Curriculum Vitae – Markus Kuhn

EDUCATION AND QUALIFICATIONS

1990 Abitur

1996 Diplom-Informatiker, University of Erlangen, Germany

1997 Master of Science, Computer Sciences, Purdue University, Indiana

2002 PhD, University of Cambridge, UK

ACADEMIC EXPERIENCE

since 2001 University Lecturer, Computer Laboratory, University of Cambridge, UK

since 2001 Fellow of Wolfson College, Cambridge

INDUSTRIAL AND COMMERCIAL EXPERIENCE

Consulting projects:

1994–96 News Datacom Ltd. (now NDS Ltd.)

1997 Dallas Semiconductor

1998 Matsushita Electronics Corp.

2000–01 SuSE GmbH

2006–08 GBS mbH

2006 Bundeskriminalamt

2007 IP-Vision AB

2007 Sdu Uitgevers

2007 Acute Technology

PRIZES, AWARDS AND SCHOLARSHIPS

1986 First prize at the *Bundeswettbewerb Informatik*
(German National Student Computer Science Contest)

1987 same again

1989 First prize at the *International Olympiad on Informatics*, Bulgaria

1990–97 Scholarship by the *Studienstiftung des deutschen Volkes*

1994 *Siemens Internationaler Studentenkreis*
(industrial support programme for the five best students each year)

1996 Fulbright Scholarship for 1-year study abroad in the US

1996 USENIX Best Paper Award

1997–2000 Marie Curie Research Training Grant

1999 USENIX Best Student Paper Award

2002 IEEE Computer Society Outstanding Paper Award

PROFESSIONAL MEMBERSHIP

since 1987 Member of Gesellschaft für Informatik

since 1991 Member of Association for Computing Machinery

since 2001 Member of IEEE

PROGRAMME COMMITTEE MEMBERSHIP

1999 USENIX Workshop on Smartcard Technology

2000 IEEE Symposium on Security and Privacy

2000 USENIX Security Symposium

2002 ISOC Network and Distributed Systems Security Symposium

2004 IEEE Symposium on Security and Privacy

2004 ACM Conference on Computer and Communications Security

2005 ACM Symposium on Applied Computing – Security Track

2006 European Symposium on Research in Computer Security

2007 ESAS

2007 CHES

2008 ACM WiSec

2008 GI Sicherheit

2008 CHES

PUBLICATIONS

Selected journal papers (refereed)

[1] Markus G. Kuhn: Cipher Instruction Search Attack on the Bus-Encryption Security Microcontroller DS5002FP. IEEE Transactions on Computers, Vol. 47, No. 10, October 1998, pp. 1153–1157, ISSN 0018-9340.

[2] Fabien A.P. Petitcolas, Ross J. Anderson, Markus G. Kuhn: Information Hiding – A Survey, Proceedings of the IEEE, Vol. 87, No. 7, July 1999, pp. 1062–1078, ISSN 0018-9219.

Selected conference and workshop contributions (refereed)

[3] Markus G. Kuhn, Markus Prosch: Vorschlag für ein Dateiformat für die Verarbeitung, die Archivierung und den Austausch von Biosignal-Daten, in: R.G. Müller, J. Erb: Medizinische Physik 1993, 24. Wissenschaftliche Tagung der Deutschen Gesellschaft für Medizinische Physik e.V., Tagungsband, S. 116f, Erlangen, Oktober 1993.

[4] Ross J. Anderson, Markus G. Kuhn: Tamper Resistance – a Cautionary Note, The Second USENIX Workshop on Electronic Commerce Proceedings, Oakland, California, November 18–21, 1996, pp. 1–11, ISBN 1-880446-83-9.

[5] Ross J. Anderson, Markus G. Kuhn: Low Cost Attacks on Tamper Resistant Devices, in M. Lomas et al. (ed.): Security Protocols, 5th International Workshop, Paris, France, April 7–9, 1997, Proceedings, LNCS 1361, Springer-Verlag, pp. 125–136, ISBN 3-540-64040-1.

[6] Markus G. Kuhn, Ross J. Anderson: Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations, in David Aucsmith (Ed.): Information Hiding, Second International Workshop, IH'98, Portland, Oregon, USA, April 15–17, 1998, Proceedings, LNCS 1525, Springer-Verlag, pp. 124–142, ISBN 3-540-65386-4.

