

# Michael Steiner

525 East 72<sup>nd</sup> Street, New York, NY 10021-9606, USA  
home: +1 (212) 249 1323      office: +1 (914) 784-7529  
fax: +1 (914) 784 6205      email: [steiner@acm.org](mailto:steiner@acm.org)  
www: <http://vcard.acm.org/~steiner/>

## Areas of Interest

---

- Computer Security: network security, security engineering, multi-party security, cryptographic protocols, and formal security models.
- Distributed Systems: operating systems, middle-ware, group communication, nomadic computing.

## Education

---

- Doktor der Ingenieurwissenschaften (Dr. Ing.) der Naturwissenschaftlich-Technischen Fakultät der Universität des Saarlandes, March, 2002.  
Title: “Secure Group Key Agreement”.  
Advisors: Prof. Dr. B. Pfitzmann, Prof. Dr. G. Tsudik (University of California, Irvine).  
Grade: Summa cum laude / Mit Auszeichnung
- Diplom Informatik-Ingenieur, Eidgenössische Technische Hochschule (ETH) Zürich, November 1992.  
Title: “TCP/IP on the Ceres: Design and Implementation of a Communication Stack”  
Advisor: Prof. Dr. Beverly Sanders.
- Matura Typus B. Gymnasium Laufental-Thierstein, Laufen, September 1986.

## Employment History

---

- November 2002 - present  
Research Scientist, IBM T.J Watson Research Laboratory, Hawthorne, NY, USA. Member of the Secure Software and Services Department<sup>1</sup>. Research in intrusion response, risk management, middle ware security and cryptographic protocols, most recently on deploying static analysis techniques and code rewriting to address isolation in portals. Instrumental in developing a Tivoli compliance and remediation management solution based on Network Admission Control as well as in the security design and implementation of a large software-as-a-service infrastructure for IGS (IBM Global Services).
- October 2001 - June 2002  
Head of the cryptography and security group<sup>2</sup> (Lehrstuhlvertretung), Universität des Saarlandes, Saarbrücken. Group leader of the EU ITS project MAFTIA<sup>3</sup> working on the

formal modeling of dependable cryptographic systems. Teaching course on cryptographic protocols.

- April 1999 - September 2001  
Research Scientist, Universität des Saarlandes, Saarbrücken. Member of the cryptography and security group<sup>4</sup>. Research in formal models and proofs for secure group key agreements, protocols for password-based authentication and number-theoretic cryptographic assumptions.
- January 1993 - December 2001  
Research Scientist, IBM Research Laboratory, Rüschlikon, Switzerland. Member of the security group<sup>5</sup>. Participation in the EU RACE project SAMSON and in several projects in the area of secure electronic commerce: Design of the *iKP* payment protocol family<sup>6</sup>, micro-payment extensions, and the core of the MasterCard/Visa SET Secure Electronic Transactions Protocol. Technical co-leader of the EU ACTS project SEMPER<sup>7</sup> working on the architecture of a secure e-commerce platform and the design of a generic and modular payment framework.
- January 1990 - December 1992  
System administrator, ETH Zürich, Switzerland. Management of network of MacIntosh Computers running MacOS and A/UX. (Part time work).
- June 1990 - October 1990  
Software Engineer, S.A. GEOLINK, Paris, France. Work within a EU RACE project on data retrieval / compression for a distributed database.
- March 1989 - December 1989  
Hard- and software consultant, METTLER Instrumente AG, Greifensee, Switzerland (part time work).

## Publications

---

- **Thesis**

- [1] Michael Steiner. *Secure Group Key Agreement*. Dissertation, Naturwissenschaftlich-Technische Fakultät der Universität des Saarlandes, Saarbrücken, March 2002.
- [2] Michael Steiner. *TCP/IP on the Ceres: Design and implementation of a communication stack*. Diplomarbeit, Eidgenössische Technische Hochschule (ETH), Zürich, November 1992.

