References

1. http://www.ebay.com
2. http://www.paypal.com
3. http://www.ipswitch.com/Products/WhatsUp/
4. http://www.gnutella.com
5. http://freenet.sourceforge.net
6. http://www.jxta.org
7. http://www.gnunet.org
8. Arma international. http://www.arma.org
9. Bbb dispute resolution. http://www.dr.bbb.org
10. e-Government eEurope 2005.
11. i2010 initiative. http://ec.europa.eu/information_society/eeurope/i2010/index_en.htm
12. JSR 219: Foundation Profile 1.1. http://jcp.org/en/jsr/detail?id=219
13. kXML. http://kxml.sourceforge.net
14. Ltans-charter. URL `http://www.ietf.org/html.charters/`
15. Mobile Information Device Profile. http://java.sun.com/products/midp/
16. Statistical office of the european communities. http://epp.eurostat.ec.europa.eu/
17. The Legion of the Bouncy Castle. http://www.bouncycastle.org
18. The us national archives electronic records archives (era). http://www.archives.gov/era
19. 3-D Secure Team: 3-D Secure impementation Guide. Visa Internatitonal Service Association, 1.0.2 edn. (2004)
20. Adar, E., Huberman, B.: Free riding on gnutella (2000). URL `citeseer.nj.nec.com/adar00free.html`
21. Anantharaman, L., Bao, F.: An efficient and practical peer-to-peer e-payment system (2002). Manuscript
22. Antoniadis, P., Courcoubetis, C.: Market models for P2P content distribution. In: AP2PC'02 (2002)
23. Asokan, N.: Fairness in electronic commerce. Ph.D. thesis, University of Waterloo, Computer Science (1998)
24. Asokan, N., Baum-Waidner, B., Schunter, M., Waidner, M.: Optimistic synchronous multi-party contract signing. Tech. Rep. RZ 3089, IBM Zurich Research Lab (1998)
25. Asokan, N., Janson, P.A., Steiner, M., Waidner, M.: The state of the art in electronic payment systems. IEEE Computer **30**(9), 28–35 (1997)
26. Asokan, N., Schunter, M., Waidner, M.: Optimistic protocols for multi-party fair exchange. Tech. Rep. RZ 2892 (# 90840), IBM, Zurich Research Laboratory (1996)
27. Asokan, N., Schunter, M., Waidner, M.: Optimistic protocols for fair exchange. In: Proceedings of the 4th ACM Conference on Computer and Communications Security, pp. 7–17. ACM Press (1997). DOI http://doi.acm.org/10.1145/266420.266426

