Scientific Publications co-authored by Giampaolo Bella

Contents

1 Monograph

[M1] G. Bella. Formal Correctness of Security Protocols. Series *Information Security and Cryptography*. Springer. 2007. Hardcover, 274 pagine, 64 illustrations. ISBN: 978-3-540-68134-2. http://www.springer.com/computer/foundations/book/978-3-540-68134-2

2 Ph.D. Thesis

[T1] G. Bella. *Inductive Verification of Cryptographic Protocols*. PhD thesis, Research Report 493, Computer Laboratory, University of Cambridge, 2000. Entered among "Distinguished Dissertations" in the UK in the A.Y. 1999-2000. Accepted for publication on 27th January 2005 as a volume in Springer's Lecture Notes in Computer Science series.

3 Book chapter

[B1] G. Bella and S. Bistarelli and F. Massacci. Retaliation: Can we live with Flaws?. Capitolo 1 in *Information Assurance and Computer Security*. IOS. 2006. Hardcover, 216 pagine. ISBN: 1-58603-678-5. http://www.iospress.nl/flyers_b/fl9781586036782.pdf

4 Journal articles

Single author

[J26] G. Bella. Out to Explore the Cybersecurity Planet. *Emerald Journal of Intellectual Capital*, 21(2):291–307, 2020. doi:https://doi.org/10.1108/JIC-05-2019-0127.

[J25] G. Bella. Inductive Study of Confidentiality, for Everyone. *Springer Formal Aspects of Computing*, 26(1):3–36, 2014. doi:https://doi.org/10.1007/s00165-012-0246-3.

[J24] G. Bella. The Principle of Guarantee Availability for Security Protocol Analysis. *Springer International Journal of Information Security*, 9(2):83–97, 2010. doi:https://doi.org/10.1007/s10207-009-0097-y.

[J23] G. Bella. What is Correctness of Security Protocols? *Journal of Universal Computer Science*, 14(12):2083–2197, 2008. URL: https://scholar.google.com/scholar?cluster=18098711463260385278&hl=en&as_sdt=0,5.

[J22] G. Bella. Inductive Verification of Smart Card Protocols. *IOS Journal of Computer Security*, 11(1):87–132, 2003. doi:https://doi.org/10.3233/jcs-2003-11103.

Multiple authors

[J21] G. Bella, P. Biondi, and G. Tudisco. A Double Assessment of Privacy Risks Aboard Top-Selling Cars. *Springer Automotive Innovation*, 2023. To appear.

[J20] G. Bella, P. Biondi, P. Costantino, and I. Matteucci. Designing and Implementing an AUTOSAR-based Basic Software Module for Enhanced Security. *Elsevier Computer Networks*, 218:109377, 2022. doi:https://doi.org/10.1016/j.comnet.2022.109377.

[J19] G. Bella, J. Ophoff, K. Renaud, D. Sempreboni, and L. Viganò. Perceptions of Beauty in Security Ceremonies. *Springer Philosophy & Technology*, 35(72), 2022. doi:https://doi.org/10.1007/s13347-022-00552-0.

[J18] M. C. Eisele, M. Maugeri, R. Shriwas, C. Huth, and G. Bella. Embedded Fuzzing: a Review of Challenges, Tools, and Solutions. *Springer Cybersecurity Journal*, 5(18), 2022. doi:https://doi.org/10.1186/s42400-022-00123-y.

[J17] G. Bella, R. Giustolisi, and C. Schürmann. Modelling Human Threats in Security Ceremonies. *IOS Journal of Computer Security*, 2022. In press.

[J16] G. Bella, P. Biondi, and S. Bognanni. Multi-service Threats: Attacking and Protecting Network Printers and VoIP Phones Alike. *Elsevier Internet of Things*, 18, 2022. doi:https://doi.org/10.1016/j.iot.2022.100507.

[J15] R. Giustolisi, G. Bella, and G. Lenzini. Invalid Certificates in Modern Browsers: A Socio-Technical Analysis. *IOS Journal of Computer Security*, 26(4):509–541, 2018. doi:https://doi.org/10.3233/JCS-16891.

[J14] G. Bella, R.Giustolisi, G.Lenzini, and P.Ryan. Trustworthy Exams without Trusted Parties. *Elsevier Computers & Security*, 67:291–307, 2017. doi:https://doi.org/10.1016/j.cose.2016.12.005.

[J13] G. Bella, P. Curzon, and G.Lenzini. Service Security and Privacy as a Socio-Technical Problem. *IOS Journal of Computer Security*, 23(5):563–585, 2015. doi:https://doi.org/10.3233/jcs-150536.

[J12] G. Bella, G. Costantino, J. Crowcroft, and S. Riccobene. Enhancing DSR Maintainance with Power Awareness. *Elsevier Computer Standards & Interfaces*, 35(1):107–113, 2013. doi:https://doi.org/10.1016/j.csi.2012.06.007.

[J11] G. Bella, R. Giustolisi, and S. Riccobene. Enforcing privacy in e-commerce by balancing anonymity and trust. *Elsevier Computers and Security*, 30(8):705–718, 2011. doi:https://doi.org/10.1016/j.cose.2011.08.005.

