Curriculum Vitae of Rolf Oppliger

May 8, 2018

Contents

1 Personal Data

Nationality	Swiss
Date of birth	November 2, 1965
Place of birth	Bern (Switzerland)
Place of origin	Heimiswil (Switzerland)
Marital status	Married
Children	2
Languages	German (native language)
	English (fluent in spoken and written)
	French (in spoken and written)

2 Academic Degrees

Adjunct professor for computer science	University of Zurich	2007
Venia legendi* for computer science	University of Zurich	1999
Ph.D. in computer science	University of Bern	1993
M.Sc. in computer science	University of Bern	1991

* The venia legendi is the result of a process called habilitation, which is common in German-speaking countries. In this process the scientific achievements of a candidate in the postdoctoral stage, together with his or her teaching ability, are scrutinized by renowned experts in their field. To fulfil the requirements for the venia legendi, several years of research at a high level are necessary. In German-speaking countries the venia legendi or an equivalent qualification is required to be eligible for appointment as a full professor. When the candidate is given the venia legendi she or he is at the same time awarded the academic degree of a Privatdozentin or Privatdozent respectively (abbreviated PD). She or he is then obliged to give lectures at her or his university.

3 Contact Information

Private Address

Breichtenstrasse 18
CH-3074 Muri b. Bern, Switzerland
Phone +41 31 951 57 70

Business Addresses

eSECURITY Technologies Rolf Oppliger
Breichtenstrasse 18
CH-3074 Muri b. Bern, Switzerland
Phone/Fax +41 79 654 84 37
E-mail `rolf.oppliger@esecurity.ch`

Federal IT Steering Unit FITSU
Schwarztorstrasse 59
CH-3003 Bern, Switzerland
Phone (direct) +41 31 325 96 96 or +41 79 513 21 46
Phone (secretariate) +41 31 322 45 38
Fax +41 31 322 45 66
E-mail `rolf.oppliger@isb.admin.ch`

4 Memberships

- Association for Computing Machinery (ACM), senior member and distinguished speaker (until 2015)
- Institute of Electrical and Electronics Engineers (IEEE), senior member
  - IEEE Computer Society, member
    - Technical Committee on Computer Communications (TCCC)
    - Technical Committee on Distributed Processing (TCDP)
    - Technical Committee on Fault-Tolerant Computing (TCFT)
    - Technical Committee on Security & Privacy (TCSP)
- International Association for Cryptologic Research (IACR), member
- International Federation for Information Processing (IFIP)
  - Technical Committee 11 (TC11)
    - Working Group 4 (WG4) on Network Security, former vice-chair

5 Professional Career

2007 to present	Adjunct professor for computer science at the University of Zurich, Switzerland
1999 to present	Founder and owner of eSECURITY Technologies Rolf Oppliger in Muri b. Bern, Switzerland
1999	Venia legendi for computer science from the University of Zurich
1999 to present	Artech House series editor for information computer security and privacy (former computer security)
1995 to present	Scientific employee at the Swiss Federal Strategy Unit for Information Technology (FSUIT)
1994 to 1995	Post-doctoral researcher at the International Computer Science Institute (ICSI) in Berkeley, California (USA)
1993 to 1994	Scientific employee at the Institute for Computer Science and Applied Mathematics (IAM) of the University of Bern, Switzerland
1993	Ph.D. in computer science from the University of Bern
1991 to 1993	Research and teaching assistant at the IAM
1991	M.Sc. in computer science from the University of Bern
1985 to 1991	Studies at the University of Bern • Computer science (major subject) • Mathematics (first minor subject) • Economics (second minor subject)

6 Teaching Activities

- University of Zurich, Switzerland
  - 2004–2018 (held annually): IT Security
  - 2003: Security Technologies for the World Wide Web

  - 2002: IT Security (with Prof. Dr. K. Bauknecht)
  - 2001/2002: Seminar on IT Security
  - 2000/2001: Internet Security Protocols
  - 1999/2000: Security Solutions for Internet and World Wide Web Applications

- Lucerne University of Applied Sciences and Arts, Switzerland
  - 2018: Compact Course on the SSL and TLS Protocols
- Swiss Federal Institute of Technology, Switzerland
  - 2008: Compact Course on Secure Messaging in Theory and Practice (with Prof. Dr. D. Basin and Dr. R. Hauser)
  - 2007: Compact Course on Securing Online Applications (with Prof. Dr. D. Basin and Dr. R. Hauser)
- Georg-August-University Göttingen, Germany
  - 2007: Cryptography
- University of Lübeck, Germany
  - 1999: Network Security
  - 1998: Network Security
  - 1996: IT Security
- University of Duisburg-Essen, Germany
  - 2001: System Security III: Internet and Intranet Security
  - 2000: Security Technologies for the WWW
  - 1998: Security in TCP/IP-based Networks
  - 1997: System Security II: Security in Information and Communications Technology
- University of Bern, Switzerland
  - 1995/1996: Information and Communication System Security
  - 1994: Computer Security
  - 1993: Computer Security (with Prof. Dr. D. Hogrefe)
- Bern University of Applied Sciences, Switzerland
  - 1999/2000: IT Security (with P. Trachsel and R. Kraus-Ruppert)
  - 1998/1999: IT Security (with P. Trachsel, Dr. A. Greulich, and R. Kraus-Ruppert)
  - 1997/1998: IT Security (with P. Trachsel and Dr. A. Greulich)
  - 1994: Computer Security (with P. Trachsel)

7 Review Activities

- Series Editor
  - Book series on information security and privacy (former computer security), Artech House Publishers, Norwood, MA, since 1999
- Editorial Board Member
  - IEEE Security & Privacy Magazine, since 2010
  - International Journal of Information Security (IJIS), since 2013
  - Journal of Autonomic and Trusted Computing (JoATC), American Scientific Publishers (ASP), since 2005
  - IEEE Computer Magazine, Security and Privacy Area, 2011 – 2017
  - digma — Swiss Magazine for Data Protection Legislation and Information Security, Schulthess Juristische Medien AG, Zurich (Switzerland), 2000 – 2002
- Associate Editor
  - Security and Communication Networks (SCN), John Wiley & Sons, 2007 – 2016
- Guest Editor
  - Computer, Special Issue on Security Risk Assessment, scheduled for April 2017
  - Computer, Special Issue on Security and Privacy in an Online World, Vol. 44, No. 9, September 2011
  - Computer Communications, Special Issue on Advanced Security Techniques for Network Protection, Vol. 23, No. 17, November 2000, pp. 1581–1728
  - Annals of telecommunications, Special Issue on Network Security, Vol. 55, No. 7-8, July-August 2000, pp. 309–420
- Steering Committee Member
  - IEEE Cloud Computing Magazine, since 2013
- Program Committee Member
  - 14th International Conference on Information Assurance and Security (IAS 2018), Porto (Portugal), December 13 - 15, 2018
  - 6th International Symposium on Security in Computing and Communications (SSCC 2018), Bangalore (India), September 19 - 22, 2018
  - 15th International Conference on Trust, Privacy & Security in Digital Business (TrustBus 2018), held in conjunction with the 29th International Conference on Database and Expert Systems Applications (DEXA 2018), Regensburg (Germany), September 5 - 6, 2018
  - 23rd European Symposium on Research in Computer Security (ESORICS 2018), Barcelona (Spain), September 3 - 7, 2018
  - 17th International Information Security South Africa Conference (ISSA 2018), Johannesburg (South Africa), August 15 - 16, 2018

– 15th International Conference on Security and Cryptography (SECRYPT 2018), Porto (Portugal), July 26 - 28, 2018

– 7th International Conference on e-Democracy, Athens (Greece), December 14 - 15, 2017

– 22nd European Symposium on Research in Computer Security (ESORICS 2017), Oslo (Norway), September 11 - 15, 2017

– 1st ESORICS Doctoral Consortium — COINS Nordic PhD Workshop, held in conjunction with ESORICS 2017, Oslo (Norway), September 14 - 15, 2017

– 14th International Conference on Trust, Privacy & Security in Digital Business (TrustBus 2017), held in conjunction with the 28th International Conference on Database and Expert Systems Applications (DEXA 2017), Lyon (France), August 28 - 31, 2017

– 16th International Information Security South Africa Conference (ISSA 2017), Johannesburg (South Africa), August 16 - 17, 2017

– 14th International Conference on Security and Cryptography (SECRYPT 2017), Madrid (Spain), July 24 - 26, 2017

– 4th Workshop on Security in Highly Connected IT Systems (SHCIS 2017), held in conjunction with the 12th International Federated Conference on Distributed Computing Techniques (DisCoTec 2017), Neuchâtel (Switzerland), June 22, 2017

– 9th International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage (SpaCCS 2016), Zhangjiajie (China), November 18 - 20, 2016

– 21st European Symposium on Research in Computer Security (ESORICS 2016), Crete (Greece), September 26 - 30, 2016

– 10th WISTP International Conference on Information Security Theory and Practice (WISTP 2016), Crete (Greece), September 26 - 27, 2016

– 4th International Symposium on Security in Computing and Communications (SSCC 2016), Jaipur (India), September 21 - 24, 2016