28. Asokan, N., Shoup, V., Waidner, M.: Optimistic fair exchange of digital signatures. IEEE J. Sel. Area. Comm. **18**(4), 593–610 (2000). URL `citeseer.nj.nec.com/asokan98optimistic.html`
29. Ateniese, G., de Medeiros, B., Goodrich, M.T.: TRICERT: A distributed certified E-mail scheme. In: Network and Distributed System Security Symposium Conference Proceedings (2001)
30. Banks, J., Carson, J., Nelson, B., D.Nicol: Discrete-event system simulation. Prentice Hall (2000)
31. Bao, F., Deng, R., Mao, W.: Efficient and practical fair exchange protocols with off-line ttp. In: IEEE Symposium on Security and Privacy, pp. 77–85. IEEE (1998)
32. Bao, F., Deng, R., Nguyen, K., Varadharajan, V.: Multi-party fair exchange with an off-line trusted neutral party. In: Database and Expert Systems Applications, 1999. Proceedings. Tenth International Workshop on, pp. 858–862 (1999)
33. Bao, F., Deng, R., Zhou, J.: Electronic payment systems with fair on-line verification. In: IFIP TC11 16th Annual Working Conference on Information Security: Information Security for Global Information Infrastructures, pp. 451 – 460. IFIP TC11, Kluwer Academic Publishers (2000)
34. Baum-Waidner, B.: Optimistic asynchronous multi-party contract signing with reduced number of rounds. In: F. Orejas, P. Spirakis, J.V. Leeuwen (eds.) Automata, Languages and Programming, pp. 898–911. 28th International Colloquium, ICALP 2001, Springer-Verlag (2001)
35. Baum-Waidner, B., Waidner, M.: Optimistic asynchronous multi-party contract signing. Tech. Rep. RZ 3078, IBM Zurich Research Lab (1998)
36. Baum-Waidner, B., Waidner, M.: Round-optimal and abuse-free multi-party contract signing. In: 27th International Colloquium on Automata, Languages and Programming, *LNCS*, vol. 1853, pp. 524–535. Springer (2000)
37. Ben-Or, M., Goldreich, O., Micali, S., Rivest, R.: A fair protocol for signing contracts. In: IEEE Transactions on Information Theory, vol. 36, pp. 40–46 (1990)
38. Blum, M.: Three applications of the oblivious transfer: Part i: Coin flipping by telephone; part ii: How to exchange secrets; part iii: How to send certified electronic mail. Tech. rep., Department of EECS, University of California (1981)
39. Boly, J.P., Bosselaers, A., Cramer, R., Michelsen, R., Mjolsnes, S.F., Muller, F., Pedersen, T.P., Pfitzmann, B., de Rooij, P., Schoenmakers, B., Schunter, M., Vallee, L., Waidner, M.: The ESPRIT project CAFE - high security digital payment systems. In: ESORICS, pp. 217–230 (1994)
40. Bradner, S.: Rfc 2119. key words for use in rfcs to indicate requirement levels (1997)
41. Brannigan, C.: Beyond e-commerce: Expanding the potential of Online Dispute Resolution. Interaction **16**(4), 15–17 (2004)
42. Carbonell, M., Onieva, J.A., Lopez, J., Zhou, J.: Timeout estimation using a simulation model for non-repudiation protocols. In: Fourth International Conference on Computational Science and Its Applications ICCSA, *LNCS*, vol. 3043, pp. 903–914. Springer (2004)
43. Chadha, R., Kremer, S., Scedrov, A.: Formal analysis of multi-party contract signing. In: Proceedings of the 17th IEEE Computer Security Foundations Workshop (CSFW'04), pp. 266–279. IEEE Computer Society Press (2004)
44. Cheng, J.S., Wei, V.K.: Defenses against the truncation of computation results of free-roaming agents. In: Fourth International Conference on Information and Communications Security, *LNCS*, vol. 2513, pp. 1–12 (2002)
45. Chiou, G., Chen, W.: Secure broadcasting using the secure lock. IEEE Transaction on Software Engineering **15**(8), 929–934 (1989)
46. Damiani, E., Vimercati, S.C.D., Paraboschi, S., Samarati, P., Violante, F.: A reputation-based approach for choosing reliable resources in peer-to-peer networks. In: V. Atluri (ed.) Computer and Commmunications Security, pp. 207–216. ACM (2002)
47. DeMillo, R.A., Merritt, M.: Protocols for data security. IEEE Computer **16**, 39–50 (1983)