[J10] W. Arsac, G. Bella, X. Chantry, and L. Compagna. Multi-Attacker Protocol Validation. *Springer International Journal of Automated Reasoning*, 46(3-4):353–388, 2011. doi:https://doi.org/10.1007/s10817-010-9185-y.

[J9] G. Bella, G. Costantino, and S. Riccobene. Evaluating the Device Reputation through Full Observation in MANETs. *MIR Labs Journal of Information Assurance and Security*, 4(4):458–465, 2009. URL: https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=Evaluating+the+Device+Reputation+through+Full+Observation+in+MANETs&btnG=.

[J8] G. Bella, S. Bistarelli, and F. Massacci. Retaliation Against Protocol Attacks. *Dynamic Publishers Journal of Information Assurance and Security*, 3(4):313–325, 2008. URL: https://scholar.google.com/scholar?cluster=7498092036029681993&hl=en&as_sdt=0,5.

[J7] G. Bella and L. C. Paulson. Accountability Protocols: Formalized and Verified. *ACM Transactions on Information and System Security*, 9(2):138–161, 2006. doi:https://doi.org/10.1145/1151414.1151416.

[J6] G. Bella, F. Massacci, and L. C. Paulson. Verifying the SET Purchase Protocols. *Springer Journal of Automated Reasoning*, 36(1-2):5–37, 2005. doi:https://doi.org/10.1007/s10817-005-9018-6.

[J5] G. Bella and S. Bistarelli. Information Assurance for Security Protocols. *Elsevier Computers and Security*, 24(4):322–333, 2005. doi:https://doi.org/10.1016/j.cose.2004.10.004.

[J4] G. Bella, F. Massacci, and L. C. Paulson. An Overview of the Verification of SET. *Springer International Journal of Information Security*, 4(1-2):175–192, 2005. doi:https://doi.org/10.1007/s10207-004-0047-7.

[J3] G. Bella and S. Bistarelli. Soft Constraint Programming to Analysing Security Protocols. *Cambridge University Press Journal of Theory and Practice of Logic Programming*, 4(5):1–28, 2004. doi:https://doi.org/10.1017/s1471068404002121.

[J2] G. Bella, F. Massacci, and L. C. Paulson. Verifying the SET Registration Protocols. *IEEE Journal of Selected Areas in Communications*, 21(1):77–87, 2003. doi:https://doi.org/10.1109/jsac.2002.806133.

[J1] G. Bella and E. Riccobene. Formal Analysis of the Kerberos Authentication System. *Springer Journal of Universal Computer Science*, 3(12):1337–1381, 1997. URL: https://scholar.google.com/scholar?cluster=2138398936265151976&hl=en&as_sdt=0,5.

5 Editorials

International journals

[E36] G. Bella and H. Janicke. Editorial of Special Issue on ACM SAC 2013. *Springer International Journal of Information Security*, 14(2):101–102, 2015.

[E35] G. Bella and P. Y. Ryan. Editorial of Special Issue. *IOS Journal of Computer Security*, 17(3):2-3, 2009.

[E34] G. Bella and P. Y. Ryan. Editorial of Special Issue. *IOS Journal of Computer Security*, 13(15):2-3, 2005.

[E33] G. Bella and R. Menezes. Editorial of Special Issue in Computer Security. *Wiley Concurrency and Computation: Practice and Experience*, 16(11):1061–1062, 2004.

Proceedings of international conferences

[E32] G. Bella and S. Radomirovic. Editorial of the Special Track in Computer Security. In B. Panda, editor, *Proc. of the 37th ACM Symposium on Applied Computing (ACM SAC'22)*. ACM Press, April 2022.

[E31] G. Bella and G. Lenzini. Foreword from the Workshop Chairs. In L. Viganò and S. Parkin, editors, *Proc. of the 11th Workshop on Socio-Technical Aspects in Security and Trust*, LNCS. Springer, 2021.

[E30] G. Bella and R. Giustolisi. Editorial of the Special Track in Computer Security. In B. Panda, editor, *Proc. of the 36th ACM Symposium on Applied Computing (ACM SAC'21)*. ACM Press, March 2021.

[E29] G. Bella and G. Lenzini. Foreword from the Workshop Chairs. In T. Gross and L. Viganò, editors, *Proc. of the 10th Workshop on Socio-Technical Aspects in Security and Trust*, LNCS 12812. Springer, 2020.

[E28] G. Bella and R. Giustolisi. Editorial of the Special Track in Computer Security. In B. Panda, editor, *Proc. of the 35th ACM Symposium on Applied Computing (ACM SAC'20)*. ACM Press, March 2020.

[E27] G. Bella and G. Lenzini. Foreword from the Workshop Chairs. In T. Gross and T. Tryfonas, editors, *Proc. of the 9th Workshop on Socio-Technical Aspects in Security and Trust*, LNCS 11739. Springer, 2019.

[E26] G. Bella and R. Giustolisi. Editorial of the Special Track in Computer Security. In B. Panda, editor, *Proc. of the 34th ACM Symposium on Applied Computing (ACM SAC'19)*. ACM Press, April 2019.

[E25] G. Bella and G. Lenzini. Foreword from the Workshop Chairs. In *Proc. of the 8th Workshop on Socio-Technical Aspects in Security and Trust*. ACM Press, 2018.

