Marko Hölbl

Assistant Professor at University of Maribor, Faculty of Electrical Engineering and Computer Science,

E-mail: marko.holbl@um.si
Office: +386 2 220 7361
Address: FERI UM, Smetanova ulica 17, 2000 Maribor, Slovenia
LinkedIn: http://si.linkedin.com/in/markoholbl/
ResearchGate: https://www.researchgate.net/profile/Marko_Hoelbl/
Google Scholar: http://scholar.google.si/citations?user=gDGZxoUAAAAJ&hl=en

Short introduction

Marko Hölbl is an assistant professor in Computer Science at the Institute of Informatics at the University of Maribor, Faculty of Electrical Engineering and Computer Science.
His research interests include authentication and key agreement, securing data and communication in specific domains (e.g. wireless sensor networks (WSN), Internet of Things (IoT) and cryptography.
He is also working on user perspective of security, particularly privacy issues of social networks, cybersecurity education and protections of data.
He is currently involved in a TEMPUS project on the topic of cybersecurity education.
He is actively participating in the CEPIS LSI (Council of European Professional Informatics Societies – Legal and Security Issues Special Interest Network) and in the NIS WG 3 (Network and Information Security – Working Group 3 on secure ICT research and innovation).

Biography

Education and Training

University of Maribor, Slovenia

- PhD, Computer Science, March 2009
- BSc, Computer Science, September 2004

Work experience

- Assistant Professor, Jun 2009 - Present
  Faculty of Electrical Engineering and Computer Science, University of Maribor, Slovenia.

- Visiting Researcher, Mar 2007 – Jun 2007
  Institute for Applied Information Processing and Communications (IAIK), Faculty of Computer Science, Graz University of Technology, Graz, Austria.
  - Research on hash functions design flaws

- Junior Researcher and Teaching Assistant, Oct 2004 - Mar 2009
  Database Technology Laboratory, Faculty of Electrical Engineering and Computer Science, University of Maribor, Slovenia.
  - Analysis and development of hash functions
  - Analysis and development of authentication protocols
  - Analysis and development of authenticated key agreement protocols
  - User aspects of privacy and security

Project work

- TEMPUS ECESM (Enhancing Cyber-Security Education in Montenegro)
  2013 - 2016

Other experience

- Secretary, 2007 – Present
  Council of European Professional Informatics Societies – Legal and Security Issues Special Interest Network (CEPIS LSI)
- Member
  Network and Information Security – Working Group 3 on secure ICT research and innovation (NIS WG 3)

Teaching

1st Bologna-level courses (Bachelor, undergraduate):

- Security of Information and Communications Technology, 3rd year, Informatics and Technologies of Communication, University level
- Data Warehousing, 3rd year, Informatics and Technologies of Communication, Professional level
- Dynamic Web Solutions, 3rd year, Informatics and Technologies of Communication (optional course), and Media Communications, University level
- Programming for Media, 1st year, Informatics and Technologies of Communication (optional course), and Media Communications, University level

2nd Bologna-level courses (Master, graduate):

- Data protection, 2nd year, Informatics and Technologies of Communication

3rd Bologna-level courses (PhD):

- User aspect of security, Media Communications
- Advanced Data protection, Computer Science

Lectures and invited talks

- Identity-based authenticated key agreement protocols, Katholieke Universiteit Leuven, Dept. of electrical engineering ESAT/COSIC, Leuven, 2010.
- Authenticated Key agreement protocols, Rovira i Virgili University, Department of Computer Engineering and Mathematics, Tarragona, 2008.
- Security of dedicated hash functions, Rovira i Virgili University, Department of computer engineering and Mathematics, Tarragona, 2006.
- Cryptographic hash functions, Tampere University of Technology, Pori, Finland, 2005.

Supervision

Master Program Students (Bologna study program):

- Jernej Flisar
- Tina Schweighofer

PhD students:
- Muhamed Turkanović, Authentication and Key Agreement for IoT
- Boštjan Kežmah

Honours and Awards
- National "Junior Researcher" Grant (PhD scholarship), Oct 2004 - Mar 2009
- National award of the Slovene Society Informatika (Slovene Professional Informatics Society) for the year 2015.