– 13th International Conference on Trust, Privacy & Security in Digital Business (TrustBus 2016), held in conjunction with the 27th International Conference on Database and Expert Systems Applications (DEXA 2016), Porto (Portugal), September 5 - 8, 2016

– 11th International Conference on Availability, Reliability and Security (ARES 2016), Salzburg (Austria), August 31 - September 2, 2016

– 15th Annual Information Security South Africa Conference (ISSA 2016), Johannesburg (South Africa), August 17 - 18, 2016

– 13th International Conference on Security and Cryptography (SECRYPT 2016), Lisbon (Portugal), July 26 - 28, 2016

– 6th International Conference on e-Democracy (eDemocracy 2015), Athens (Greece), December 10 - 11, 2015

– 11th International Conference on Information Assurance and Security (IAS 2015), Bhubaneswar (India), December 5 - 6, 2015

– 8th International Conference on Security Technology (SecTech 2015), Jeju Island (Korea), November 25 - 28, 2015

- 18th International Conference on Information Security and Cryptology (ICISC 2015), Seoul (South Korea), November 25 - 27, 2015
- 20th European Symposium on Research in Computer Security (ESORICS 2015), Vienna (Austria), September 21 - 25, 2015
- 2nd Workshop on Security in Highly Connected IT Systems (SHCIS 2015), held in conjunction with the 20th European Symposium on Research in Computer Security (ESORICS 2015), Vienna (Austria), September 21 - 25, 2015
- 12th International Conference on Trust, Privacy & Security in Digital Business (TrustBus 2015), held in conjunction with the 26th International Conference on Database and Expert Systems Applications (DEXA 2015), Valencia (Spain), September 1 - 4, 2015
- 10th International Conference on Availability, Reliability and Security (ARES 2015), Toulouse (France), August 24 - 28, 2015
- 14th Annual Information Security South Africa Conference (ISSA 2015), Johannesburg (South Africa), August 12 - 14, 2015
- 12th International Conference on Security and Cryptography (SECRYPT 2015), Colmar (France), July 20 - 22, 2015
- 12th International Conference on Wirtschaftsinformatik (WI 2015), Track 8: Data Privacy and Security, Osnabrück (Germany), March 4 - 6, 2015
- 12th Annual IEEE Consumer Communications & Networking Conference (CCNC 2015), Las Vegas (USA), January 9 - 12, 2015
- 17th International Conference on Information Security and Cryptology (ICISC 2014), Seoul (South Korea), December 3 - 5, 2014
- 10th International Conference on Information Assurance and Security (IAS 2014), Okinawa (Japan), November 27 - 30, 2014
- 9th International Conference on Availability, Reliability and Security (ARES 2014), Fribourg (Switzerland), September 8 - 12, 2014
- 11th International Conference on Trust, Privacy & Security in Digital Business (TrustBus 2014), held in conjunction with the 25th International Conference on Database and Expert Systems Applications (DEXA 2014), Munich (Germany), September 1 - 5, 2014
- 11th International Conference on Security and Cryptography (SECRYPT 2014), Vienna (Austria), August 28 - 30, 2014
- 13th Annual Information Security South Africa Conference (ISSA 2014), Sandton Johannesburg (South Africa), August 13 - 15, 2014
- 10th International Conference on Information Security Practice and Experience (ISPEC 2014), Fuzhou (China), May 13 - 15, 2014
- 11th Annual IEEE Consumer Communications & Networking Conference (CCNC 2014), Technical Track on Security, Privacy and Content Protection, Las Vegas (USA), January 10 - 13, 2014
- 9th International Conference on Information Assurance and Security (IAS 2013), Tunis (Tunisia), December 4 - 6, 2013
- 5th IEEE International Conference on Cloud Computing and Science (IEEE CloudCom 2013), Security and Privacy Track, Bristol (UK), December 2 - 5, 2013

– 16th International Conference on Information Security and Cryptology (ICISC 2013), Seoul (South Korea), November 27 - 29, 2013
– 10th European Workshop on Public Key Infrastructures, Services and Applications (EuroPKI 2013), held in conjunction with the 18th European Symposium on Research in Computer Security (ESORICS 2013), London (UK), September 12 - 13, 2013
– 8th International Conference on Availability, Reliability and Security (ARES 2013), Regensburg (Germany), September 2 - 6, 2013
– 10th International Conference on Trust, Privacy & Security in Digital Business (TrustBus 2013), held in conjunction with the 24th International Conference on Database and Expert Systems Applications (DEXA 2013), Prague (Czech Republic), August 26 - 30, 2013
– 12th Annual Information Security South Africa Conference (ISSA 2013), Johannesburg (South Africa), August 14 - 16, 2013
– 10th International Conference on Security and Cryptography (SECRYPT 2013), Reykjavik (Iceland), July 29 - 31, 2013
– 7th International Conference on Information Security and Assurance (ISA 2013), Cebu (Philippines), April 26 - 28, 2013
– 4th IEEE International Conference on Cloud Computing and Science (IEEE CloudCom 2012), Security and Privacy Track, Taipei (Taiwan), December 3 - 6, 2012
– 15th International Conference on Information Security and Cryptology (ICISC 2012), Seoul (South Korea), November 28 - 30, 2012
– 8th International Conference on Information Assurance and Security (IAS 2012), São Carlos (Brazil), November 21 - 23, 2012
– 7th International Conference on Systems and Networks Communications (ICSNC 2012), Lisbon (Portugal), November 18 - 23, 2012
– 9th European PKI Workshop: Research and Applications (EuroPKI 2012), held in conjunction with the 17th European Symposium on Research in Computer Security (ESORICS 2012), Pisa (Italy), September 13 - 14, 2012
– 9th International Conference on Trust, Privacy and Security in Digital Business (TrustBus 2012) held in conjunction with the 23rd International Conference on Database and Expert Systems Applications (DEXA 2012), Vienna (Austria), September 3 - 7, 2012
– 7th International Conference on Availability, Reliability and Security (ARES 2012), Prague (Czech Republic), August 20 - 24, 2012
– 13th International Workshop on Information Security Applications (WISA 2012), Jeju Island (Korea), August 16 - 18, 2012
– 11th Annual Information Security South Africa Conference (ISSA 2012), Johannesburg (South Africa), August 15 - 17, 2012
– International Conference on Security and Cryptography (SECRYPT 2012), Rome (Italy), July 24 - 27, 2012
– International Summer FTRA Symposium on Advances in Cryptography, Security and Applications for Future Computing (FTRA ACSA 2012), Vancouver (Canada), June 26 - 28, 2012

– 9th Annual IEEE Consumer Communications & Networking Conference (CCNC 2012), Technical Track on Security and Content Protection, Las Vegas (USA), January 7 - 10, 2012

– International Conference on Security Technology (SecTech 2011), Jeju Island (Korea), December 8 - 10, 2011

– 7th International Conference on Information Assurance and Security (IAS 2011), Malacca (Malaysia), December 5 - 8, 2011

– 14th International Conference on Information Security and Cryptology (ICISC 2011), Seoul (South Korea), November 30 - December 2, 2011

– 6th International Conference on Systems and Networks Communications (ICSNC 2011), Barcelona (Spain), October 23 - 28, 2011

– 8th European Workshop on Public Key Infrastructures, Services, and Applications (EuroPKI 2011), Leuven (Belgium), September 15 - 16, 2011

– 8th International Conference on Trust, Privacy and Security in Digital Business (TrustBus 2011) held in conjunction with the 22nd International Conference on Database and Expert Systems Applications (DEXA 2011), Toulouse (France), August 29 - September 2, 2011

– 12th International Workshop on Information Security Applications (WISA 2011), Jeju Island (Korea), August 22 - 24, 2011

– 10th Annual Information Security South Africa Conference (ISSA 2011), South Africa, August 15 - 17, 2011

– 5th International Conference on Information Security and Assurance (ISA 2011), Brno University (Czech Republic), August 15 - 17, 2011

– 9th Annual Conference on Privacy, Security and Trust (PST 2011), Montreal (Canada), July 19 - 21, 2011

– International Conference on Security and Cryptography (SECRYPT 2011), Seville (Spain), July 18 - 21, 2011

– 26th IFIP International Information Security Conference (IFIP SEC 2011), Lucerne (Switzerland), June 7 - 9, 2011

– 8th Annual IEEE Consumer Communications & Networking Conference (CCNC 2011), Technical Track on Security and Content Protection, Las Vegas (USA), January 8 - 11, 2011

– International Conference on Security Technology (SecTech 2010), Jeju Island (Korea), December 13 - 15, 2010

– ISSE/SICHERHEIT 2010, Berlin (Germany), October 5 - 7, 2010

– 25th IFIP International Information Security Conference (IFIP SEC 2010), Brisbane (Australia), September 20 - 23, 2010

– 7th International Conference on Trust, Privacy and Security in Digital Business (TrustBus '10) held in conjunction with the 21st International Conference on Database and Expert Systems Applications (DEXA 2010), Bilbao (Spain), August 30 - September 3, 2010

– 11th International Workshop on Information Security Applications (WISA 2010), Jeju Island (Korea), August 24 - 26, 2010