[E24] G. Bella and L. Desmet. Editorial of the Special Track in Computer Security. In B. Panda, editor, *Proc. of the 33rd ACM Symposium on Applied Computing (ACM SAC'18)*. ACM Press, April 2018.

[E23] G. Bella and G. Lenzini. Foreword from the Workshop Chairs. In *Proc. of the 7th Workshop on Socio-Technical Aspects in Security and Trust*. ACM Press, 2017.

[E22] G. Bella and L. Desmet. Editorial of the Special Track in Computer Security. In B. Panda, editor, *Proc. of the 32nd ACM Symposium on Applied Computing (ACM SAC'17)*. ACM Press, April 2017.

[E21] G. Bella and G. Lenzini. Foreword from the Workshop Chairs. In *Proc. of the 6th Workshop on Socio-Technical Aspects in Security and Trust*. IEEE Xplore Digital Library, 2016.

[E20] G. Bella and S. Maffeis. Editorial of the Special Track in Computer Security. In B. Panda, editor, *Proc. of the 31st ACM Symposium on Applied Computing (ACM SAC'16)*. ACM Press, April 2016.

[E19] G. Bella and G. Lenzini. Foreword from the Workshop Chairs. In *Proc. of the 5th Workshop on Socio-Technical Aspects in Security and Trust*. IEEE Xplore Digital Library, 2015.

[E18] G. Bella and S. Maffeis. Editorial of the Special Track in Computer Security. In B. Panda, editor, *Proc. of the 30th ACM Symposium on Applied Computing (ACM SAC'15)*. ACM Press, April 2015.

[E17] G. Bella and G. Lenzini. Foreword from the Workshop Chairs. In *Proc. of the 4th Workshop on Socio-Technical Aspects in Security and Trust*. IEEE Xplore Digital Library, 2014.

[E16] G. Bella, S. Kremer, and M. Barbosa. Editorial of the Special Track in Computer Security. In B. Panda, editor, *Proc. of the 29th ACM Symposium on Applied Computing (ACM SAC'14)*. ACM Press, March 2014.

[E15] G. Bella and G. Lenzini. Foreword from the Workshop Chairs. In *Proc. of the 3rd Workshop on Socio-Technical Aspects in Security and Trust*. IEEE Xplore Digital Library, 2013.

[E14] G. Bella, H. Janicke, and G. Steel. Editorial of the Special Track in Computer Security. In B. Panda, editor, *Proc. of the 28th ACM Symposium on Applied Computing (ACM SAC'13)*. ACM Press, March 2013.

[E13] G. Bella and G. Lenzini. Foreword from the Workshop Chairs. In *Proc. of the 2nd Workshop on Socio-Technical Aspects in Security and Trust*. IEEE Xplore Digital Library, 2012.

[E12] G. Bella, H. Janicke, and A. Sorniotti. Editorial of the Special Track in Computer Security. In B. Panda, editor, *Proc. of the 27th ACM Symposium on Applied Computing (ACM SAC'12)*. ACM Press, March 2012.

[E11] G. Bella and G. Lenzini. Foreword from the General Chairs. In *Proc. of the 1st Workshop on Socio-Technical Aspects in Security and Trust*. IEEE Xplore Digital Library, 2011.

[E10] G. Bella, H. Janicke, and A. Sorniotti. Editorial of the Special Track in Computer Security. In B. Panda, editor, *Proc. of the 26th ACM Symposium on Applied Computing (ACM SAC'11)*. ACM Press, March 2011.

[E9] G. Bella, L. Compagna, and A. Sorniotti. Editorial of the Special Track in Computer Security. In B. Panda, editor, *Proc. of the 25th ACM Symposium on Applied Computing (ACM SAC'10)*. ACM Press, March 2010.

[E8] G. Bella and L. Compagna. Editorial of the Special Track in Computer Security. In B. Panda, editor, *Proc. of the 24th ACM Symposium on Applied Computing (ACM SAC'09)*. ACM Press, March 2009.

[E7] G. Bella. Editorial of the Special Track in Computer Security. In B. Panda, editor, *Proc. of the 20th ACM Symposium on Applied Computing (ACM SAC'08)*, pages 2095–2096. ACM Press, March 2008.

[E6] G. Bella and P. Y. Ryan. Editorial of the Special Track in Computer Security. In B. Panda, editor, *Proc. of the 21th ACM Symposium on Applied Computing (ACM SAC'07)*, pages 239–240. ACM Press, March 2007.

[E5] G. Bella and P. Y. Ryan. Editorial of the Special Track in Computer Security. In B. Panda, editor, *Proc. of the 21th ACM Symposium on Applied Computing (ACM SAC'06)*, pages 321–322. ACM Press, March 2006.

[E4] G. Bella and P. Y. Ryan. Editorial of the Special Track in Computer Security. In B. Panda, editor, *Proc. of the 20th ACM Symposium on Applied Computing (ACM SAC'05)*, pages 304–305. ACM Press, March 2005.

[E3] G. Bella and P. Y. Ryan. Editorial of the Special Track in Computer Security. In B. Panda, editor, *Proc. of the 19th ACM Symposium on Applied Computing (ACM SAC'04)*, pages 373–374. ACM Press, March 2004.

[E2] G. Bella and R. Menezes. Editorial of the Special Track in Computer Security. In B. Panda, editor, *Proc. of the 18th ACM Symposium on Applied Computing (ACM SAC'03)*, pages 280–281. ACM Press, March 2003.