48. Dumortier, J., Kelm, S., Nilsson, H., Skouma, G., Eecke, P.V.: The legal and market aspects of electronic signatures. Study for the european comission - dg information society, Interdisciplinary centre for Law & Information Technology, Leuven Universiteit (2003)
49. E-Arbitration-T: Online arbitration: What technology can do for arbitral institutions. Seminar (2003)
50. ElGamal, T.: A public-key cryptosystem and a signature scheme based on discrete logarithms. In: IEEE Transactions on Information Theory, vol. IT-31, pp. 469–472 (1985)
51. Eschenauer, L., Gligor, V.D., Baras, J.: On trust establishment in mobile ad-hoc networks (2002). Submitted for publication 2002
52. EU Information Society: DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (1999)
53. Even, S., Goldreich, O., Lempel, A.: A randomized protocol for signing contracts. In: Communications of the ACM, vol. 28, pp. 637–647 (1985)
54. Ezhilchelvan, P., Shrivastava, S.: A family of trusted third party based fair-exchange protocols. IEEE T. Depend. Secure. **2**(4), 273–286 (2005)
55. Federal Information, N.B.o.S.: Data encryption standard (des). Tech. Rep. fips-46-3, NIST (1999)
56. Federal Information, N.B.o.S.: Advanced encryption standard (aes). Tech. Rep. fips-197, NIST (2001)
57. Ferrer-Gomila, J.L., Payeras-Capellà, M., Huguet-Rotger, L.: Efficient optimistic n-party contract signing protocol. In: Proceedings of the 4th International Conference on Information Security, pp. 394–407. Springer-Verlag (2001)
58. Ferrer-Gomila, J.L., Payeras-Capellà, M., Huguet-Rotger, L.: A realistic protocol for multiparty certified electronic mail. In: Information Security ISC 2002, *LNCS*, vol. 2433, pp. 210–219 (2002)
59. Ferrer-Gomila, J.L., Payeras-Capellà, M., Huguet-Rotger, L.: Optimality in asynchronous contract signing protocols. In: 1st International Conference on Trust and Privacy in Digital Business, vol. 3184, pp. 200–208. Springer-Verlag (2004)
60. Franklin, M., Tsudik, G.: Secure group barter: Multi-party fair exchange with semi-trusted neutral parties. In: Proceedings of Financial Cryptography 1998, *Lecture Notes in Computer Science*, vol. 1465, pp. 90–102. Springer (1998)
61. Garay, J.A., MacKenzie, P.D.: Abuse-free multi-party contract signing. In: Proceedings of the 13th International Symposium on Distributed Computing, pp. 151–165. Springer-Verlag (1999)
62. Golle, P., Leyton-Brown, K., Mironov, I.: Incentives for sharing in peer-to-peer networks. In: EC '01: Proceedings of the 3rd ACM conference on Electronic Commerce, pp. 264–267. ACM Press (2001). DOI http://doi.acm.org/10.1145/501158.501193
63. Gondrom, T., Brandner, R., Pordesch, U.: Evidence Record Syntax (ERS). RFC 4998 (Proposed Standard) (2007). URL `http://www.ietf.org/rfc/rfc4998.txt`
64. González-Deleito, N.: Trust reletionships in exchange protocols. Ph.D. thesis, Faculté des Sciences, Université Libre de Bruselles (2005)
65. González-Deleito, N., Markowitch, O.: An optimistic multi-party fair exchange protocol with reduced trust requirements. In: Proceedings of the 4th International Conference on Information Security and Cryptology, *Lecture Notes in Computer Science*, vol. 2288, pp. 258–267. Springer-Verlag (2001)
66. González-Deleito, N., Markowitch, O.: Exclusion-freeness in multi-party exchange protocols. In: Lecture Notes in Computer Sciences, pp. 200–209. 5th International Conference on Information Security (ISC 2002), Springer-Verlag (2002)
67. Gullou, L.C., Quisquater, J.: A paradoxical indentity-based signature scheme resulting from zero-knowledge. In: Advances in Cryptology, *LNCS*, vol. 403, pp. 216–231. Springer (1988)
68. Gürgens, S., Rudolph, C.: Security analysis of (un-) fair non-repudiation protocols. In: Formal Aspects of Security, *LNCS*, vol. 2629, pp. 99–114. Spinger-Verlag (2002)
69. Haber, S., Kaliski, B., Stornetta, S.: How do digital time-stamps support digital signatures? Cryptobytes Newsletter **1**(3), 14–15 (1995)

