 Working Conference on Data and Applications Security XXIII*. Montreal, P.Q., Canada: Springer-Verlag, 307–314.

Trcek, D. (2011). Trust Management in the Pervasive Computing Era. *IEEE Security and Privacy*. 9(4), 52–55.

Tripathi, A., Ahmed, T., Kulkarni, D., Kumar, R., Kashiramka, K. (2004). Context-Based Secure Resource Access in Pervasive Computing Environments. In *Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops*. IEEE Computer Society, 159–163.

University Of Illinois Department of Computer Science (2000). Project Gaia. [online]. Available from: http://gaia.cs.uiuc.edu/ [Accessed July 28, 2009].

Wang, Y., Varadharajan, V. (2005). Trust2: Developing Trust in Peer-to-Peer Environments. In *Proceedings of the 2005 IEEE International Conference on Services Computing - Volume 01*. IEEE Computer Society, 24–34.

Weiser, M. (1991). The computer for the 21st century. *Scientific American*. 265(3), 75–66.

Weiser, M. (1999). The computer for the 21st century. *SIGMOBILE Mobile Computing and Communications Review*. 3(3), 3–11.

Winter, J. (2008). Trusted computing building blocks for embedded linux-based ARM trustzone platforms. In *Proceedings of the 3rd ACM workshop on Scalable trusted computing*. Alexandria, Virginia, USA: ACM, 21–30.

Xiong, L., Liu, L. (2004). PeerTrust: Supporting Reputation-Based Trust for Peer-to-Peer Electronic Communities. *IEEE Transactions on Knowledge and Data Engineering*. 16(7), 843–857.

Yan, Z. (2006). A Conceptual Architecture of a Trusted Mobile Environment. In *Second International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing, SecPerU 2006*. SecPerU 2006. Lyon: IEEE Computer Society, 75–81.

Yan, Z., Holtmanns, S. (2008). Trust Modeling and Management: from Social Trust to Digital Trust. In *Computer Security, Privacy and Politics: Current Issues, Challenges and Solutions*. IGI Global, 290–323.

Yan, Z., MacLaverty, R. (2006). Autonomic Trust Management in a Component Based Software System. In *Autonomic and Trusted Computing*. Lecture Notes in Computer Science. Springer Berlin / Heidelberg, 279–292.

Yang, Y., Wang, X., Zhu, S., Cao, G. (2007). Distributed Software-based Attestation for Node Compromise Detection in Sensor Networks. In *Proceedings of the 26th IEEE International Symposium on Reliable Distributed Systems*. SRDS ’07. Washington, DC, USA: IEEE Computer Society, 219–230.

Yang, Y., Zhou, J., Deng, R.H., Bao, F. (2011). Better security enforcement in trusted computing enabled heterogeneous wireless sensor networks. *Security and Communication Networks*. 4(1), 11–22.

Zahariadis, T., Leligou, H.C., Trakadas, P., Voliotis, S. (2010). Trust Management in Wireless Sensor Networks. *European Transactions on Telecommunications*. 21(4), 386–395.

Zhang, X., Acıiçmez, O., Seifert, J.-P. (2007). A trusted mobile phone reference architecturevia secure kernel. In *Proceedings of the 2007 ACM workshop on Scalable trusted computing*. Alexandria, Virginia, USA: ACM, 7–14.

Zhou, M., Mei, H., Zhang, L. (2005). A Multi-Property Trust Model for Reconfiguring Component Software. In *Proceedings of the Fifth International Conference on Quality Software*. IEEE Computer Society, 142–149.

Zhou, R., Hwang, K. (2007). PowerTrust: A Robust and Scalable Reputation System for Trusted Peer-to-Peer Computing. *IEEE Trans. Parallel Distrib. Syst.* 18(4), 460–473.