– 6th International Conference on Information Assurance and Security (IAS 2010), Atlanta (USA), August 23 - 25, 2010
– 5th International Conference on Systems and Networks Communications (ICSNC 2010), Nice (France), August 22 - 27, 2010
– 9th Annual Information Security South Africa Conference (ISSA 2010), Johannesburg (South Africa), August 2 - 4, 2010
– International Conference on Security and Cryptography (SECRYPT 2010), Athens (Greece), July 26 - 28, 2010
– 4th International Conference on Information Security and Assurance (ISA 2010), India, June 3 - 5, 2010
– 4th Workshop in Information Security Theory and Practices (WISTP 2010), Passau (Germany), April 12 - 14, 2010
– 25th ACM Symposium on Applied Computing (SAC 2010), Technical Track on Privacy on the Web, Sierre (Switzerland), March 22 - 26, 2010
– International Conference on Security Technology (SecTech 2009), Jeju Island (Korea), December 10 - 12, 2009
– 12th Information Conference on Information Security and Cryptology (ICISC '09), Seoul (South Korea), December 2 - 4, 2009
– 4th International Conference on Systems and Networks Communications (ICSNC 2009), Porto (Portugal), September 20 - 25, 2009
– 6th European Workshop on Public Key Services, Applications and Infrastructures (EuroPKI '09), Pisa (Italy), September 9 - 11, 2009
– 3rd Workshop in Information Security Theory and Practices (WISTP 2009), Bruxelles (Belgium), September 2 - 4, 2009
– 6th International Conference on Trust, Privacy and Security in Digital Business (TrustBus '09) held in conjunction with the 20th International Conference on Database and Expert Systems Applications (DEXA 2009), Linz (Austria), August 31 - September 4, 2009
– 10th International Workshop on Information Security Applications (WISA 2009), Jeju Island (Korea), August 25 - 27, 2009
– 5th International Conference on Information Assurance and Security (IAS 2009), Xi'an (China), August 8 - 10, 2009
– International Conference on Security and Cryptography (SECRYPT 2009), Milan (Italy), July 7 - 10, 2009
– 24th IFIP International Information Security Conference (IFIP SEC 2009), Pafos (Cyprus), May 18 - 20, 2009
– 9th International Conference on Information Management (Wirtschaftsinformatik 2009), Track 21: Security, Vienna (Austria), February 25 - 27, 2009
– 11th Information Conference on Information Security and Cryptology (ICISC '08), Seoul (South Korea), December 4 - 5, 2008
– 3rd International Conference on Systems and Networks Communications (ICSNC 2008), Sliema (Malta), October 26 - 31, 2008
– 4th International Conference on Information Assurance and Security (IAS 2008), Naples (Italy), September 8 - 10, 2008

- 9th International Conference on Electronic Commerce and Web Technologies (EC-Web '08) held in conjunction with the 19th International Conference on Database and Expert Systems Applications (DEXA 2008), Turin (Italy), September 1 - 5, 2008
- 5th International Conference on Trust, Privacy and Security in Digital Business (TrustBus '08) held in conjunction with the 19th International Conference on Database and Expert Systems Applications (DEXA 2008), Turin (Italy), September 1 - 5, 2008
- International Conference on Security and Cryptography (SECRYPT 2008), Porto (Portugal), July 26 - 29, 2008
- 5th European PKI Workshop: Theory and Practice (EuroPKI '08), Trondheim (Norway), June 16 - 17, 2008
- 2nd Workshop in Information Security Theory and Practices (WISTP 2008), Sevilla (Spain), May 13 - 16, 2008
- 10th Information Conference on Information Security and Cryptology (ICISC '07), Seoul (South Korea), November 29 - 30, 2007
- International Association of Science and Technology for Development (IASTED) International Conference on Communication, Network, and Information Security (CNIS 2007), Berkeley, CA (USA), September 24 - 26, 2007
- 8th International Conference on Electronic Commerce and Web Technologies (EC-Web '07) held in conjunction with the 18th International Conference on Database and Expert Systems Applications (DEXA 2007), Regensburg (Germany), September 3 - 7, 2007
- 4th International Conference on Trust, Privacy and Security in Digital Business (TrustBus '07) held in conjunction with the 18th International Conference on Database and Expert Systems Applications (DEXA 2007), Regensburg (Germany), September 3 - 7, 2007
- 2nd International Conference on Systems and Networks Communications (ICSNC '07), Cap Esterel (France), August 25 - 31, 2007
- International Security Symposium on Information Assurance and Security (IAS '07), Manchester (UK), August 29 - 30, 2007
- International Conference on Security and Cryptography (SECRYPT 2007), Barcelona (Spain), July 28 - 31, 2007
- 4th European PKI Workshop: Theory and Practice (EuroPKI '07), Mallorca (Spain), June 28 - 30, 2007
- 9th Information Conference on Information Security and Cryptology (ICISC '06), Busan (Korea), November 30 - December 1, 2006
- 2nd International Conference on Signal-Image Technology & Internet-Based Systems (SITIS '06), Track II - Web-Based Information Technologies & Distributed Systems, Hammamet (Tunisia), December 17 - 21, 2006
- International Conference on Systems and Networks Communications (ICSNC 2006), Mini-conference on Security Systems (SESYS 2006), Tahiti (French Polynesia), November 2 - 4, 2006
- International Association of Science and Technology for Development (IASTED) International Conference on Communication, Network, and Information Security (CNIS 2006), Cambridge, MA (USA), October 9 - 11, 2006

– 3rd International Conference on Trust, Privacy and Security in Digital Business (TrustBus '06) held in conjunction with the 17th International Conference on Database and Expert Systems Applications (DEXA 2006), Krakov (Poland), September 4 - 8, 2006
– 7th International Conference on Electronic Commerce and Web Technologies (EC-Web '06) held in conjunction with the 17th International Conference on Database and Expert Systems Applications (DEXA 2006), Krakov (Poland), September 4 - 8, 2006
– 9th Information Security Conference (ISC '06), Island of Samos (Greece), August 30 - September 2, 2006
– International Conference on Security and Cryptography (SECRYPT 2006), Setúbal (Portugal), August 7 - 10, 2006
– 1st Conference on Advances in Computer Security and Forensics (ACSF), Liverpool (UK), July 13 - 14, 2006
– 4th International Conference on Applied Cryptography and Network Security (ACNS 2006), Singapore, June 6 - 9, 2006
– 20th IEEE International Conference on Advanced Information Networking and Applications (AINA 2006), Vienna (Austria), April 18 - 20, 2006
– Multikonferenz Wirtschaftsinformatik (MKWI 2006) IT-Security Track, Passau (Germany), February 20 - 22, 2006
– 8th Information Conference on Information Security and Cryptology (ICISC '05), Seoul (South Korea), December 1 - 2, 2005
– International Association of Science and Technology for Development (IASTED) International Conference on Communication, Network, and Information Security (CNIS 2005), Phoenix, AZ (USA), November 14 - 16, 2005
– International Association of Science and Technology for Development (IASTED) International Conference on Communications and Computer Networks (CCN 2005), Marina Del Rey, CA (USA), October 24 - 26, 2005
– 4th International Workshop for Applied PKI (IWAP 05), Singapore, September 21 - 23, 2005
– 8th Information Security Conference (ISC '05), Singapore, September 20 - 23, 2005
– 2nd International Conference on Trust, Privacy, and Security in Digital Business (TrustBus '05) held in conjunction with the 16th International Conference on Database and Expert Systems Applications (DEXA 2005), Copenhagen (Denmark), August 22 - 26, 2005
– 6th International Conference on Electronic Commerce and Web Technologies (EC-Web '05) held in conjunction with the 16th International Conference on Database and Expert Systems Applications (DEXA 2005), Copenhagen (Denmark), August 22 - 26, 2005
– 2nd European PKI Workshop on Research and Applications, Kent (UK), June 30 - July 1, 2005
– IEEE GLOBECOM 2004 Symposium on Security and Network Management, Dallas, TX (USA), November 29 - December 3, 2004