70. Horne, B., Pinkas, B., Sander, T.: Escrow services and incentives in peer-to-peer networks. In: Proceedings of the 3rd ACM conference on Electronic Commerce, pp. 85–94. ACM Press (2001). DOI http://doi.acm.org/10.1145/501158.501168
71. International, M.: MasterCard SecureCode Merchant Implementation Guide. MasterCard International Incorporated (2004)
72. ISO/IEC: 1st WD 13888-2. Non-repudiation using a symmetric key algorithm. JTC1/SC27/WG2 N83 (1991)
73. ISO/IEC: DIS 10181-4. Information technology - Open systems interconnection - Security frameworks in open systems - Part 4: Non-repudiation (1996)
74. ISO/IEC: 2nd CD 13888-3. Information technology - Security techniques - Non-repudiation - Part 3: Using asymmetric techniques. JTC1/SC27 N1379 (1997)
75. ISO/IEC: 3rd CD 13888-2. Information technology - Security techniques - Non-repudiation - Part 2: Using symmetric encipherment algorithms. JTC1/SC27 N1276 (1998)
76. ISO/IEC: 13888-1. Information technology - Security techniques - Non-repudiation - Part 1: General model. JTC1/SC27 (2004)
77. ITU-T: Information technology - Open Systems Interconnection - The Directory: Overview of concepts, models and services (1997)
78. ITU-T: Security architecture for systems providing end to end communications (2003)
79. ITU-T: Security in Telecommunications and Information Technology (2006)
80. ITU-T X.509: Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks (2000)
81. ITU-T X.813: Information technology - Open Systems Interconnection - Security frameworks for open systems: Non-repudiation framework (1996)
82. Jakobsson, M.: Mini-cash: a minimalistic approach to e-commerce. In: Proceedings of PKC'99, *LNCS*, vol. 1560, pp. 122–135. Springer (1999)
83. Karjoth, G., Asokan, N., Gülcü, C.: Protecting the computation results of free-roaming agents. In: Mobile Agents, *LNCS*, vol. 1477, pp. 195–207 (1998)
84. Karjoth, G., Posegga, J.: Mobile agents and telcos' nightmares. Tech. Rep. 55(7/8):29-41, IBM (2000)
85. Ketchpel, S., Garcia-Molina, H.: Distributed commerce transactions. Tech. rep., Standford University, Computer Science Department (1997)
86. Khill I.and Kim, J., Han, I., Ryou, J.: Multi-party fair exchange protocol using ring architecture model. Computers & Security **20**(5), 422–439 (2001)
87. Kremer, S., Markowitch, O.: A multi-party non-repudiation protocol. In: Proceedings of SEC 2000: 15th International Conference on Information Security, pp. 271–280. IFIP World Computer Congress (2000)
88. Kremer, S., Markowitch, O.: Optimistic non-repudiable information exchange. In: J. Biemond, editor, 21st Symp. on Information Theory in the Benelux, pp. 139–146. Werkgemeenschap Informatie- en Communicatietheorie (2000)
89. Kremer, S., Markowitch, O.: Fair multi-party non-repudiation protocols. International Journal of Information Security **1**(4), 223 – 235 (2003)
90. Kremer, S., Markowitch, O., Zhou, J.: An intensive survey of fair non-repudiation protocols. Computer Communications **25**(17), 1606–1621 (2002)
91. Liew, C.C., Ng, W.K., Lim, E.P., Tan, B.S., Ong, K.L.: Non-repudiation in an agent-based electronic commerce system. In: Proceedings of 1999 DEXA International Workshop on Electronic Commerce and Security, pp. 864–868. Florence, Italy (1999)
92. Lindell, Y.: Composition of Secure Multi-Party Protocols. Springer (2003)
93. Lopez, J.: Diseño de una Infraestructura de Notarización para Comercio Electrónico. Ph.D. thesis, E.T.S.I. Informatica, Malaga, Spain (2000)
94. Mao, W.: Modern Cryptography: Theory and Practice. Hewlett-Packard Books (2004)
95. Markowitch, O., Gollmann, D., Kremer, S.: On fairness in exchange protocols. In: Springer-Verlag (ed.) 5th International Conference on Information Security and Cryptology, *LNCS*, vol. 2587, pp. 451–464 (2002)