- **Books (Editor) and Book chapters**

- [1] Gérard Lacoste, Birgit Pfitzmann, Michael Steiner, and Michael Waidner, editors. *SEMPER – Secure Electronic Marketplace for Europe*, volume 1854 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin Germany, August 2000.
- [2] Birgit Baum-Waidner, Gérard Lacoste, Birgit Pfitzmann, Michael Steiner, Michael Waidner, and Arnd Weber. Part i: The vision of SEMPER. In Lacoste et al. [1], pages 1–37.

- [3] N. Asokan, Birgit Baum-Waidner, Torben P. Pedersen, Birgit Pfizmann, Matthias Schunter, Michael Steiner, and Michael Waidner. Architecture. In Lacoste et al. [1], pages 45–64.
- [4] N. Asokan and Michael Steiner. The payment framework. In Lacoste et al. [1], pages 187–214.
- [5] N. Asokan, Phil Janson, Michael Steiner, and Michael Waidner. State of the art in electronic payment systems. In Marvin V. Zelkowitz, editor, *Advances in Computers*, volume 43, pages 425–449. Academic Press, March 2000.

• **Journals**

- [1] Michael Backes, Birgit Pfizmann, Michael Steiner, and Michael Waidner. Polynomial liveness. *Journal of Computer Security*, 12(3/4):589–618, 2004.
- [2] Chun-Li Lin, Hung-Min Sun, Michael Steiner, and Tzonelih Hwan. Three-party encrypted key exchange without server public-keys. *IEEE Communications Letters*, 5(12):497–499, December 2001.
- [3] Michael Steiner, Peter Buhler, Thomas Eirich, and Michael Waidner. Secure password-based cipher suite for TLS. *ACM Transactions on Information and System Security*, 4(2):134–157, May 2001.
- [4] Michael Steiner, Gene Tsudik, and Michael Waidner. Key agreement in dynamic peer groups. *IEEE Transactions on Parallel and Distributed Systems*, 11(8):769–780, August 2000.
- [5] Mihir Bellare, Juan Garay, Ralf Hauser, Amir Herzberg, Hugo Krawczyk, Michael Steiner, Gene Tsudik, Els Van Herreweghen, and Michael Waidner. Design, implementation and deployment of the *iKP* secure electronic payment system. *IEEE Journal on Selected Areas in Communications*, 18(4):611–627, April 2000.
- [6] Giuseppe Ateniese, Michael Steiner, and Gene Tsudik. New multiparty authentication services and key agreement protocols. *IEEE Journal on Selected Areas in Communications*, 18(4):628–639, April 2000.
- [7] N. Asokan, Hervé Debar, Michael Steiner, and Michael Waidner. Authenticating public terminals. *Computer Networks*, 31(8):861–870, May 1999.
- [8] Jose L. Abad-Peiro, N. Asokan, Michael Steiner, and Michael Waidner. Designing a generic payment service. *IBM Systems Journal*, 37(1):72–88, January 1998.
- [9] Michael Steiner, Günter Karjoth, and Ralf Hauser. Management von Sicherheitsdiensten in verteilten Systemen. *Datenschutz und Datensicherheit DuD, Verlag Friedrich Vieweg & Sohn, Wiesbaden*, 19(3):150–155, March 1995.

• **Conferences (refereed)**

- [1] Ran Canetti, Shai Halevi, and Michael Steiner. Mitigating dictionary attacks on password-protected local storage. In *Advances in Cryptology – CRYPTO ’2006*, Lecture Notes in Computer Science. International Association for Cryptologic Research, Springer-Verlag, Berlin Germany, 2006.