- 1st International Conference on Trust and Privacy in Digital Business (TrustBus '04) held in conjunction with the 15th International Conference on Database and Expert Systems Appliactions (DEXA 2004), Zaragoza (Spain), August 30 - September 3, 2004
- 5th International Conference on Electronic Commerce and Web Technologies (EC-Web 2004) held in conjunction with the 15th International Conference on Database and Expert Systems Appliactions (DEXA 2004), Zaragoza (Spain), August 30 - September 3, 2004
- International Association for Development of the Information Society (IADIS) e-Society Conference, Spain, July 16 - 19, 2004
- 1st European PKI Workshop on Research and Applications, Samos Island (Greece), June 25 - 26, 2004
- International Association of Science and Technology for Development (IASTED) International Conference on Communication, Network, and Information Security (CNIS 2003), New York, NY (USA), December 10 - 12, 2003
- 1st MiAn International Conference on Applied Cryptography and Network Security (ACNS 2003), Kunming (China), October 16 - 19, 2003
- International Workshop on Trust and Privacy in Digital Business (TrustBus '03) held in conjunction with the 14th International Conference on Database and Expert Systems Appliactions (DEXA 2003), Prague (Czech Republic), September 1 - 5, 2003
- 4th International Conference on Electronic Commerce and Web Technologies (EC-Web 2003) held in conjunction with the 14th International Conference on Database and Expert Systems Appliactions (DEXA 2003), Prague (Czech Republic), September 1 - 5, 2003
- International Association for Development of the Information Society (IADIS) e-Society Conference, Lisabon (Portugal), June 3 - 6, 2003
- International Workshop on Trust and Privacy in Digital Business (TrustBus '02) held in conjunction with the 13th International Conference on Database and Expert Systems Appliactions (DEXA 2002), Aix-en-Provence (France), September 2 - 6, 2002
- 3rd International Conference on Electronic Commerce and Web Technologies (EC-Web 2002) held in conjunction with the 13th International Conference on Database and Expert Systems Appliactions (DEXA 2002), Aix-en-Provence (France), September 2 - 6, 2002
- 2nd International Conference on Electronic Commerce and Web Technologies (EC-Web 2001) held in conjunction with the 12th International Conference on Database and Expert Systems Appliactions (DEXA 2001), Munich (Germany), September 4 - 6, 2001
- Workshop on Security in Media Data held in conjunction with the GI Conference "Informatik 2000," Berlin (Germany), September 19 - 22, 2000
- 1st International Conference on Electronic Commerce and Web Technologies (EC-Web 2000) held in conjunction with the 11th International Conference on Database and Expert Systems Appliactions (DEXA 2000), Greenwich (UK), September 4 - 6, 2000
- Research Workshop on Security and Electronic Commerce (WSSEC 2000), Darmstadt (Germany), March 23 - 24, 2000

- IFIP TC6 and TC11 Joint Working Conference on Communications and Multimedia Security (CMS '99), Leuven (Belgium), September 20 - 21, 1999
- Workshop on Security and Electronic Commerce held in conjunction with the 10th International Conference on Database and Expert Systems Appliactions (DEXA '99), Florence (Italy), August 30 - September 3, 1999
- Workshop on Security in Large-Scale Distributed Systems held in conjunction with the IEEE Symposium on Reliable Distributed Systems, Purdue University, West Lafayette, IN (USA), October 20 - 23, 1998
- IFIP TC6 and TC11 Joint Working Conference on Communications and Multimedia Security (CMS '97), Athens (Greece), September 22 - 23, 1997

- Reviewer
  - Conferences and Workshops
    * 8th Annual Information Security South Africa Conference (ISSA 2009), Johannesburg (South Africa), July 6 - 8, 2009
    * 7th Annual Information Security South Africa Conference (ISSA 2008), Johannesburg (South Africa), July 7 - 9, 2008
    * 6th Annual Information Security South Africa Conference (ISSA 2006), Johannesburg (South Africa), July 5 - 7, 2006
    * 5th Annual Information Security South Africa Conference (ISSA 2005), Johannesburg (South Africa), June 29 - July 1, 2005
    * 4th Annual Information Security South Africa Conference (ISSA 2004), Johannesburg (South Africa), June 30 - July 2, 2004
    * 19th Annual Computer Security Applications Conference (ACSAC 2003), Las Vegas, NV, December 8 - 12, 2003
    * 18th Annual Computer Security Applications Conference (ACSAC 2002), Las Vegas, NV, December 9 - 13, 2002
    * 17th Annual Computer Security Applications Conference (ACSAC 2001), New Orleans, LA, December 10 - 14, 2001
    * 8th Annual IFIP TC 11 Working Conference on Information Security Management & Small Systems Security, Las Vegas, NV, September 27 - 28, 2001
    * 16th Annual Computer Security Applications Conference (ACSAC 2000), New Orleans, LA, December 11 - 15, 2000
    * IFIP TC 11 International Conference on Information Security (IFIP SEC 2000), Bejing, China, August 21 - 25, 2000
    * 15th Annual Computer Security Applications Conference (ACSAC '99), Scottsdale, AZ, December 6 - 10, 1999
    * 14th Annual Computer Security Applications Conference (ACSAC '98), Scottsdale, AZ, December 7 - 11, 1998
    * 13th Annual Computer Security Applications Conference (ACSAC '97), San Diego, CA, December 8 - 12, 1997
    * 12th Annual Computer Security Applications Conference (ACSAC '96), San Diego, CA, December 9 - 13, 1996
  - Book Publishers
    * John Wiley & Sons, New York, NY

- Journals and Magazines
  - ACM Computing Surveys
  - ACM Transactions on Computer Systems (TOCS)
  - Applied Computing and Informatics
  - Autonomous Agents and Multi-Agent Systems
  - Communications of the ACM (CACM)
  - Computer Communications
  - Computer Journal
  - Computer Standards & Interfaces
  - Computers & Security
  - Electronic Commerce Research
  - EURASIP Journal on Information Security
  - EURASIP Journal on Wireless Communications and Networking
  - IBM Systems Journal
  - IEEE/ACM Transactions on Networking
  - IEEE Computer
  - IEEE Internet Computing
  - IEEE Security & Privacy
  - IEEE Transactions on Dependable and Secure Computing (TDSC)
  - IEEE Transactions on Mobile Computing (TMC)
  - IET Information Security
  - Information Sciences
  - International Journal of Computers and Applications
  - International Journal of Information Security (IJIS)
  - Journal of Computer Security
  - Journal of Network and Computer Applications
  - Journal of Systems and Software
  - Software Practice & Experience

8 Tutorials

- Oppliger, R., *Sicherheit im E-Commerce*, half-day tutorial held at the 5th Conference on "Sicherheit in Informationssystemen" (SIS 2002), Vienna (Austria), October 3 - 4, 2002
- Oppliger, R., *Java Security APIs: What is Going on Behind the Scenes?* half-day tutorial held at the 16th European Conference on Object-Oriented Programming (ECOOP 2002), Málaga (Spain), June 10 - 14, 2002
- Oppliger, R., *Security Technologies for the World Wide Web*, full-day tutorial held at the 17th Annual Computer Security Applications Conference (ACSAC 2001), New Orleans, LA, December 10 - 14, 2001
- Oppliger, R., *Web Security*, full-day tutorial held at the 15th Annual Computer Security Applications Conference (ACSAC '99), Scottsdale, AZ, December 6 - 10, 1999
- Oppliger, R., *Securing the Internet*, full-day tutorial held at the Internet Society Internet Networking Conference (INET '99), San Jose, CA, June 22 - 25, 1999

- Oppliger, R., *Sicherheit im Internet*, half-day tutorial held at the 11th ITG/VDI Conference on "Kommunikation in Verteilten Systemen" (KiVS '99), Darmstadt (Germany), March 2 - 5, 1999
- Oppliger, R., *Security in TCP/IP-based Networks*, full-day tutorial held at the 14th Annual Computer Security Applications Conference (ACSAC '98), Scottsdale, AZ, December 7 - 11, 1998
- Oppliger, R., *Internet and Intranet Security*, full-day tutorial held at the 13th Annual Computer Security Applications Conference (ACSAC '97), San Diego, CA, December 8 - 12, 1997
- Oppliger, R., *Security Protocols for the Internet*, full-day tutorial held at the 12th Annual Computer Security Applications Conference (ACSAC '96), San Diego, CA, December 9 - 13, 1996
- Oppliger, R., *Sicherheit im Internet*, half-day tutorial held at the 2nd Conference on "Sicherheit in Informationssystemen" (SIS '96), Vienna (Austria), March 21 - 22, 1996
- Oppliger, R., *Authentication and Key Distribution Systems*, half-day tutorial held at the 11th Annual Computer Security Applications Conference (ACSAC '95), New Orleans, LA, December 11 - 15, 1995

9 Invited Talks

- Oppliger, R., *SSL/TLS Angriffe und Gegenmassnahmen*, Bern University of Applied Sciences, Biel (Switzerland), June 9, 2017
- Oppliger, R., *SSL/TLS: Playing "Cops and Robbers" on the Internet*, University of Florida, Gainesville, FL (USA), July 25, 2016
- Oppliger, R., *State-of-the-Art in Information Security*, University of Houston, Houston, TX (USA), July 20, 2016
- Oppliger, R., *SSL/TLS: Angriffe und Gegenmassnahmen*, Beer-Talk at Compass Security Schweiz AG (Switzerland), May 26, 2016 (Berne) and June 9, 2016 (Jona)
- Oppliger, R., *Certification Authorities Under Attack: A Plea for Certificate Legitimation*, University of Lausanne (Switzerland), April 18, 2016
- Oppliger, R., *Information Security: Key Concepts and Common Misconceptions*, Imperial College London (United Kingdom), April 11, 2014
- Oppliger, R., *SSL/TLS Session-Aware User Authentication Against Man-In-The-Middle (MITM) Attacks*, Technical University of Lisbon (Portugal), April 10, 2013
- Oppliger, R., *Geld im digitalen Zeitalter: Eine Standortbestimmung*, University of Zurich (Switzerland), October 17, 2012
- Oppliger, R., *Sicherheit — die Herausforderungen beim Outsourcing*, Symposium on Privacy and Security, Zurich (Switzerland), August 29, 2012
- Oppliger, R., *SSL/TLS and Web Application (In-)Security*, HEIG-VD IT Security Days, Yverdon-les-Bains (Switzerland), March 16, 2011