[E1] G. Bella, R. Menezes, and J. Wittaker. Editorial of the Special Track in Computer Security. In B. Panda, editor, *Proc. of the 17th ACM Symposium on Applied Computing (ACM SAC'02)*, pages 194–195. ACM Press, March 2002.

6 Papers in proceedings of international conferences

Single author upon invitation

[C84] G. Bella. Cybersecurity's Way Forward: to get Beautiful or Invisible (Invited Paper). In V. Bilò and A. Caruso, editors, *Proc. of the 17th Italian Conference on Theoretical Computer Science (ICTCS'16)*, CEUR 1720. CEUR Workshop Proceedings, September 2016.

[C83] G. Bella. What is Correctness of Security Protocols? (Invited Paper). In E. Börger and M. Prinz, editors, *Proc. of the 14th International Workshop on Abstract State Machines (ASM07)*, June 2007.

Single author

[C82] Bella. You Already Used Formal Methods but Did Not Know It. In Brijesh Dongol, Luigia Petre, and Graeme Smith, editors, *Proc. of the 3rd International Workshop and Tutorial, FMTea 2019, held as part of the 3rd World Congress on Formal Methods*, LNCS 11758, pages 228–243. Springer, 2019.

[C81] G. Bella. Inductive analysis when state enumeration explodes. In R.Breitling et al., editor, *Report of Dagstuhl Seminar 11151, Dagstuhl Reports 1(4)*. Schloss Dagstuhl–Leibniz-Zentrum für Informatik Press, 2011.

[C80] G. Bella. Availability of Protocol Goals. In B. Panda, editor, *Proc. of the 18th ACM Symposium on Applied Computing (ACM SAC'03)*, pages 312–317. ACM Press, March 2003.

[C79] G. Bella. Interactive Simulation of Security Policies. In B. Panda, editor, *Proc. of the 17th ACM Symposium on Applied Computing (ACM SAC'02)*, pages 247–252. ACM Press, March 2002.

[C78] G. Bella. Mechanising a Protocol for Smart Cards. In I. Attali and T. Jensen, editors, *Proc. of the 1st International Conference on Research in Smart Cards (e-Smart'01)*, LNCS 2140, pages 19–33. Springer, Sept. 2001.

[C77] G. Bella. Lack of Explicitness Strikes Back. In B. Christianson et al., editor, *Proc. of the 8th International Workshop on Security Protocols (IWSP'00)*, LNCS 2133, pages 87–99. Springer, April 2000.

[C76] G. Bella. Modelling Security Protocols Based on Smart Cards. In M. Blum and C. H. Lee, editors, *Proc. of the 1st International Workshop on Cryptographic Techniques & E-Commerce (CrypTEC'99)*, pages 139–146. Hong Kong CityU Press, July 1999.

[C75] G. Bella. Modelling Agents' Knowledge Inductively. In B. Christianson, B. Crispo, J. A. Malcolm, and M. Roe, editors, *Proc. of the 7th International Workshop on Security Protocols (IWSP'99)*, LNCS 1796, pages 85–94. Springer, April 1999.

Multiple authors

[C74] S. Esposito, D. Sgandurra, and G. Bella. Alexa versus Alexa: Controlling Smart Speakers by Self-Issuing Voice Commands. In *Proc of the 17th ACM ASIA Conference on Computer and Communications Security (ACM ASIACCS 2022)*. ACM Press, 2022.

[C73] G. Bella, C. Daniele, and M. Raciti. The AILA Methodology for Automated and Intelligent Likelihood Assignment. In *Proc of the 6th International Conference on Cryptography, Security and Privacy (CSP'22)*, 2022.

[C72] P. Biondi, S. Bognanni, and G. Bella. Vulnerability assessment and penetration testing on ip camera. In *Proc of the 8th International Conference on Internet of Things: Systems, Management and Security (IOTSMS'21)*, pages 1–8. IEEE Xplore, 2021.

[C71] G. Bella, P. Biondi, M. Vincenzi, and G. Tudisco. Privacy and modern cars through a dual lens. In *Proc of the IEEE European Symposium on Security and Privacy Workshops (EuroS&PW'21)*, pages 136–143. IEEE Xplore, 2021.

[C70] G. Bella, P. Biondi, and G. Tudisco. Car drivers' privacy concerns and trust perceptions. In Simone et al. Fischer-Hübner, editor, *Proc. of the 18th International Conference on Trust, Privacy and Security in Digital Business (TrustBus'21)*, LNCS 12927, pages 143–154. Springer, 2021.

[C69] G. Bella, D. Cantone, C. Longo, M. Nicolosi Asmundo, and D. F. Santamaria. Blockchains through ontologies: the case study of the ethereum ERC721 standard in OASIS. Studies in Computational Intelligence, pages 191–198. Springer, 2021.

[C68] G. Bella, D. Cantone, C. Longo, M. Nicolosi Asmundo, and D. F. Santamaria. Semantic representation as a key enabler for blockchain-based commerce. In K. et al. Tserpes, editor, *Proc. of the International Conference on the Economics of Grids, Clouds, Systems, and Services (GECON'21)*, LNCS 13072, pages 191–198. Springer, 2021.