Research
Research topics:
- Authentication protocols
- Key establishment protocols
- Security protocols in WSNs (wireless sensor networks,) and IoT (Internet of Things)
- Security protocols in RFID
- User aspects of computer security
- Privacy
- Cryptography
- Applied cryptography

Reviewer
- Ad hoc networks, Amsterdam, London, New York, Oxford, Paris, Shannon, Tokyo, Elsevier, ISSN 1570-8705.
- Annales des télécommunications, Paris, Centre national d'études des télécommunications, ISSN 0003-4347.
- Computer communications, Amsterdam, Lausanne, New York, Oxford, Elsevier, 1978-, ISSN 0140-3664.
- Computer Science and Information Systems, Belgrade, ComSIS Consortium., ISSN 1820-0214.
- Computers & electrical engineering, New York, Pergamon Press, ISSN 0045-7906.
- Computers & mathematics with applications, Oxford, Pergamon Press, ISSN 0898-1221.
- Computers & security, New York, Elsevier, ISSN 0167-4048.
- Cryptologia, Laguna Hills, Calif., Aegean Park Press, ISSN 0161-1194.
- IET information security, Stevenage, Institution of Engineering and Technology, ISSN 1751-8709.
- Informatica, Vilnius, Institute of Mathematics and Informatics, ISSN 0868-4952.
- Information processing letters, Amsterdam, North-Holland, ISSN 0020-0190.
- Information sciences, New York, North-Holland, ISSN 0020-0255.
- Information Sciences Letters (Online), Natural Sciences Publishing Corporation, ISSN 2090-956X.
- Information systems, Oxford; New York: Pergamon Press., ISSN 0306-4379.
- International journal of computer mathematics, London, New York, Gordon and Breach Science Publishers, ISSN 0020-7160.
- Journal of applied mathematics and informatics, Cheongju, Korean Society for Computational & Applied Mathematics and Korean Sigcam, ISSN 2234-8417.

- Journal of network and computer applications, London, New York, Academic Press, ISSN 1084-8045.
- The Journal of systems and software, New York, Elsevier North Holland, ISSN 0164-1212.
- Journal of the Brazilian Computer Society, Sociedade Brasileira de Computação, ISSN 0104-6500.
- Journal of Zhejiang University. Science C, Computers & electronics, Berlin, Hangzhou, Zhejiang Univ. Press, Springer, ISSN 1869-196X.
- Mathematical and computer modelling, 2011, Oxford, New York, Pergamon Press, ISSN 0895-7177.
- Mathematical problems in engineering, New York, Hindawi Publishing Corporation, ISSN 1024-123X.
- Scientia iranica, Tehran, Sharif University of Technology, ISSN 1026-3098.
- Transactions on internet and information systems, Seoul, Korean Society for Internet Information, ISSN 1976-7277.
- Turkish journal of electrical engineering and computer sciences, Ankara, Scientific and Technical Research Council of Turkey, ISSN 1303-6203.

Selected Publications

(more publications available from DLBP, COBISS or Google Scholar)

Book Chapters and Sections:

- **HÖLBL, Marko**, WELZER-DRUŽOVEC, Tatjana, NEMEC ZLATOLAS, Lili. Security and privacy related issues in the internet of things. V: WELZER-DRUŽOVEC, Tatjana (ur.), et al. Information modelling and knowledge bases XXVII, (Frontiers in artificial intelligence and applications, ISSN 0922-6389, vol. 280). Amsterdam; Berlin; Washington (DC): IOS Press, cop. 2016, str. 321-326. [COBISS.SI-ID 19312406]
- **HÖLBL, Marko**, RECHBERGER, Christian, WELZER-DRUŽOVEC, Tatjana, "Searching for messages conforming to arbitrary sets of conditions in SHA-256", In: *Research in cryptology: revised selected papers : Second Western European Workshop, WEWoRC 2007 Bochum, Germany, July 4-6, 2007*, (Lecture notes in computer science, Vol. 4945), Berlin, Heidelberg, New York, Springer, cop. 2008, pp.28-38, http://www.springerlink.com/content/v7711530n2651970/, doi: 10.1007/978-3-540-88353-1_3.