96. Markowitch, O., Kremer, S.: A multi-party optimistic non-repudiation protocol. In: Proceedings of 3rd International Conference on Information Security and Cryptology, *LNCS*, vol. 2015, pp. 109–122. Springer-Verlag (2000)
97. Markowitch, O., Roggeman, Y.: Probabilistic non-repudiation without trusted third party. In: Second Workshop on Security in Communication Network 99 (1999). URL `citeseer.nj.nec.com/markowitch99probabilistic.html`
98. Markowitch, O., Saeednia, S.: Optimistic fair-exchange with transparent signature recovery. In: Proceedings of Financial Cryptography 2001, *LNCS*, vol. 2339, pp. 339–350. Springer-Verlag (2001)
99. Massias, H., Quisquater, J.: Time and cryptography. Tech. rep., Project Timesec Digital Timestamping and the Evaluation of Security Primitives (1997)
100. Maurer, U.: New approaches to digital evidence. In: Proceedings of the IEEE, vol. 92, pp. 933–947. IEEE (2004)
101. Menezes, A.J., Oorschot, P.C.V., Vanstone, S.A.: Handbook of Applied Cryptography, 5 edn. CRC Press (1996)
102. Micali, S.: Simple and fast optimistic protocols for fair electronic exchange. In: Proceedings of the twenty-second annual symposium on Principles of distributed computing, pp. 12–19. ACM Press (2003). DOI http://doi.acm.org/10.1145/872035.872038
103. Mills, D.L.: Network time protocol (version 3) specification, implementation and analysis. Tech. Rep. RFC 1305, IETF Working Group (1992)
104. Mullen, T., Wellman, M.: The auction manager: Market middleware for large-scale electronic commerce. In: Proceedings of the 3rd USENIX Workshop on Electronic Commerce, pp. 37–48. Boston, Massachusetts (1998)
105. Onieva, J.A., Zhou, J., Lopez, J.: Practical service charge for P2P content distribution. In: Proceedings of 2003 Fifth International Conference on Information and Communications Security, *LNCS*, vol. 2836, pp. 112 – 123 (2003)
106. Onieva, J.A., Zhou, J., Lopez, J.: Non-repudiation protocols for multiple entities. Computer Communications **27**(16), 0140-3664 (2004)
107. Onieva, J.A., Zhou, J., Lopez, J.: Attacking an asynchronous multi-party contract signing protocol. In: Proceedings of 6th International Conference on Cryptology in India, *LNCS*, vol. 3797, pp. 311–321. Springer (2005)
108. Onieva, J.A., Zhou, J., Lopez, J., Carbonell, M.: Agent-mediated non-repudiation protocols. Electronic Commerce Research and Applications **3**(2), 1567-4223 (2004)
109. Open Mobile Alliance: DRM Specification, 2 edn. (2006)
110. Pancho-Festin, S., Gollmann, D.: On the formal analyses of the zhou-gollmann non-repudiation protocol. In: Formal Aspects in Security and Trust, pp. 5–15 (2005)
111. Peterson, M.: The coming archive crisis. Tech. rep., Storage Networking Industry Association (SNIA) (2006)
112. Pfitzmann, B., Schunter, M., Waidner, M.: Optimal efficiency of optimistic contract signing. In: Proceedings of the seventeenth annual ACM symposium on Principles of distributed computing, pp. 113–122. ACM Press (1998). DOI http://doi.acm.org/10.1145/277697.277717
113. Rajput, W.E.: E-Commerce Systems Architecture and Applications. Artech House (2000)
114. Rivest, R.L., Shamir, A.: Payword and micromint: Two simple micropayment schemes. In: Security Protocols Workshop, pp. 69–87 (1996)
115. Robinson, N.: Handbook of Legislative Procedures of Computer and Network Misuse in EU Countries. RAND Europe, Brussels (2003). Study for the European Commission Directorate-General Information Society (2002)
116. Roth, V.: Programming satan's agents. Electr. Notes Theor. Comput. Sci. **63**, 1–16 (2001)
117. Sander, T., Tschudin, C.F.: Protecting mobile agents against malicious hosts. In: Mobile Agents and Security, *LNCS*, vol. 1419, pp. 44–60 (1998)
118. Schneider, S.: Formal analysis of a non-repudiation protocol. In: 11th Computer Security Foundations Workshop (1998)
119. Senate, of Representatives, H.: Public law 107347dec. 17 2002 (2002)