[C67] F. Pollicino, D. Stabili, G. Bella, and M. Marchetti. Sixpack: Abusing abs to avoid misbehavior detection in vanets. In *Proc. of the IEEE 93rd Vehicular Technology Conference (VTC'21)*, pages 1–6. IEEE Xplore, 2021.

[C66] G. Bella, P. Biondi, G. Costantino, I. Matteucci, and M. Marchetti. Towards the COSCA framework for COnseptualing Secure CArs. In Heiko RoAYnagel, Christian H. Schunck, and Sebastian Mödersheim, editors, *Proc of the Open Identity Summit 2021*, Lecture Notes in Informatics, pages 37–46. Gesellschaft für Informatik, 2021.

[C65] G. Bella, P. Biondi, P. Costantino, and I. Matteucci. CINNAMON: A module for autosar secure onboard communication. In *Proc. of the 16th European Dependable Computing Conference (EDCC'20)*, pages 103–110. ACM Press, 2020.

[C64] P. Biondi, S. Bognanni, and G. Bella. VoIP Can Still Be Exploited — Badly. In *Proc. of the 5th International Conference on Fog and Mobile Edge Computing, (FMEC'20)*, pages 237–243. IEEE, 2020.

[C63] G. Bella and P. Biondi. You Overtrust your Printer. In *Proc. of the 2nd International Workshop on Safety, securiTy, and pRivacy In automotiVe systEms (STRIVE'19)*, LNCS 11699, pages 264–274. Springer, 2019.

[C62] P. Biondi, G. Bella, G. Costantino, and I. Matteucci. Implementing CAN bus security by TOUCAN. In *Proc. of the 20th ACM International Symposium on Mobile Ad Hoc Networking and Computing (Mobihoc 2019)*, pages 399–400. ACM, 2019.

[C61] P. Biondi, G. Bella, G. Costantino, and I. Matteucci. Are You Secure in Your Car? In *Proc. of the 12th Conference on Security and Privacy in Wireless and Mobile Networks (WiSec'19)*, pages 308–309, New York, NY, USA, 2019. ACM Press.

[C60] D. Sempreboni, G. Bella, R. Giustolisi, and L. Viganò. What are the threats? (charting the threat models of security ceremonies). In P. Samarati, W. Lou, and J. Zhou, editors, *Proc of the 16th International Conference on Security and Cryptography (Secrypt'19)*. SciTe Press, 2019.

[C59] G. Bella, K. Renaud, D. Sempreboni, and L. Viganò. An investigation into the beautification of security ceremonies. In P. Samarati, W. Lou, and J. Zhou, editors, *Proc of the 16th International Conference on Security and Cryptography (Secrypt'19)*. SciTe Press, 2019.

[C58] G. Bella, P. Biondi, P. Costantino, and I. Matteucci. TOUCAN: A proTocol tO secUre Controller Area Network. In *Proc. of the ACM Workshop on Automotive Cybersecurity (AutoSec'19)*, pages 3–8. ACM Press, 2019.

[C57] G. Bella and P. Biondi. Towards an integrated penetration testing environment for the CAN protocol. In *Proc. of the 1st International Workshop on Safety, securiTy, and pRivacy In automotiVe systEms (STRIVE'18)*, LNCS 11094, pages 344–352. Springer, 2018.

[C56] G. Bella, G. Costantino, F. Marino, and F. Martinelli. Getmewhere: A location-based privacy-preserving information service. In *Proc. of the 26th Euromicro International Conference on Parallel, Distributed and Network-based Processing (PDP'18)*, pages 529–532. CPS Press, 2018.

[C55] G. Bella and R. Giustolisi. Idea: A unifying theory for evaluation systems. In *Proc. of the 9th International Symposium on Engineering Secure Software and Systems (ESSoS'18)*, LNCS 10379, pages 231–239. Springer, 2017.

[C54] G. Bella, D. Butin, and H. Jonker. Analysing Privacy Analyses. In A. Armando, R. Baldoni, and R. Focardi, editors, *Proc. of the 1st Italian Conference on Cybersecurity (ITA-SEC'17)*, CEUR Series. CEUR Workshop Proceedings, January 2017.

[C53] G. Bella, B. Christianson, and L. Viganò. Invisible Security. In J. Anderson et al., editor, *Proc. of the 24th International Workshop on Security Protocols Cambridge (IWSP'16)*, LNCS 10368, pages 1–18. Springer, March 2016.

[C52] G. Bella, R. Giusolisi, G. Lenzini, and P. Ryan. A Secure Exam Protocol Without Trusted Parties. In D.Gritzalis, S.Furnell, and M.Theoharidou, editors, *Proc of 30th IFIP International Information Security and Privacy Conference (IFIP SEC'15)*. IFIPAICT 455, pages 495–509. Springer, 2015.

[C51] G. Bella and L. Viganò. Security is Beautiful. In B. Christianson et al., editor, *Proc. of the 23rd International Workshop on Security Protocols Cambridge (IWSP'15)*, LNCS 9379, pages 247–260. Springer, April 2015.

[C50] G. Bella, R. Giustolisi, and G.Lenzini. Secure exams despite malicious management. In *Proc of 12th International Conference on Privacy, Security and Trust (PST'14)*, pages 274–281. IEEE Xplore, 2014.