Journal Papers:

- ABZINEJAD FARASH, Mohammad, TURKANOVIĆ, Muhamed, KUMARI, Saru, **HÖLBL, Marko**. An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment. Ad hoc networks, ISSN 1570-8705, Jan. 2016, vol. 36, part 1, str. 152-176, doi: 10.1016/j.adhoc.2015.05.014. [COBISS.SI-ID 18766614]
- NEMEC ZLATOLAS, Lili, WELZER-DRUŽOVEC, Tatjana, HERIČKO, Marjan, **HÖLBL, Marko**. Privacy antecedents for SNS self-disclosure : the case of Facebook. Computers in human behavior, ISSN 0747-5632. [Print ed.], April 2015, vol. 45, str. 158-167, doi: 10.1016/j.chb.2014.12.012.
- GROSS, Hannes, **HÖLBL, Marko**, SLAMANIG, Daniel, SPREITZER, Raphael. Privacy-aware authentication in the internet of things. V: REITER, Michael (ur.), NACCACHE, David (ur.). Cryptology and network security : proceedings, (Lecture notes in computer science, ISSN 0302-9743, 9476). Heidelberg; Dordrecht; London; New York: Springer, cop. 2015, str. 32-39, ilustr. [COBISS.SI-ID 19236630]
- TURKANOVIĆ, Muhamed, BRUMEN, Boštjan, **HÖLBL, Marko**. A novel user authentication and key agreement scheme for heterogeneous ad-hoc wireless sensor networks, based on

the Internet of Things notion. Ad hoc networks, ISSN 1570-8705, 2014, vol. 20, pp. 96-112, doi: 10.1016/j.adhoc.2014.03.009.

- TURKANOVIĆ, Muhamed, **HÖLBL, Marko**. The (in)adequacy of applicative use of quantum cryptography in wireless sensor networks. Quantum information processing, ISSN 1570-0755, Oct. 2014, vol. 13, iss. 10, pp. 2255-2275, doi:10.1007/s11128-014-0769-z.
- TURKANOVIĆ, Muhamed, **HÖLBL, Marko**. Notes on "A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks". Wireless personal communications, ISSN 0929-6212, Jul. 2014, vol. 77, iss. 2, pp. 907-922, doi: 10.1007/s11277-013-1543-8.
- TURKANOVIĆ, Muhamed, **HÖLBL, Marko**. An improved dynamic password-based user authentication scheme for hierarchical wireless sensor networks. Elektronika ir elektrotechnika, ISSN 1392-1215. [Print ed.], 2013, vol. 19, no. 6, pp. 109-116, doi: 10.5755/j01.eee.19.6.2038.
- BRUMEN, Boštjan, HERIČKO, Marjan, ROZMAN, Ivan, **HÖLBL, Marko**, et al. Security analysis and improvements to the psychopass method. Journal of medical internet research, ISSN 1438-8871, 2013, vol. 15, iss. 8, pp. 1-7, doi:10.2196/jmir.2366.
- BRUMEN, Boštjan, HERIČKO, Marjan, SEVČNIKAR, Andrej, ZAVRŠNIK, Jernej, **HÖLBL, Marko**. Outsourcing medical data analyses : can technology overcome legal, privacy and confidentiality issues?. Journal of medical internet research, ISSN 1438-8871, 2013, vol. 15, iss. 12, pp. 1-18, doi: 10.2196/jmir.2471.
- **HÖLBL, Marko**, WELZER-DRUŽOVEC, Tatjana, BRUMEN, Boštjan. An improved two-party identity-based authenticated key agreement protocol using pairings. Journal of computer and system sciences, ISSN 0022-0000, Jan. 2012, vol. 78, iss. 1, pp 142-150, doi: 10.1016/j.jcss.2011.01.002.
- **HÖLBL, Marko**, WELZER-DRUŽOVEC, Tatjana, BRUMEN, Boštjan. Two proposed identity-based three-party authenticated key agreement protocols from pairings. Computers & security, ISSN 0167-4048. [Print ed.], 2010, vol. 29, iss. 2, pp 244-252, doi: 10.1016/j.cose.2009.08.006.
- **HÖLBL, Marko**, WELZER-DRUŽOVEC, Tatjana. Students' feedback and communication habits using Moodle. Elektronika ir elektrotechnika, ISSN 1392-1215. [Print ed.], 2010, nr. 6, pp 63-66.
- **HÖLBL, Marko**, WELZER-DRUŽOVEC, Tatjana. Two improved two-party identity-based authenticated key agreement protocols. Computer standards & interfaces, ISSN 0920-5489. [Print ed.], Nov. 2009, vol. 31, iss. 6, pp 1056-1060, doi: 10.1016/j.csi.2008.09.024.
- **HÖLBL, Marko**, WELZER-DRUŽOVEC, Tatjana, BRUMEN, Boštjan. Attacks and improvement of an efficient remote mutual authentication and key agreement scheme. Cryptologia, ISSN 0161-1194, 2010, vol. 34, no. 1, pp 1-9, ilupp, doi: 10.1080/01611190903030912.
- **HÖLBL, Marko**, WELZER-DRUŽOVEC, Tatjana, BRUMEN, Boštjan. Comparative study of tripartite identity-based authenticated key agreement protocols. Informatica, ISSN 0350-5596, 2009, let. 33, št. 3, pp 347-355. [COBISS.SI-ID 13512982]
- **HÖLBL, Marko**, WELZER-DRUŽOVEC, Tatjana, BRUMEN, Boštjan. Improvement of the Peyravian-Jeffries`s user authentication protocol and password change protocol. Computer communications, ISSN 0140-3664. [Print ed.], June 2008, vol. 31, iss. 10, pp 1945-1951. http://dx.doi.org/10.1016/j.comcom.2007.12.029, doi:dx.doi.org/10.1016/j.comcom.2007.12.029.