120. Shao, M.H., Zhou, J., Wang, G.: On the security of a certified e-mail scheme with temporal authentication. In: Proceedings of 2005 ICCSA Workshop on Internet Communications Security, vol. 3482, pp. 701–710. Springer (2005)
121. Sherif, M.H.: Protocols for Secure Electronic Commerce. CRC Press (2000)
122. Smith, R.E.: Internet Cryptography. Addison-Wesley (1997)
123. Tacken, J., Flake, S., Zoth, C.: Mobile DRM in pervasive networking environments. In: Workshop on Trust and Security in Pervasive Networking, Pervasivetrust 2005, p. N.A. IEEE (2005)
124. Verhoest, P., Hawkins, R., Desruelle, P., Martinez, C., Lopez-Bassols, V., Vickery, G.: Electronic business networks: An assessment of the dynamics of b2b electronic commerce in eleven oecd countries. Tech. rep., IPTS (2003)
125. Wallace, C., Pordesch, U., Brandner, R.: Long-Term Archive Service Requirements. RFC 4810 (Informational) (2007). URL `http://www.ietf.org/rfc/rfc4810.txt`
126. Walpole, R.E., Myers, R.H.: Probabilidad y estadística, Fourth edn. McGraw-Hill (1994)
127. Wang, X., Yu, H.: How to break MD5 and other hash functions. In: R. Cramer (ed.) Advances in Cryptology, *Lecture Notes in Computer Science*, vol. 3494, pp. 19–35. EUROCRYPT, Springer (2005)
128. Yee, B.S.: A sanctuary for mobile agents. In: Secure Internet Programming, pp. 261–273 (1999)
129. Zhou, J.: Non-repudiation in electronic commerce. Computer Security Series. Artech House (2001)
130. Zhou, J.: On the security of a multi-party certified email protocol. In: Information and Communications Security: 6th International Conference, vol. 3269, pp. 40–52 (2004)
131. Zhou, J., Deng, R.: On the validity of digital signatures. ACM SIGCOMM Computer Communication Review **30**(2), 29–34 (2000). DOI http://doi.acm.org/10.1145/505680.505684
132. Zhou, J., Gollmann, D.: A fair non-repudiation protocol. In: Proceedings of IEEE Symposium on Security and Privacy, pp. 55–61. IEEE Computer Society Press (1996)
133. Zhou, J., Gollmann, D.: An efficient non-repudiation protocol. In: PCSFW: Proceedings of The 10th Computer Security Foundations Workshop, pp. 126–132. IEEE Computer Society Press (1997). URL `citeseer.nj.nec.com/article/zhou97efficient.html`
134. Zhou, J., Lam, K.: Undeniable billing in mobile communication. In: Proceedings of the 4th Annual ACM/IEEE International Conference on Mobile Computing and Networking, pp. 284–290 (1998)
135. Zhou, J., Onieva, J.A., Lopez, J.: Optimised multi-party certified email protocols. Information Management & Computer Security Journal **13**(5), 350–366 (2005)
136. Zhou, J., Onieva, J.A., Lopez, J.: A synchronous multi-party contract signing protocol improving lower bound of steps. In: 21st IFIP International Information Security Conference Security and Privacy in Dynamic Environments, *IFIP*, vol. 201, pp. 221–232. IFIP SEC, Springer (2006)