[C49] G. Bella, P. Jp̈pinen, and J. Laakkonen. The challenges behind independent living support systems. In D. Ślezak et al., editor, *Proc of the 8th International Workshop on Human Aspects in Ambient Intelligence (HAI'14)*, LNCS 8610, pages 464–474. Springer, 2014.

[C48] G. Bella, P. Curzon, R. Giustolisi, and G.Lenzini.
newblock A socio-technical methodology for the security and privacy analysis of services. In *Proc of the 38th IEEE International Computer Software and Applications Conference Workshops (COMPSACW'14)*, pages 401–406. IEEE Xplore, 2014.

[C47] R. Giustolisi, G. Lenzini, and G. Bella. What security for electronic exams? In R. Sandhu and B. Crispo, editors, *Proc of 8th International Conference on Risks and Security of Internet and Systems (CRiSIS'13)*. IEEE Xplore, 2013.

[C46] G. Bella, R. Giustolisi, and G.Lenzini. Socio-technical formal analysis of tls certificate validation in modern browsers. In Jordi Castella-Roca et al., editor, *Proc of 11th International Conference on Privacy, Security and Trust (PST'13)*, pages 309–316. IEEE Press, 2013.

[C45] G. Bella, R. Giustolisi, and G.Lenzini. A socio-technical underndng of TLS certificate validation. In M. C. Fernández Gago et al., editor, *Proc of 7th IFIP International Conference on Trust Management (IFIP TM'13)*, IFIP AICT 401, pages 281–288. Springer, 2013.

[C44] D. Butin, D. Gray, and D. Butin. Towards verifying voter privacy through unlinkability. In *Proc of the International Symposium on Engineering Secure Software and Systems (ESSoS'13)*, LNCS. Springer, 2013.

[C43] G. Bella and D. Butin. Verifying privacy by little interaction and no process equivalence. In P. Samarati, W. Lou, and J. Zhou, editors, *Proc of the 3rd International Conference on Security and Cryptography (Secrypt'12)*, pages 251–256. SciTe Press, 2012.

[C42] G. Bella and L. Coles-Kemp. Layered analysis of security ceremonies. In D.Gritzalis, S.Furnell, and M.Theoharidou, editors, *Proc of 27th IFIP International Information Security and Privacy Conference (IFIP SEC'12)*, pages 273–286. Springer, 2012.

[C41] G. Bella and L. Coles-Kemp. Seeing the full picture: the case for extending security ceremony analysis. In *Proc of 9th Australian Information Security Management Conference (AISM'11)*. Secau Security Research Centre Press, 2011.

[C40] G. Bella, D. Butin, and D. Gray. Holistic analysis of mix protocols. In *Proc of the 7th IEEE International Conference on Information Assurance and Security (IEEE IAS'11)*. IEEE Press, 2011.

[C39] G. Bella and L. Coles-Kemp. Internet users' security and privacy while they interact with Amazon. In *Proc of IEEE International Workshop on Trust and Identity in Mobile Internet, Computing and Communications (IEEE TrustID'11)*. IEEE Press, 2011.

[C38] G. Bella, L. Coles-Kemp, G. Costantino, and S. Riccobene. Remote management of face-to-face written authenticated though anonymous exams. In *Proc. of the 3nd International Conference on Computer Supported Education (CSEDU'11)*. INSTICC Press, 2011.

[C37] G. Bella, P. Ryan, and V. Teague. Virtually Perfect Democracy. In B. Christianson and J. A. Malcolm, editors, *Proc. of the 18th International Workshop on Security Protocols (IWSP'10)*, LNCS 7061, pages 161–166. Springer, April 2010.

[C36] G. Bella, G. Costantino, and S. Riccobene. Wata: A system for written authenticated though anonymous exams. In J. Cordeiro and B.Shishkov, editors, *Proc. of the 2nd International Conference on Computer Supported Education (CSEDU'10)*, pages 132–137. INSTICC Press, 2010.

[C35] G. Bella and P. Liò. Analysing the microrna-17-92/myc/e2f/rb compound toggle switch by theorem proving. In *Proc. of the 7th Workshop on Network Tools and Applications in Biology (Nettab'09)*, pages 59–62, 2009.

[C34] G. Bella and P. Liò. Formal analysis of the genetic toggle. In P. Degano and R. Gorrieri, editors, *Proc. of the 9th Conference on Computational*

Methods in Systems Biology (CMSB'09), LNBI 5688, pages 96–110. Springer, 2009.

[C33] G. Bella, G. Costantino, and S. Riccobene. Enforcing collaboration in manet routing protocols. In *Proc. of the 5th International Conference on Wireless and Mobile Communications (ICWM'09)*, pages 128–133. IEEE Computer Society, 2009.

[C32] W. Arsac, G. Bella, X. Chantry and L. Compagna. Attacking each other. In *Proc. of the 17th International Workshop on Security Protocols (CIWSP'09)*, LNCS 7028, pages 41–47. Springer, 2009.

[C31] X. Chantry W. Arsac, G. Bella and L. Compagna. Validating security protocols under the general attacker. In P. Degano and L. Viganò, editors, *Proc. of the Joint Workshop on Automated Reasoning for Security Protocol Analysis and Issues in the Theory of Security (ARSPA-WITS'09)*, LNCS 5511, pages 34–51. Springer, 2009.