- [2] Liqun Chen, Matthias Enzmann, Ahmad-Reza Sadeghi, Markus Schneider, and Michael Steiner. A privacy-protecting coupon system. In *Proceedings of the Nineth Conference on Financial Cryptography (FC '05)*, Lecture Notes in Computer Science, Roseau, The Commonwealth Of Dominica, 2005. International Financial Cryptography Association (IFCA), Springer-Verlag, Berlin Germany.
- [3] Ran Canetti, Shai Halevi, and Michael Steiner. Hardness amplification of weakly verifiable puzzles. In *Theory of Cryptography Conference*, Lecture Notes in Computer Science. Springer-Verlag, Berlin Germany, 2005.
- [4] Naga Ayachitula, Suresh Chari, Josyula R. Rao, Michael Steiner, and Maheswaran Surendra. Autonomic enterprise security through orchestration. In *4th Annual Conference on Emerging Information Technology*, Princeton, NJ, USA, Oct 2004.
- [5] Michael Backes, Birgit Pfitzmann, Michael Steiner, and Michael Waidner. Polynomial fairness and liveness. In *15th IEEE Computer Security Foundations Workshop*, pages 160–174. IEEE Computer Society Press, June 2002.
- [6] Ahmad-Reza Sadeghi and Michael Steiner. Assumptions related to discrete logarithms: Why subtleties make a real difference. In Birgit Pfitzmann, editor, *Advances in Cryptology – EUROCRYPT '2001*, volume 2045 of *Lecture Notes in Computer Science*, pages 243–260, Innsbruck, Austria, 2001. Springer-Verlag, Berlin Germany.
- [7] Peter Buhler, Thomas Eirich, Michael Steiner, and Michael Waidner. Secure password-based cipher suite for TLS. In *Proceedings of the Symposium on Network and Distributed Systems Security (NDSS '00)*, pages 129–142, San Diego, CA, February 2000. Internet Society.
- [8] Giuseppe Ateniese, Michael Steiner, and Gene Tsudik. Authenticated group key agreement and friends. In *Proceedings of the 5th ACM Conference on Computer and Communications Security*, pages 17–26, San Francisco, California, November 1998. ACM Press.
- [9] N. Asokan, Els Van Herreweghen, and Michael Steiner. Towards a framework for handling disputes in payment systems. In *Proceedings of the 3rd USENIX Workshop on Electronic Commerce*, pages 187–202, Boston, Mass., September 1998. USENIX.
- [10] Michael Steiner, Gene Tsudik, and Michael Waidner. CLIQUES: A new approach to group key agreement. In *18th International Conference on Distributed Computing Systems (ICDCS'98)*, pages 380–387, Amsterdam, May 1998. IEEE Computer Society Press.
- [11] N. Asokan, Phil Janson, Michael Steiner, and Michael Waidner. Electronic payment systems. In *Public-Key Solutions 96*, September 1996.
- [12] Ralf Hauser, Michael Steiner, and Michael Waidner. Micro-payments based on iKP. In *14th Worldwide Congress on Computer and Communications Security Protection*, pages 67–82, C.N.I.T Paris-La Defense, France, June 1996.
- [13] Michael Steiner, Gene Tsudik, and Michael Waidner. Diffie-Hellman key distribution extended to groups. In Clifford Neuman, editor, *Proceedings of the 3rd ACM Conference on Computer and Communications Security*, pages 31–37, New Delhi, India, March 1996. ACM Press.
- [14] Mihir Bellare, Juan Garay, Ralf Hauser, Amir Herzberg, Hugo Krawczyk, Michael Steiner, Gene Tsudik, and Michael Waidner. iKP – A family of secure electronic

payment protocols. In *Proceedings of the First USENIX Workshop on Electronic Commerce*, pages 89–106, New York, July 1995. USENIX.

- [15] Ralf Hauser and Michael Steiner. Generic extensions of WWW browsers. In *Proceedings of the First USENIX Workshop on Electronic Commerce*, pages 147–154, New York, July 1995. USENIX.
- [16] Ralf Hauser, Günter Karjoth, and Michael Steiner. Management von sicherheitsdiensten in verteilten systemen. In Prof. Dr. Kurt Bauknecht and Dr. Stephanie Teufel, editors, *Sicherheit in Informationssystemen SIS'94*, Proceedings der Fachtagung SIS '94, Universität Zürich-Irchel, Institut für Informatik, pages 7–21. vdf Verlag der Fachvereine Zürich, March 1994.

- **Magazines**

- [1] Gérard Lacoste and Michael Steiner. SEMPER: A security framework for the global electronic marketplace. *comtec – the magazine for telecommunications technology*, 77(9):56–63, September 1999.
- [2] N. Asokan, Phil Janson, Michael Steiner, and Michael Waidner. State of the art in electronic payment systems. *IEEE Computer*, 30(9):28–35, September 1997.