- Oppliger, R., *Der Client als Achillesferse beim Remote Internet Voting*, Swiss E-Voting Workshop, Murten (Switzerland), June 5, 2009
- Oppliger, R., *Digital Signatures: From Theory to Practice*, ZISC Information Security Colloquium, Zurich (Switzerland), June 14, 2005
- Oppliger, R., *Digitale Dokumente: Alte und neue Herausforderungen sowie Lösungsansätze*, Tagung für Informatik und Recht, Bern (Switzerland), October 26, 2004
- Oppliger, R., *Internet Banking — Aktuelle Bedrohungen und Risiken*, Trüb PKI Fachtagung "Internetbanking mit Smartcards," Aarau (Switzerland), September 1, 2004
- Oppliger, R., *Digitale Evidenz: Zwischen Traum und Wirklichkeit*, Swiss Infosec Tagung, Kloten (Switzerland), October 29 - 31, 2003
- Oppliger, R., *Beweiskraft von digitalen Signaturen: Traum und Wirklichkeit*, University of Regensburg, Regensburg (Germany), May 9, 2003
- Oppliger, R., *Informatiksicherheit und die Jagd nach dem heiligen Gral*, IT-Stammtisch Regensburg in collaboration with the German Informatics Society (GI), Regensburg (Germany), May 8, 2003
- Oppliger, R., *IT Security: Empowering or Policing Employees*, Microsoft CIO Forum, Neuchâtel (Switzerland), June 18 - 21, 2002
- Oppliger, R., *Authentifizierungs- und Autorisierungsinfrastrukturen für Computernetze und verteilte Systeme*, University of Fribourg, Fribourg (Switzerland), March 7, 2002
- Oppliger, R., *Public Key Infrastrukturen und digitale Signaturen: Wo stehen wir?* Swiss Society of Administration Sciences, Bern (Switzerland), November 15 - 16, 2001
- Oppliger, R., *PKI: Current Situation and Future Prospects*, Symposium on Privacy and Security, Zurich (Switzerland), November 1 - 2, 2001
- Oppliger, R., *Public Key Infrastrukturen und digitale Signaturen: Wo stehen wir?* University of St. Gallen, St. Gallen (Switzerland), June 28, 2001
- Oppliger, R., *PKI: Ein Tanz um das goldene Kalb?* FGSec Conference on "Public Key Infrastructure — Möglichkeiten und Nutzen", Zurich (Switzerland), March 28, 2001
- Oppliger, R., *Authentication and Authorization Infrastructures: Kerberos vs. PKI*, SWITCH Workshop on Authentication and Authorization Infrastructures (AAIs), Gerzensee (Switzerland), November 20 - 21, 2000
- Oppliger, R., *Informatiksicherheit: Quo vadis?* 4th Conference on "Sicherheit in Informationssystemen" (SIS 2000), Zurich (Switzerland), October 5 - 6, 2000
- Oppliger, R., *Sicherheitsfragen im E-Business*, 30th SOUG Conference on "E-Business: Management, Security & Availability", Zurich (Switzerland), September 7, 2000
- Oppliger, R., *Internet Security: State-of-the-art and Missing Pieces*, ETH/IBM Colloquium on Information Security, Zurich (Switzerland), June 15, 2000
- Oppliger, R., *Public Key Infrastrukturen (PKI) in Theorie und Praxis*, TelNetCom 2000, Zurich (Switzerland), June 6, 2000

- Oppliger, R., *Elektronische Zahlungssysteme*, University GH Essen, Essen (Germany), April 18, 2000
- Oppliger, R., *Informatiksicherheit: Herausforderungen heute und morgen*, University of Zurich (Switzerland), October 25, 1999
- Oppliger, R., *Shaping the Research Agenda for Security in Electronic Commerce*, Workshop on Security and Electronic Commerce held in conjunction with the 10th International Workshop on Database and Expert Systems (DEXA '99), Florence (Italy), September 1 - 3, 1999
- Oppliger, R., *Security in Electronic Commerce*, International Computer Science Institute (ICSI), Berkeley, CA, June 22, 1999
- Oppliger, R., *Internet Security Protocols*, Computer Security Institute NetSec '99 Conference, St. Louis, MO, June 14 - 16, 1999
- Oppliger, R., *Managing Certificates in a Corporate Environment*, Computer Security Institute NetSec '99 Conference, St. Louis, MO, June 14 - 16, 1999
- Oppliger, R., *Security Issues related to Mobile Code and Agent-based Systems*, Computer Security Institute NetSec '99 Conference, St. Louis, MO, June 14 - 16, 1999
- Oppliger, R., *Braucht das Internet Ressourcen-Reservationsschemata?* University of Zurich (Switzerland), January 20, 1999
- Oppliger, R., *Anonymität im World Wide Web — Technische Lösungsansätze für das anonyme Browsen und Publizieren im WWW*, University GH Essen, Essen (Germany), November 26, 1998
- Oppliger, R., *Sichere Kommunikation in vernetzten und verteilten Systemen*, Lecture Series on "Informationstechnik und Armee", ETH Zurich (Switzerland), January 7, 1998
- Oppliger, R., *Das Internet, Möglichkeiten und Herausforderungen eines Informationssuperhighway*, Münchenwiler-Tagung of the Collegium Generale, University of Bern (Switzerland), May 2 - 3, 1997
- Oppliger, R., *Communication security on the internet/intranet*, ISACA Switzerland Internet Series 97, Zurich (Switzerland), April 23, 1997
- Oppliger, R., *Das Internet — Möglichkeiten und Herausforderungen eines Information Superhighway*, University GH Essen, Essen (Germany), January 15, 1997
- Oppliger, R., *Sicherheit im Internet*, Swiss Association for the Security of Information Services (CLUSIS) Meeting on "Sicherheit und Gefahren des Internet," Zurich (Switzerland), November 21, 1996
- Oppliger, R., *Sicherheit im Intranet*, 4th International Management Forum "Intranet - Groupware - Workflow", Zurich-Regensdorf (Switzerland), November 13 - 14, 1996
- Oppliger, R., *Sicherheit im Internet*, Annual Meeting COMMON Switzerland (AC-CH '96), Bern (Switzerland), September 11 - 12, 1996
- Oppliger, R., *Distributed Registration and Key Distribution (DiRK)*, ICSI-Alumni e.V. Meeting, Karlsruhe (Germany), May 14 - 15, 1996

- Oppliger, R., *Authentication and Key Distribution Systems*, 4th Annual RSA Data Security Conference, Redwood Shores, CA, January 9 - 11, 1995

- Oppliger, R., *Sicherheitskonzepte für ein Kommunikationsnetz der Bundesverwaltung*, UNIGS (UNIX Interessengemeinschaft Schweiz) Spring Meeting, Zurich (Switzerland), April 14, 1994

10 Panel Discussions

- Pernul, G. (moderator), Casassa-Mont, M., Fernández, E.B., Katsikas, S.K., Kobsa, A., and R. Oppliger, *Managing Digital Identities - Challenges and Opportunities*, 4th International Conference on Trust, Privacy and Security in Digital Business (TrustBus '07) held in conjunction with the 18th International Conference on Database and Expert Systems Applications (DEXA 2007), Regensburg (Germany), September 4, 2007

- Böhm, A., Meierhans, D. (moderator), Noser, R., Oppliger, R., Roncaglioni, E., Rosenast, C., and Senn, D., *ELM und PKI - Wie soll der Amtsverkehr elektronisch werden?* Topsoft '07, Bern (Switzerland), March 7, 2007

11 Patents

- Oppliger, R., and P. Stadlin, *Verfahren und Vorrichtung zur Erbringung von temporal authentifizierten Versand- und Empfangsbestätigungen in einem elektronischen Nachrichtenvermittlungssystem*, CH 698115B1, May 29, 2009

- Oppliger, R., and P. Stadlin, *Verfahren zur Erbringung von Empfangsbestätigungen für die Umsetzung von "eingeschriebenen Nachrichten" in einem elektronischen Nachrichtenvermittlungssystem*, CH 695844A5, September 15, 2006

- Oppliger, R., and A. Albanese, *Distributed Registration and Key Distribution System and Method*, US 6002768, December 14, 1999

12 Publications

12.1 Books

- Oppliger, R., *SSL/TLS: Theory and Practice, Second Edition*, ISBN 978-1-60807-998-8, Artech House Publishers, Norwood, MA, 2016

- Oppliger, R., *Secure Messaging on the Internet*, ISBN 978-1-60807-717-5, Artech House Publishers, Norwood, MA, 2014

- Oppliger, R., *Contemporary Cryptography, Second Edition*, ISBN 978-1-60807-145-6, Artech House Publishers, Norwood, MA, 2011

- Oppliger, R., *SSL/TLS: Theory and Practice*, ISBN 978-1-59693-447-4, Artech House Publishers, Norwood, MA, 2009

- Oppliger, R., *Contemporary Cryptography*, ISBN 978-1-58053-642-4, Artech House Publishers, Norwood, MA, 2005