[C30] G. Bella, G. Costantino, and S. Riccobene. Spreading of reputation values in a mobile network. In Nikola Rozic and Dinko Begusic, editors, *Proc. of the 2008 Workshop on Information and Communication Technologies - SoftCOM events*. IEEE Computer Society, 2008.

[C29] G. Bella, F. Librizzi, and S. Riccobene. A privacy paradigm that tradeoffs anonymity and trust. In Nikola Rozic and Dinko Begusic, editors, *Proc. of the 2008 International Conference on Software, Telecommunications and Computer Networks (SoftCOM'08)*, pages 384–388. IEEE Computer Society, 2008.

[C28] G. Bella, G. Costantino, and S. Riccobene. Managing reputation over manets. In Massimiliano Rak, Ajith Abraham, and Valentina Casola, editors, *Proc. of the 4th International Symposium on Information Assurance and Security (IAS'08)*, pages 255–260. IEEE Computer Society, 2008.

[C27] G. Bella, F. Librizzi, and S. Riccobene. Realistic threats to self-enforcing privacy. In Massimiliano Rak, Ajith Abraham, and Valentina Casola, editors, *Proc. of the 4th International Symposium on Information Assurance and Security (IAS'08)*, pages 155–160. IEEE Computer Society, 2008.

[C26] S. Foley, G. Bella, and S. Bistarelli. Security Protocol Deployment Risk. In B. Christianson and J. A. Malcolm, editors, *Proc. of the 16th International Workshop on Security Protocols (IWSP'08)*, LNCS 6615, pages 12–20. Springer, April 2008.

[C25] G. Bella, S. Bistarelli, P. Peretti, and S. Riccobene. Augmented Risk Analysis. In F. Gadducci and M. ter Beek, editors, *Proc. of the 2nd International Workshop on Views on Designing Complex Architectures (VODCA'06)*, ENTCS 168, pages 207–220. Elsevier, Sept. 2006.

[C24] G. Bella, C. Pistagna, and S. Riccobene. Locating Mobile Nodes Within Logical Networks. In M. Denko and J. Youn, editors, *Proc. of the 2005 International Conference on Pervasive Systems and Computing (PSC'05)*, pages 54–62. CSREA Press, May 2005.

[C23] G. Bella, S. Bistarelli, and S. Foley. Soft Constraints for Security (Invited Paper). In F. Gadducci and M. ter Beek, editors, *Proc. of the 1st International Workshop on Views on Designing Complex Architectures (VODCA'04)*, ENTCS 142, pages 11–29. Elsevier, Sept. 2004.

[C22] G. Bella, C. Pistagna, and S. Riccobene. Distributed Backup through Information Dispersal. In F. Gadducci and M. ter Beek, editors, *Proc. of the 1st International Workshop on Views on Designing Complex Architectures (VODCA'04)*, ENTCS Series, pages 63–77. Elsevier, Sept. 2004.

[C21] S. Battiato, G. Bella, and S. Riccobene. Should We Prove Security Policies Correct? In M. S. Obaidat and N. Boudriga, editors, *Proc. of the 1st International Workshop on Views on Designing Complex Architectures (EGCDMAS'04)*, pages 56–65. INSTICC Press, Sept. 2004.

[C20] G. Bella and S. Bistarelli. Advancing Assurance for Secure Distributed Communications. In *Proc. of the 5th Annual IEEE Information Assurance Workshop (IEEE IAW'04)*, pages 306–313. IEEE Press, June 2004.

[C19] G. Bella, C. Longo, and L. C. Paulson. Verifying Second-Level Security Protocols. In David Basin and Burkhart Wolff, editors, *Prof of the 16th International Conference on Theorem Proving in Higher Order Logics (TPHOLs'03)*, LNCS 2758, pages 352–366. Springer, Sept. 2003.

[C18] G. Bella, S. Bistarelli, and F. Massacci. A protocol's life after attacks. In B. Christianson et al., editor, *Proc. of the 11th International Workshop on Security Protocols (IWSP'03)*, LNCS 3364. Springer, April 2003.

[C17] G. Bella, S. Bistarelli, and F. Martinelli. Biometrics to Enhance Smartcard Security: Simulating MOC using TOC. In B. Christianson et al., editor, *Proc. of the 11th International Workshop on Security Protocols (IWSP'03)*, LNCS 3364. Springer, April 2003.

[C16] G. Bella, C. Longo, and L. C. Paulson. Is The Verification Problem For Cryptographic Protocols Solved? In B. Christianson et al., editor, *Proc. of the 11th International Workshop on Security Protocols (IWSP'03)*, LNCS 3364. Springer, April 2003.

[C15] G. Bella, F. Massacci, and L. C. Paulson. The Verification of an Industrial Payment Protocol: The SET Purchase Phase. In Vijay Atluri, editor, *Proc. of the 9th ACM Conference on Computer and Communications Security (ACM CCS'02)*, pages 12–20. ACM Press, Nov. 2002.

[C14] G. Bella and S. Bistarelli. Confidentiality Levels and Deliberate/Indeliberate Protocol Attacks. In B. Christianson, B. Crispo, W. S.

Harbison, and M. Roe, editors, *Proc. of the 10th International Workshop on Security Protocols Cambridge (IWSP'02)*, LNCS 2845, pages 104–119. Springer, April 2002.