- **Unrefereed**

- [1] Michael Steiner, Gene Tsudik, and Michael Waidner. Refinement and extension of Encrypted Key Exchange. *ACM Operating Systems Review*, 29(3):22–30, July 1995.

- **Project Deliverables (Editor)**

- [1] Cryptographic semantics for algebraic model. Deliverable D08, EU Project IST-1999-11583 Malicious- and Accidental-Fault Tolerance for Internet Applications (MAFTIA), February 2002.
- [2] SEMPER Consortium. Final report. Public deliverable D13, ACTS Project AC026, 2000.
- [3] SEMPER Consortium. Architecture, services and protocols. Deliverable D10, public specification, ACTS Project AC026, January 1999.

- **Technical Reports**

- [1] Ahmad-Reza Sadeghi and Michael Steiner. Assumptions related to discrete logarithms: Why subtleties make a real difference. Report 2002/126, Cryptology ePrint Archive, August 2002.
- [2] Final report on verification and assessment. Deliverable D22, EU Project IST-1999-11583 Malicious- and Accidental-Fault Tolerance for Internet Applications (MAFTIA), January 2003.
- [3] Birgit Pfitzmann, Michael Steiner, and Michael Waidner. A formal model for multi-party group key agreement. Technical Report RZ 3383 (# 93419), IBM Research, 2002.

- [4] Mihir Bellare, Juan Garay, Ralf Hauser, Amir Herzberg, Hugo Krawczyk, Michael Steiner, Gene Tsudik, Els Van Herreweghen, and Michael Waidner. Design, implementation and deployment of a secure account-based electronic payment system. Research Report RZ 3137, IBM Research Division, June 1999.
- [5] Giuseppe Ateniese, Michael Steiner, and Gene Tsudik. New multi-party authentication services and key agreement protocols. Research Report RZ 3115 (# 93161), IBM Research, March 1999.
- [6] Giuseppe Ateniese, Michael Steiner, and Gene Tsudik. Authenticated group key agreement and friends. Research Report RZ 3063 (#93109), IBM Research, October 1998.
- [7] N. Asokan, Els Van Herreweghen, and Michael Steiner. Towards a framework for handling disputes in payment systems. Research Report RZ 2996, IBM Research, March 1998.
- [8] Michael Steiner, Gene Tsudik, and Michael Waidner. CLIQUES: A new approach to group key agreement. Research Report RZ 2984 (# 93030), IBM Research, December 1997.
- [9] Jose L. Abad-Peiro, N. Asokan, Michael Steiner, and Michael Waidner. Designing a generic payment service. Research Report RZ 2891 (# 90839), IBM Research, December 1996.
- [10] N. Asokan, Phil Janson, Michael Steiner, and Michael Waidner. Electronic payment systems. Research Report RZ 2890 (# 90838), IBM Research, December 1996.
- [11] Ralf Hauser, Michael Steiner, and Michael Waidner. Micro-payments based on iKP. Research Report 2791 (# 89269), IBM Research, February 1996.

Many of above publications can be found in electronic form on the Internet<sup>8</sup> .

## Lectures and Talks

---

- Invited tutorial on secure electronic commerce and participation at panel at COMDEX Internet, Frankfurt, October 1997.
- Invited lecture on security in electronic commerce as part of the Postgraduate Course in Computer Science “Distributed Systems”, École Polytechnique Fédérale de Lausanne (EPFL), May, 1999.
- Conference Talks (see section on publications for more details): EITC, Princeton, October, 2004; NDSS, San Diego, February 2000; SecuriCom, Paris, June 1996; 3rd ACM CCS, New Delhi, March 1996; SIS, Zurich, March 1994.
- Invited seminar talks: “Secure Password-Based Cipher Suite for TLS”, Johns Hopkins University, June 2000; “Secure password-based cipher suite for TLS: The importance of end-to-end security”, University of Helsinki, November 2000; “Fairness in Electronic Commerce”, Technische Universität Darmstadt, July 1998; “SEMPER”, ISACA Internet Seminar, Zurich, August 1997.
- Further presentations: “Architecture of SEMPER”, 2nd Public SEMPER Workshop, Zurich, November 1998; “Secure Electronic Marketplace for Europe”, ICX Workshop,

London, February 1998; Various presentations at IBM-wide Technical Symposia in 1995, 1996 & 1997.