- Oppliger, R., *Security Technologies for the World Wide Web, Second Edition*, ISBN 978-1-58053-348-5, Artech House Publishers, Norwood, MA, 2003
- Oppliger, R., *Internet and Intranet Security, Second Edition*, ISBN 978-1-58053-166-5, Artech House Publishers, Norwood, MA, 2002
- Oppliger, R., *Secure Messaging with PGP and S/MIME*, ISBN 978-1-58053-161-0, Artech House Publishers, Norwood, MA, 2001
- Oppliger, R., *Security Technologies for the World Wide Web*, ISBN 978-1-58053-045-3, Artech House Publishers, Norwood, MA, 2000 (tanslated into Chinese)
- Oppliger, R., *Internet and Intranet Security*, ISBN 978-0-89006-829-8, Artech House Publishers, Norwood, MA, 1998
- Oppliger, R., *IT-Sicherheit — Grundlagen und Umsetzung in der Praxis*, ISBN 978-3-52805-566-0, DuD Fachbeiträge, Friedr. Vieweg & Sohn Verlagsgesellschaft mbH, Wiesbaden (Germany), 1997
- Oppliger, R., *Authentication Systems for Secure Networks*, ISBN 978-0-89006-510-5, Artech House Publishers, Norwood, MA, 1996 (translated into Spanish)
- Oppliger, R., and Ph. J. Stüssi, *Unternehmensweite Kommunikationsnetze*, ISBN 978-3-52805-423-6, Friedr. Vieweg & Sohn Verlagsgesellschaft mbH, Wiesbaden (Germany), 1994
- Oppliger, R., *Computersicherheit — Eine Einführung*, ISBN 978-3-52805-296-6,Friedr. Vieweg & Sohn Verlagsgesellschaft mbH, Wiesbaden (Germany), 1992

12.2 Book Chapters

- Oppliger, R., *Geld im digitalen Zeitalter — Eine Standortbestimmung*, In: Baer, J., and W. Rother (Eds.), "Geld - Philosophische, literaturwissenschaftliche und ökonomische Perspektiven," ISBN 978-3-7965-2913-9, Schwabe Verlag, Basel (Switzerland), 2013, pp. 187–207
- Oppliger, R., *Network Security*, In: Proakis, J.G. (Ed.), "Wiley Encyclopedia of Telecommunications," Vol. 3, ISBN 978-0471369721, John Wiley & Sons, New York, NY, 2003, pp. 1644–1652
- Oppliger, R., *Datenschutzfreundliche Technologien für das World Wide Web (WWW)*, In: Baeriswil, B., and B. Rudin (Eds.), "Perspektive Datenschutz — Praxis und Entwicklungen in Recht und Technik," ISBN 978-3725543298, Schulthess Juristische Medien AG, Zurich (Switzerland), 2002, pp. 295–326

12.3 Academic Theses

- Oppliger, R., *Contributions to Research in Network Security*, Habilitation thesis (Habilitationsschrift), Department of Computer Science, Faculty of Economical Sciences, University of Zurich (Switzerland), January 1999
- Oppliger, R., *Analyse und Entwurf von unternehmensweiten Kommunikationsnetzen*, Ph.D. thesis (Dissertation), Institute for Computer Science and Applied Mathematics (IAM), Faculty of Natural Sciences, University of Bern (Switzerland), June 1993 (supervised by Prof. Dr. D. Hogrefe)

- Oppliger, R., *Computersicherheit*, M.Sc. thesis (Diplomarbeit), Institute for Computer Science and Applied Mathematics (IAM), Faculty of Natural Sciences, University of Bern (Switzerland), May 1991 (supervised by Prof. Dr. D. Hogrefe)

12.4 Refereed Articles

- Oppliger, R., *Disillusioning Alice and Bob*, IEEE Security & Privacy, Vol. 15, No. 5, September/October 2017, pp. 82–84
- Oppliger, R., Pernul, G., and S. Katsikas, *Guest Editor's Introduction — New Frontiers: Assessing and Managing Security Risks*, IEEE Computer, Vol. 50, No. 4, April 2017, pp. 48–51
- Oppliger, R., *Quantitative Risk Analysis in Information Security Management: A Modern Fairy Tale*, IEEE Security & Privacy, Vol. 13, No. 6, November/December 2015, pp. 18–21
- Oppliger, R., *Certification Authorities Under Attack: A Plea for Certificate Legitimation*, IEEE Internet Computing, Vol. 18, No. 1, January/February 2014, pp. 40–47
- Oppliger, R., and B. Wildhaber, *Common Misconceptions in Computer and Information Security*, IEEE Computer, Vol. 45, No. 6, June 2012, pp. 102–104
- Oppliger, R., *Guest Editor's Introduction — Security and Privacy in an Online World*, IEEE Computer, Vol. 44, No. 9, September 2011, pp. 21–22
- Oppliger, R., Rytz, R., and T. Holderegger, *Internet Banking: Client-Side Attacks and Protection Mechanisms*, IEEE Computer, Vol. 42, No. 6, June 2009, pp. 27–33
- Oppliger, R., Hauser, R., and D. Basin, *SSL/TLS Session-Aware User Authentication Revisited*, Computers & Security, Vol. 27, Issues 3–4, May/June 2008, pp. 64–70
- Oppliger, R., and R. Hauser, *Protecting TLS-SA Implementations for the Challenge-Response Feature of EMV-CAP Against Challenge Collision Attacks*, Security and Communication Networks, Vol. 1, Issue 2, March/April 2008, 125–134
- Oppliger, R., Hauser, R., and D. Basin, *SSL/TLS Session-Aware User Authentication*, IEEE Computer, Vol. 41, No. 3, March 2008, pp. 59–65
- Oppliger, R., *IT Security: In Search of the Holy Grail*, Communications of the ACM, Vol. 50, No. 2, February 2007, pp. 96–98
- Oppliger, R., *Providing Certified Mail Services on the Internet*, IEEE Security & Privacy, Vol. 5, No. 1, January/February 2007, pp. 16–22
- Oppliger, R., Hauser, R., and D. Basin, *SSL/TLS session-aware user authentication—Or how to effectively thwart the man-in-the-middle*, Computer Communications, Vol. 29, Issue 12, August 2006, pp. 2238–2246
- Lopez, J., Oppliger, R., and G. Pernul, *Why have public key infrastructures failed so far?* Internet Research, Vol. 15, No. 5, October 2005, pp. 544–556
- Oppliger, R., *Privacy-enhancing technologies for the world wide web*, Computer Communications, Vol. 28, Issue 16, 2005, pp. 1791–1797

- Oppliger, R., and R. Rytz, *Does Trusted Computing Remedy the Computer Security Problems?* IEEE Security & Privacy, Vol. 3, No. 2, March/April 2005, pp. 16–19
- Lopez, J., Oppliger, R., and G. Pernul, *Authentication and authorization infrastructures (AAIs): a comparative survey*, Computers & Security, Vol. 23, Issue 7, October 2004, pp. 578–590
- Oppliger, R., *Certified Mail: The Next Challenge for Secure Messaging*, Communications of the ACM, Vol. 47, No. 8, August 2004, pp. 75–79
- Oppliger, R., and P. Stadlin, *A certified mail system (CMS) for the Internet*, Computer Communications, Vol. 27, Issue 13, August 2004, pp. 1229–1235
- Oppliger, R., *Microsoft .NET Passport and identity management*, Information Security Technical Report, Vol. 9, No. 1, 2004, pp. 26–34
- Oppliger, R., *Sicherheit von Open Source Software - Mythos oder Wirklichkeit?* Datenschutz und Datensicherheit (DuD), Vol. 27, No. 11, November 2003, pp. 669–675
- Oppliger, R., and R. Rytz, *Digital Evidence: Dream and Reality*, IEEE Security & Privacy, Vol. 1, No. 5, September/October 2003, pp. 44–48
- Oppliger, R., *Microsoft .NET Passport: A Security Analysis*, IEEE Computer, Vol. 36, No. 7, July 2003, pp. 29–35
- Oppliger, R., *Microsoft Outlook Web Access: Blessing or Bane to Security?* IEEE IT Professional, Vol. 5, No. 1, January/February 2003, pp. 27–31
- Oppliger, R., *Managing certificates in a corporate environment*, Annals of telecommunications, Vol. 55, No. 7-8, July/August 2000, pp. 341–351
- Oppliger, R., *Privacy protection and anonymity services for the world wide web (WWW)*, Future Generation Computer Systems (FGCS) Journal, Vol. 16, Issue 4, February 2000, pp. 379–391
- Oppliger, R., *Security issues related to mobile code and agent-based systems*, Computer Communications, Vol. 22, Issue 12, July 1999, pp. 1165–1170
- Oppliger, R., *Security at the Internet Layer*, IEEE Computer, Vol. 31, No. 9, September 1998, pp. 43–47
- Oppliger, R., *Sicherheitsprotokolle für das Internet*, Datenschutz und Datensicherheit (DuD), Vol. 21, No. 12, December 1997, pp. 686–690
- Oppliger, R., and A. Albanese, *Participants Registration, Validation, and Key Distribution for large-scale Conferencing Systems*, IEEE Communications, Vol. 35, No. 6, June 1997, pp. 130–135
- Oppliger, R., *Internet Security: Firewalls and Beyond*, Communications of the ACM, Vol. 40, No. 5, May 1997, pp. 92–102
- Oppliger, R., *Internet Kiosk: Internet security enters the Middle Ages*, IEEE Computer, Vol. 28, No. 10, October 1995, pp. 100–101
- Oppliger, R., and D. Hogrefe, *Sicherheit in unternehmensweiten Kommunikationsnetzen (CCN)*, Praxis der Informationsverarbeitung und Kommunikation (PIK), Vol. 15, No. 4, 1992, pp. 213–217