[C13] G. Bella and L. C. Paulson. Analyzing Delegation Properties. In B. Christianson, B. Crispo, W. S. Harbison, and M. Roe, editors, *Proc. of the 10th International Workshop on Security Protocols Cambridge (IWSP'02)*, LNCS 2845, pages 120–127. Springer, April 2002.

[C12] G. Bella and L. C. Paulson. Mechanical Proofs about a Non-Repudiaton Protocol. In R. J. Boulton and P. B. Jackson, editors, *Proc. of the 14th International Conference on Theorem Proving in Higher Order Logics (TPHOLs'01)*, LNCS 2152, pages 91–104. Springer, Sept. 2001.

[C11] G. Bella and L. C. Paulson. A Proof of Non-Repudiation. In B. Christianson et al., editor, *Proc. of the 9th International Workshop on Security Protocols (IWSP'01)*, LNCS 2467, pages 119–133. Springer, April 2001.

[C10] G. Bella and S. Bistarelli. Soft Constraints for Security Protocol Analysis: Confidentiality. In I. V. Ramakrishnan, editor, *Proc. of the 3rd International Symposium on Practical Aspects of Declarative Languages (PADL'01)*, LNCS 1990, pages 108–122. Springer, March 2001.

[C9] G. Bella, F. Massacci, L. C. Paulson, and P. Tramontano. Formal Verification of Cardholder Registration in SET. In F. Cuppens, Y. Deswarte, D. Gollmann, and M. Waidner, editors, *Proc. of the 6th European Symposium on Research in Computer Security (ESORICS'00)*, LNCS 1985, pages 159–174. Springer, Oct. 2000.

[C8] G. Bella and S. Bistarelli. SCSPs for Modelling Attacks to Security Protocols. In P. Codognet and F. Rossi, editors, *Proc. of the Workshop on Soft Constraints of the Conference on Constraint Programming (CP'00)*, Sept. 2000.

[C7] G. Bella, F. Massacci, L. C. Paulson, and P. Tramontano. Making Sense of Specifications: the Formalization of SET. In B. Christianson et al., editor, *Proc. of the 8th International Workshop on Security Protocols (IWSP'00)*, LNCS 2133, pages 74–86. Springer, April 2000.

[C6] G. Bella and L. C. Paulson. Kerberos Version IV: Inductive Analysis of the Secrecy Goals. In J.-J Quisquater, Y. Deswarte, C. Meadows, and D. Gollmann, editors, *Proc. of the 5th European Symposium on Research in Computer Security (ESORICS'98)*, LNCS 1485, pages 361–375. Springer, Sept. 1998.

[C5] G. Bella and E. Riccobene. A Realistic Environment for Crypto-Protocol Analyses by ASMs. In U. Glässer, editor, *Proc. of the 5th International Workshop on Abstract State Machines (INFORMATIK'98)*, pages 127–138, Sept. 1998.

[C4] G. Bella and L. C. Paulson. Mechanising BAN Kerberos by the Inductive Method. In A. J. Hu and M. Y. Vardi, editors, *Proc. of the 10th International Conference on Computer-Aided Verification (CAV'98)*, LNCS 1427, pages 416–427. Springer, June 1998.

[C3] G. Bella and L. C. Paulson. Using Isabelle to prove Properties of the Kerberos Authentication System. In H. Orman and C. Meadows, editors, *Proc. of the Workshop on Design and Formal Verification of Security Protocols (DIMACS'97)*, Sept. 1997.

[C2] G. Bella and E. Riccobene. The Validation of a Bidirectional Serial/Parallel Shift Register by Evolving Algebras. In *Proc. of Annual Conference of Associazione Italiana per l'Informatica ed il Calcolo Automatico (AICA'97)*, pages 89–106, Sept. 1997.

[C1] G. Bella and E. Riccobene. Le Algebre Evolventi per la Validazione di Hardware. In *Proc. of Annual Conference of Associazione Italiana per l'Informatica ed il Calcolo Automatico (AICA'96)*, Sept. 1996.

7 Technical report

[TR6] G. Bella, F. Massacci, and L. C. Paulson. Verifying the SET Registration Protocols. Research Report 531, Computer Laboratory, University of Cambridge, March 2002.

[TR5] G. Bella and S. Bistarelli. Soft Constraint Programming to Analysing Security Protocols. Technical Report IAT-B4-2001-013, Istituto per le Applicazioni Telematiche, Consiglio Nazionale delle Ricerche, Nov. 2001.

[TR4] G. Bella, F. Massacci, and L. C. Paulson. Verifying the SET Purchase Protocols. Research Report 524, Computer Laboratory, University of Cambridge, Nov. 2001.

[TR3] G. Bella, F. Massacci, L. C. Paulson, and P. Tramontano. Formal Verification of Card-holder Registration in SET. Research Report 488, Computer Laboratory, University of Cambridge, March 2000.

[TR2] G. Bella. Message Reception in the Inductive Approach. Research Report 460, Computer Laboratory, University of Cambridge, March 1999.

[TR1] G. Bella and L. C. Paulson. Are Timestamps Worth the Effort? A Formal Treatment. Research Report 447, Computer Laboratory, University of Cambridge, Sept. 1998.