Index

Biographies

Dr. Jose A. Onieva received his M.S. in Computer Science in 2002 in the University of Malaga (UMA), Spain, actively collaborating with the Computer Science Department. Afterwards, he stayed as a "Research fellow" in Infocomm Research Institute (I2R), Singapore, period in which initiated a research in the areas of non-repudation, mobile agents and P2P. Funded by the Junta de Andaluca government, he joined the Security Group of the Computer Science department at UMA where he received his PhD degree in 2006. Among other activities he has been actively involved in the IST European project from the VI Programme Framework - UBISEC (Ubiquitious Networks with a Secure Provision of Services, Access and Content Delivery) and has actively collaborated in security-related National funded projects. He has published several international journal and papers in the field of Security for Information Technologies. Currently, he is an Assistant Professor at the Computer Science Department and participates as a research collaborator in several European and National Projects and Programmes. He is an involved member of the ARES (Advanced Research on Information Security and Privacy) National Program (Ingenio 2010) whose objective is to advance the state of the art and the practice of information security and privacy in Spain. He also served as a General Chair in WISTP'08 (Workshop in Information Security Theory and Practices) and as a member of several Conference Programme Committees.

Dr. Javier Lopez received his M.S. and Ph.D. in Computer Science in 1992 and 2000, respectively, from University of Malaga, where he currently is Full Professor. His research activities are mainly focused on information and network security, leading some international research projects in those areas. Prof. Lopez is the Co-Editor in Chief of Springer's International Journal of Information Security (IJIS) and member of the Editorial Boards of Computer Networks (COMNET), Wireless Communication and Mobile Computing (WCMC), Journal of Network and Computer Applications (JNCA), Security and Communications Network Journal (SCN), Information Management and Computer Security Journal (IMCS) and the International Journal of Internet Technology and Secured Transactions (IJITST). Additionally, Prof. Lopez is the Spanish representative in the IFIP Technical Committee 11

on Security and Protection in Information Systems, a member of the Steering Committee of ERCIM's Working Group on Security and Trust Management, and Chair of the IFIP Working Group on Trust Management.

Dr. Jianying Zhou is a senior scientist at Institute for Infocomm Research (I2R), and heads the Network Security Group. Dr. Zhou worked in China, Singapore, and USA before joining I2R. He was a security consultant at the headquarters of Oracle Corporation, and took an architect role on securing e-business applications. He was a project manager at Kent Ridge Digital Labs, and led an R&D team to develop network security technologies. He was a post-doctoral fellow in National University of Singapore, and involved in a strategic research programme on computer security funded by National Science and Technology Board. He was formerly employed in Chinese Academy of Sciences, and played a critical role in a couple of national information security projects.

Dr. Zhou obtained PhD degree in Information Security from University of London, MSc degree in Computer Science from Chinese Academy of Sciences, and BSc degree in Computer Science from University of Science and Technology of China. His research interests are in computer and network security, cryptographic protocol, digital signature and non-repudiation, mobile and wireless communications security, and secure electronic commerce.

Dr. Zhou is actively involved in the academic community, having served over 100 times in international conference committees as general chair, program chair, publication chair, publicity chair and PC member, having been in the editorial board and as a regular reviewer for over 20 international journals. He has published over 120 referred papers at international conferences and journals, of which the top 10 publications received over 1000 citations. He is a world-leading researcher on non-repudiation, and authored the book Non-repudiation in Electronic Commerce which was published by Artech House in 2001. He is a co-founder and steering committee member of International Conference on Applied Cryptography and Network Security, and served as program chair of ACNS'03 and general chair of ACNS'04. He is also a co-founder and coordinating editor of Cryptology and Information Security Series published by IOS Press. He received National Science and Technology Progress Award from Ministry of Science and Technology in 1995 in recognition of his achievement in the research and development of information security in China.