12.5 Conference and Workshop Papers

- Oppliger, R., Schwenk, J., and C. Loehr, *CAPTCHA-based Code Voting*, Proceedings of the 3rd International Conference on Electronic Voting 2008 (EVOTE08), Bregenz (Austria), August 6 - 9, 2008

- Oppliger, R., Schwenk, J., and J. Helbach, *Protecting Code Voting Against Vote Selling*, Proceedings of the GI Conference on "Sicherheit, Schutz und Zuverlässigkeit" (Sicherheit 2008), Saarbrücken (Germany), Springer-Verlag, Berlin, April 2 - 4, 2008

- Oppliger, R., Hauser, R., Basin, D., Rodenhaeuser, A., and B. Kaiser, *A Proof of Concept Implementation of SSL/TLS Session-Aware User Authentication (TLS-SA)*, Proceedings of the 15th GI/ITG Conference on "Kommunikation in Verteilten Systemen" (KiVS '07), Bern (Switzerland), Springer-Verlag, Berlin, February 26 - March 2, 2007, pp. 225–236

- Oppliger, R., Gajek, S., and R. Hauser, *Security of Microsoft's Identity Metasystem and CardSpace*, Proceedings of the 15th GI/ITG Conference on "Kommunikation in Verteilten Systemen" (KiVS '07), Industry Track, Bern (Switzerland), VDE Verlag, Berlin, February 26 - March 2, 2007, pp. 63–74

- Oppliger, R., Hauser, R., and D. Basin, *Browser Enhancements to Support SSL/TLS Session-Aware User Authentication*, Position paper, W3C Workshop on Transparency and Usability of Web Authentication, New York, NY, March 15 - 16, 2006

- Oppliger, R., and S. Gajek, *Effective Protection Against Phishing and Web Spoofing*, Proceedings of the 9th IFIP TC6 and TC11 Conference on Communications and Multimedia Security (CMS 2005), Salzburg (Austria), Springer-Verlag, LNCS 3677, September 19 - 21, 2005, pp. 32–41

- Lopez, J., Oppliger, R., and G. Pernul, *Classifying Public Key Certificates*, Proceedings of the 2nd European PKI Workshop, Canterbury (UK), Springer-Verlag, LNCS 3545, June 30 - July 1, 2005, pp. 135–143

- Lopez, J., Montenegro, J.A., Oppliger, R., and G. Pernul, *On a Taxonomy of Systems for Authentication and/or Authorization Services*, Proceedings of the TERENA Networking Conference, Rhodes (Greece), June 7 - 10, 2004

- Oppliger, R., *How to Address the Secure Platform Problem for Remote Internet Voting*, Proceedings of the 5th Conference on "Sicherheit in Informationssystemen" (SIS 2002), Vienna (Austria), October 3 - 4, 2002, vdf Hochschulverlag, pp. 153–173

- Oppliger, R., Pernul, G., and Ch. Strauss, *Using Attribute Certificates to Implement Role-based Authorization and Access Control*, Proceedings of the 4th Conference on "Sicherheit in Informationssystemen" (SIS 2000), Zurich (Switzerland), October 5 - 6, 2000, vdf Hochschulverlag, pp. 169–184

- Oppliger, R., Greulich, A., and P. Trachsel, *A Distributed Certificate Management System (DCMS) Supporting Group-based Access Controls*, Proceedings of the 15th Annual Computer Security Applications Conference, Scottsdale, AZ, December 6 - 10, 1999, IEEE Computer Society Press, Los Alamitos, CA, pp.241–248

- Oppliger, R., *Authorization Methods for E-Commerce Applications*, Proceedings of the 18th Symposium on Reliable Distributed Systems (SRDS '99), International Workshop

on Electronic Commerce, Lausanne (Switzerland), October 19 - 22, 1999, IEEE Computer Society Press, Los Alamitos, CA, pp. 366–371

- Oppliger, R., Greulich, A., and P. Trachsel, *Der Einsatz eines verteilten Zertifikat-Managementsystems in der Schweizerischen Bundesverwaltung*, Proceedings of the German Informatics Society (GI) Working Conference on "Verlässliche IT-Systeme" (VIS '99), Essen (Germany), September 22 - 24, 1999, DuD Fachbeiträge, Friedr. Vieweg & Sohn Verlagsgesellschaft mbH, Wiesbaden (Germany), pp. 81–96

- Oppliger, R., *Protecting key exchange and management protocols against resource clogging attacks*, Proceedings of the IFIP TC6 and TC11 Joint Working Conference on Communications and Multimedia Security (CMS '99), Leuven (Belgium), September 20 - 21, 1999, Kluwer Academic Publishers, pp. 163–175

- Oppliger, R., *Shaping the Research Agenda for Security in E-Commerce*, Proceedings of the Workshop on Security and Electronic Commerce held in conjunction with the 10th International Conference on Database and Expert Systems Applications (DEXA '99), Florence (Italy), August 30 - September 3, 1999, IEEE Computer Society Press, Los Alamitos, CA, pp. 810–814

- Oppliger, R., and J.L. Nottaris, *Online Casinos*, Proceedings of the GI/ITG Conference on "Kommunikation in Verteilten Systemen" (KiVS '97), Braunschweig (Germany), February 17 - 22, 1997, Springer-Verlag, Berlin, pp. 2–16

- Oppliger, R., *Participants Registration, Validation, and Key Distribution for MBone Conferencing*, Swiss Computer Science Conference (SCSC '96), Zurich (Switzerland), October 22 - 23, 1996

- Oppliger, R., Bracher, M., and A. Albanese, *Distributed registration and key distribution for online universities*, Proceedings of the IFIP TC6 and TC11 Joint Working Conference on Communications and Multimedia Security (CMS '96), Essen (Germany), September 23 - 24, 1996, Chapman & Hall, London, pp. 166–175

- Oppliger, R., and A. Albanese, *Distance Education and Online Universities*, Proceedings of the 5th IEEE Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises (WET ICE '96), Workshop on Distance Learning, Stanford University (USA), June 19 - 21, 1996, IEEE Computer Society Press, Los Alamitos, CA, pp. 10–15

- Oppliger, R., and A. Albanese, *Distributed registration and key distribution (DiRK)*, Proceedings of the 12th International Conference on Information Security (IFIP SEC '96), Island of Samos (Greece), May 21 - 24, 1996, Chapman & Hall, London, pp. 199–208

- Oppliger, R., Gupta, A., Moran, M., and R. Bettati, *A Security Architecture for Tenet Scheme 2*, Proceedings of the 2nd European Workshop on Interactive Distributed Multimedia Systems and Services (IDMS '96), Berlin (Germany), March 4 - 6, 1996, Springer-Verlag, Berlin, LNCS 1045, pp. 163–174

- Oppliger, R., *Authentication and key distribution in computer networks and distributed systems*, Proceedings of the IFIP TC6, TC11 and Austrian Computer Society Joint Working Conference on Communications and Multimedia Security (CMS '95), Graz (Austria), September 20 - 21, 1995, Chapman & Hall, London, pp. 148–159

- Oppliger, R., *Authentifikations- und Schlüsselverteilsysteme*, Proceedings of the 1st Joint Conference of the German Informatics Society and the Swiss Informaticians Society (GISI '95), Zurich (Switzerland), September 18 - 20, 1995, Springer-Verlag, Berlin, pp. 266–273

- Oppliger, R., and D. Hogrefe, *Security Concepts for Corporate Networks*, Proceedings of the 10th International Conference on Information Security (IFIP SEC '94), Curaçao (N.A.), May 23 - 27, 1994

- Oppliger, R., and D. Hogrefe, *Corporate Network Security*, Proceedings of the IEEE Singapore International Conference on Networks and International Conference on Information Engineering (SICON/ICIE '93), Singapore, September 6 - 11, 1993, pp. 426–430

- Oppliger, R., Weber, S., and D. Hogrefe, *Entwurf von virtuell privaten Netzen*, Proceedings of the GI/ITG Conference on "Kommunikation in Verteilten Systemen" (KiVS '93), Munich (Germany), March 3 - 5, 1993, Springer-Verlag, Berlin, pp. 428–441

- Oppliger, R., Weber, S., and D. Hogrefe, *An Optimization Method for Virtual Private Network Design*, Proceedings of the IEE 2nd International Conference on Private Switching Systems and Networks, London (UK), June 23 - 25, 1992, pp. 31–36

12.6 Other Articles

- Oppliger, R., *Vorsicht, Verwundbarkeit!*, return, 01/18, pp. 63–65

- Oppliger, R., *SSL/TLS: Attacks, Countermeasures, and Counterattacks*, PenTest Magazine, 09/2017, pp. 152–159

- Oppliger, R., *TLS security: Past, present and future*, Help Net Security, July 3, 2017

- Oppliger, R., *Public-Key-Infrastrukturen*, digma, Vol. 15, No. 2, August 2015, pp. 58–59

- Oppliger, R., *IT-Sicherheit und Privacy (Editorial)*, hitech, Bern University of Applied Sciences, No. 2, 2014, p. 3