<u>Conference and Workshop Papers:</u>

- Lili Nemec, **Marko Hölbl**, Jernej Burkeljca, Tatjana Welzer-Družovec, "Facebook as a teaching tool", In: *Proceedings of the 22nd EAEEIE Annual Conference, Maribor, Slovenia, June*

13-15, 2011, Tatjana Welzer-Družovec, (Eds.), Michael Hoffmann, (Ed.), Maribor, Faculty of Electrical Engineering and Computer Science, 2011, pp. 226-229.

- Lili Nemec, Boštjan Brumen, Tatjana Welzer-Družovec, **Marko Hölbl**, "Privacy awareness among students whilst using the social networking site 'Facebook'", In: *The proceedings of the 3rd International Conference on Information Society and Information Technologies - ISIT 2011, 9-11 November 2011*, Matej Mertik, (Ed.), Novo mesto, Faculty of Information Studies, 2011, pp. 11-17.
- **Marko Hölbl**, Tatjana Welzer-Družovec, "An improved authentication protocol based on One-Way Hash Functions and Diffie-Hellman Key Exchange", In: *ARES 2009, 16-19 March 2009, Fukuoka, Japan*, IEEE, 2009, pp. 894-898.
- Mirjana Ivanović, Tatjana Welzer-Družovec, Zoran Putnik, **Marko Hölbl**, Živana Komlenov, Ivan Pribela, Tina Schweighofer, "Experiences and privacy issues - usage of Moodle in Serbia and Slovenia", In: *The Challenges of Life Long Learning*, ICL2009, 23-25 September 2009, Villach/Austria, Michael E. Auer, (Eds.), Wien, International Association of Online Engineering, Kassel, University Press, 2009.
- **Marko Hölbl**, Tatjana Welzer-Družovec, "Cryptanalysis and improvement of an "improved remote authentication scheme with smart card"", In: *Proceedings*, The Third International Conference on Availability, Reliability and Security, ARES 2008, March 4-7, 2008, Barcelona, Spain, IEEE, Los Alamitos, Washnington, Tokyo, 2008, pp. 1301-1305.
- Tatjana Welzer-Družovec**, Marko Hölbl,** Ana Habjanič, Boštjan Brumen, Marjan Družovec, "Teaching of information security in the "Health Care and Nursing" postgraduate program", In: *New approaches for security, privacy and trust in complex environments : proceedings of the IFIP TC-11 22nd International security conference (SEC 2007), 14-16 May 2007, Sandton, South Africa*, (IFIP - International Federation for Information Processing, Vol. 232), IFIP TC-11 International Information Security Conference (SEC 2007), 14-16 May 2007, Sandton, South Africa, Hein Venter, (Eds.), New York, Springer, International Federation for Information Processing, 2007, pp. 479-484.