## Teaching

---

- Course on advanced cryptographic protocols, Winter 2001/2002.
- Seminar Internet security, Winter 2001/2002 (with A. Feldman, S. Steinbrecher & R. Sommer).
- Seminar cryptographic protocols, Sommer 2000 (with M. Schunter & T. Beiler).
- One semester introductory course in programming for secondary school teachers, 1985.

## Service

---

- Program Committee Member:
  - 7th ACM Conference on Computer and Communication Security, Nov. 2000, Athens;
  - 8th ACM Conference on Computer and Communication Security, Nov. 2001, Philadelphia;
  - 7th European Symposium on Research in Computer Science (ESORICS), Oct. 2002, Zurich.
  - 8th European Symposium on Research in Computer Science (ESORICS), Oct. 2003, Gjøvik.
  - 9th European Symposium on Research in Computer Science (ESORICS), Oct. 2004, Nice.
  - Symposium on Research in Security and Privacy, May 2004, Oakland.
  - ACM Symposium on Information, Computer and Communications Security (AsiaCCS), March 2006, Taipei, Taiwan.

(Invitation to join the PC of the 9th ACM Conference on Computer and Communication Security, 2002 declined for time reasons).

- Reviewer: ACM Transactions on Information and System Security, IEEE Transactions on Computers, IEEE Personal Communications, IEEE Internet Computing, Computer Communication Review, Computer Networks and ISDN Systems, Information Processing Letters, IBM Journal of Research and Development, IBM System Journal, Springer Journal of Digital Libraries, Acta Cybernetica, ETRI Journal, Eurocrypt, NDSS.
- Invited to evaluate project proposals for the EU IST Priority Call 1, the Research Council of Norway and the ETH, Zurich.
- Invited participant in workshop “Trust & Confidence in electronic commerce”. Preparation of the strategic content for the 5th Framework of european RTD projects, March 1998.
- Member of the personal commission in the IBM Research Laboratory from 1997 - 1999

## Miscellaneous

---

- Awards
  - IBM Outstanding Technical Achievement Awards, August 1996 and December 2005.
  - IBM Research Division Awards, December 1995 and December 1998.
  - IBM Invention Achievement Awards, November, 1999 (First Plateau) and June, 2005 (Second Plateau).
  - ISOC Best Paper Award, NDSS'2000, February, 2000.
  - IBM Personal Systems Institute Award for Prize Winning Design in the Advanced PC Device Contest, October, 2000.
- Grants: Graduiertenkolleg “Effizienz und Komplexität von Algorithmen und Rechenanlagen”, Deutsche Forschungsgesellschaft, April 1999 - September 2000.
- Patents: Eight patents granted and several patent applications under evaluation.
- Member: ACM (SIGSAC & SIGOPS), IEEE Computer Society.

## Personal

---

- Citizenship: Switzerland.
- DOB: March 8, 1967.
- Languages: german(mother tongue), english(fluent), french(good).
- Hobbies: cycling, soaring and skiing. Likes contemporary literature, music and playing violoncello.

## References

---

- *Available on on request*

## Notes

---

- <sup>1</sup>[http://domino.research.ibm.com/comm/research\\_teams.nsf/pages/sss-dept.index.html](http://domino.research.ibm.com/comm/research_teams.nsf/pages/sss-dept.index.html)
- <sup>2</sup>[http://krypt.cs.uni-sb.de/index\\_eng.html](http://krypt.cs.uni-sb.de/index_eng.html)
- <sup>3</sup><http://www.maftia.org/>
- <sup>4</sup>[http://krypt.cs.uni-sb.de/index\\_eng.html](http://krypt.cs.uni-sb.de/index_eng.html)
- <sup>5</sup><http://www.zurich.ibm.com/security/>
- <sup>6</sup><http://www.zurich.ibm.com/security/past-projects/ecommerce/iKP.html>
- <sup>7</sup><http://www.semper.org>
- <sup>8</sup><http://www.semper.org/sirene/lit/sirene.lit.html>