- Oppliger, R., *eSecurity — ein Fachgebiet im Wandel*, readme alumni, Issue 28, September 2012, 28/12, pp. 3–4

- Oppliger, R., *Sicherheit im Cloud Computing*, digma, Vol. 12, No. 1, April 2012, pp. 28–31

- Oppliger, R., *E-Voting auf unsicheren Client-Plattformen*, digma, Vol. 8, No. 2, June 2008, pp. 82–85

- Oppliger, R., *Anonymes E-Voting - eine Illusion?* digma, Vol. 8, No. 1, March 2008, pp. 24–27

- Oppliger, R., *Sicherheit auch in der Informatik - Jetzt gilt es ernst*, Editorial for a guidebook entitled "Schutz und Sicherheit" distributed with the Tages-Anzeiger of December 20, 2007, p. 2

- Oppliger, R., Hauser, R., and D. Basin, *Protecting Ecommerce Against The Man-In-The-Middle*, Business Communications Review, January 2007, pp. 54–58

- Oppliger, R., Hauser, R., and P. Frey, *MITM-Angriffe: Phishing in Echtzeit*, digma, Vol. 6, No. 1, March 2006, pp. 32–35

- Oppliger, R., *Die Jagd nach dem heiligen Gral*, digma, Vol. 5, No. 2, June 2005, pp. 92–93
- Oppliger, R., *"Sichere" Streichlisten*, digma, Vol. 5, No. 1, March 2005, pp. 34–35
- Oppliger, R., *Mit Hash auf Kollisionskurs — Hashfunktion SHA-1 möglicherweise geknackt*, Neue Zürcher Zeitung, February, 2005, p. 65
- Oppliger, R., *Der Mann in der Mitte — Zur Sicherheit des Internet-Banking*, Neue Zürcher Zeitung, October 8, 2004, p. 65
- Oppliger, R., *Open Source Software und Sicherheit*, digma, Vol. 3, No. 3, October 2003, pp. 122–126
- Oppliger, R., *Wie sicher ist Open Source Software? Offenheit bedeutet nicht automatisch Sicherheit*, Neue Zürcher Zeitung, Sonderbeilage Orbit/Comdex, B15, September 23, 2003
- Oppliger, R., and R. Rytz, *Digitale Signatur: Ist der Beweiswert gegeben?* Netzwoche "Netzguide E-Security," ISBN 3-907096-04-5, 2003, pp. 68–69
- Oppliger, R., *Sicherheit im E-Voting: Facettenreiche Probleme bei Wahlen und Abstimmungen*, Neue Zürcher Zeitung, Sonderbeilage Informatik, B3, February 4, 2003
- Oppliger, R., *E-Voting sicherheitstechnisch betrachtet — Sicherheitsfragen und -probleme bei elektronischen Abstimmungsmechanismen*, digma, Vol. 2, No. 4, December 2002, pp. 184–188
- Oppliger, R., *Wie weiter mit dem "Wer ist wer" im Netz: Digitale Zertifikate und elektronische Identitätskarten*, Neue Zürcher Zeitung, November 29, 2002, p. 77
- Oppliger, R., *Von der PKI zum Trust Management — Möglichkeiten und Grenzen einer Schweizer PKI aus technischer Sicht*, digma, Vol. 1, No. 2, June 2001, pp. 70–77
- Oppliger, R., *What is a security architecture and why would your enterprise need one?* CSI Computer Security Alert, May 2001, No. 219, pp. 1, 8
- Oppliger, R., and M. Holthaus, *Totale Überwachung ist möglich — Technische Aspekte der Kontrolle von Internet-Aktivitäten der Mitarbeiterinnen und Mitarbeiter am Arbeitsplatz*, digma, Vol. 1, No. 1, April 2001, pp. 14–19
- Oppliger, R., *Trouble Ahead, Trouble Behind: The Future of Computer Security*, CSI Computer Security Journal, Vol. XVII, No. 1, Winter 2001, pp. 19–25
- Oppliger, R., *SSL and TLS Protocols: How to Address Critical Security Issues*, CSI Computer Security Journal, Vol. XVI, No. 1, Winter 2000, pp. 15–38
- Oppliger, R., *Dezentralisierung erhöht die Sicherheitsrisiken: Ungelöste Probleme beim Agent-based Computing*, Neue Zürcher Zeitung, Sonderbeilage Informatik, B10, February 8, 2000
- Oppliger, R., *PKI in der Schweiz*, ISACA Switzerland Chapter Newsletter, December 1999, No. 46, pp. 11–13
- Oppliger, R., *Take a closer look to demystify provably secure systems*, CSI Computer Security Alert, October 1999, No. 199, p. 10

- Oppliger, R., *Methods of Securing Applications for the World Wide Web (WWW)*, CSI Computer Security Journal, Vol. XV, No. 1, 1999, pp. 1–9
- Oppliger, R., *Mobile code and agent-based systems*, CSI Computer Security Alert, October 1998, No. 187, p. 1, 7–8
- Oppliger, R., *Trusted Services (ETS) in Europe*, CSI Computer Security Alert, July 1998, No. 184, p. 3
- Oppliger, R., *How to build a corporate PKI*, CSI Computer Security Alert, May 1998, No. 182, pp. 1, 6 - 8
- Oppliger, R., *Sind WWW Cookies gefährlich?* BFI News Express, 3/97, p. 10
- Oppliger, R., *Choosing VPN protocols*, CSI Computer Security Alert, January 1997, No. 166, pp. 4 - 5
- Oppliger, R., *Pilotbetrieb eines "sicheren" WWW-Servers*, BFI News, 2/96, pp. 26–34
- Oppliger, R., *Authentifikations- und Schlüsselverteilsysteme: Eine übersicht*, Informatik/Informatique, Vol. 3, No. 4, 1996, pp. 28–33
- Oppliger, R., *OECD crypto standards*, CSI Computer Security Alert, August 1996, No. 161, p. 6
- Oppliger, R., *Next generation malicious code*, CSI Computer Security Alert, June 1996, No. 159, p. 7
- Oppliger, R., *Europe explores key escrow issues*, CSI Computer Security Alert, April 1996, No. 157, pp. 4–5
- Oppliger, R., *Sicherheit im WWW*, BFI News, 1/96, pp. 33–39
- Oppliger, R., *Clipper und die Diskussion um Key-Escrow*, Telematik-Spektrum, February 1996, pp. 16–17
- Oppliger, R., *Netzbasierte Softwareangriffe*, BFI News, 2/95, pp. 5–7
- Oppliger, R., *Baselines simplify risk analysis*, CSI Computer Security Alert, November 1995, No. 152, p. 4
- Oppliger, R., *Firewalls aren't Enough: Authentication and Key Distribution Systems*, CSI Computer Security Journal, Vol. XI, No. 2, 1995, pp. 15–24
- Oppliger, R., *Firewalls aren't enough: an authentication systems overview*, CSI Computer Security Alert, June 1995, No. 147, pp. 4–5
- Oppliger, R., *Sicherheit in X.400-Netzen*, Telematik-Spektrum, May 1994, pp. 35–37
- Oppliger, R., and D. Hogrefe, *Sicherheitsüberlegungen für unternehmensweite Kommunikationsnetze*, Telematik-Spektrum, February 1994, pp. 31–33
- Oppliger, R., Weber, S., and B. Liver, *Expertensystem konfiguriert virtuell private Netze*, Output, May 1992, pp. 43–47

12.7 Technical Reports

- Oppliger, R., *Open Source Software: Eine sicherheitstechnische Beurteilung*, August 14, 2003

- Belser, U., Federspiel, B., Kessler, Th., Kobel, Ch., Maurer, D., Oppliger, R., Schnyder, M., Thorn, A., Trenta, G., and H. Walter, *Cryptographic Key Recovery — Ein Beitrag zur Entspannung der Kryptographiediskussion*, Working Group on Security, Swiss Informaticians Society (SI), May 1999

- Oppliger, R., Gupta, A., Moran, M., and R. Bettati, *A Security Architecture for Tenet Scheme 2*, International Computer Science Institute (ICSI), Berkeley, CA, TR-95-051, 1995

- Oppliger, R., Greulich, A., and D. Hogrefe, *Authentifikations- und Schlüsselverteilsysteme*, Institute for Computer Science and Applied Mathematics (IAM), University of Bern (Switzerland), IAM-94-006, June 1994

12.8 Book Reviews

- Oppliger, R., *Book Review for "Tvede, L., Pircher, P., and J. Bodenkamp, Data Broadcasting: The Technology and the Business, John Wiley & Sons Ltd., 1999,"* Computer Communications, Vol. 24, Issue 11, June 2001, pp. 1115–1116

- Oppliger, R., *Book Review for "Escamilla, T., Intrusion Detection: Network Security Beyond the Firewall, John Wiley & Sons, New York, NY, 1998,"* Computer Communications, Vol. 23, Issue 4, February 2000, p. 429

- Oppliger, R., *Book Review for "Parker, D.B., Fighting computer crimes: a new framework for protecting information, John Wiley & Sons, New York, NY, 1998,"* Computer Communications, Vol. 22, Issue 5, April 1999, pp. 491–492