[7] Fabien A.P. Petitcolas, Ross J. Anderson, Markus G. Kuhn: Attacks on copyright marking systems, in David Aucsmith (Ed.): Information Hiding, Second International Workshop, IH'98, Portland, Oregon, USA, April 15–17, 1998, Proceedings, LNCS 1525, Springer-Verlag, pp. 219–239, ISBN 3-540-65386-4.

[8] Oliver Kömmerling, Markus G. Kuhn: Design Principles for Tamper-Resistant Smartcard Processors, Proceedings of the USENIX Workshop on Smartcard Technology (Smartcard '99), Chicago, Illinois, USA, May 10–11, 1999, USENIX Association, pp. 9–20, ISBN 1-880446-34-0.

[9] Andrew D. McDonald, Markus G. Kuhn: StegFS: A Steganographic File System for Linux, in Andreas Pfitzmann (Ed.): Information Hiding, Third International Workshop, IH'99, Dresden, Germany, Sep. 29–Oct. 1, 1999, Proceedings, LNCS 1768, Springer-Verlag, pp. 463–477, ISBN 3-540-67182-X.

[10] Markus G. Kuhn: Probabilistic Counting of Large Digital Signature Collections, Proceedings of the 9th USENIX Security Symposium, Denver, Colorado, USA, August 14–17, 2000, USENIX Association, pp. 73–83, ISBN 1-880446-18-9.

[11] Richard Clayton, George Danezis, Markus G. Kuhn: Real World Patterns of Failure in Anonymity Systems, in Ira S. Moskowitz (ed.): Information Hiding, 4th International Workshop, IHW 2001, Pittsburgh, USA, April 25–17, 2001, Proceedings, LNCS 2137, Springer-Verlag, pp. 230–245, ISBN 3-540-42733-3.

[12] Markus G. Kuhn: Optical Time-Domain Eavesdropping Risks of CRT Displays, Proceedings 2002 IEEE Symposium on Security and Privacy, Berkeley, California, 12–15 May 2002, IEEE Computer Society, pp. 3–18, ISBN 0-7695-1543-6.

[13] Markus G. Kuhn: An Asymmetric Security Mechanism for Navigation Signals, Proceedings of the 6th Information Hiding Workshop, 23–25 May 2004, Toronto, Springer-Verlag, LNCS 3200, pp. 239–252.

[14] Markus G. Kuhn: Electromagnetic Eavesdropping Risks of Flat-Panel Displays, Proceedings of the 4th Workshop on Privacy Enhancing Technologies, 26–28 May 2004, Toronto, Springer-Verlag, LNCS 3424, pp. 88-105.

[15] Markus G. Kuhn: Security Limits for Compromising Emanations, in J.R. Rao, B. Sundar (Eds.): Workshop on Cryptographic Hardware and Embedded Systems (CHES 2005), 29 August–1 September 2005, Edinburgh, Scotland, Springer-Verlag, LNCS 3659, pp. 265–279.

[16] Gerhard P. Hancke, Markus G. Kuhn: An RFID Distance Bounding Protocol. Proceedings IEEE SecureComm 2005, 5–9 September 2005, Athens, Greece, pp. 67–73, ISBN 0-7695-2369-2.

[17] Jolyon Clulow, Gerhard P. Hancke, Markus G. Kuhn, Tyler Moore: So Near and Yet So Far: Distance-Bounding Attacks in Wireless Networks. European Workshop on Security and Privacy in Ad-Hoc and Sensor Networks (ESAS), Hamburg, Germany, 20–21 September 2006, LNCS 4357.

[18] Gerhard P. Hancke, Markus G. Kuhn: Attacks on Time-of-Flight Distance Bounding Channels. ACM Conference on Wireless Network Security (WiSec), March 31–April 2, 2008, Alexandria, Virginia, USA.

Invited papers

[19] Markus G. Kuhn: Eavesdropping attacks on computer displays. Information Security Summit, Prague, 24–25 May 2006.

Book contributions

[20] Markus G. Kuhn: "Compromising emanations", "Data remanence", "Smartcard tamper resistance", "TEMPEST". Entries in Henk C.A. van Tilborg (ed.): Encyclopedia on Cryptography and Security, Springer, 2005, ISBN 0-387-23473-X.

Technical Reports

[21] Markus G. Kuhn: Specification of the EBS File Format for Bio-Signals, Institut für Physiologie und Biokybernetik, Erlangen, Oktober 1993.

[22] Markus G. Kuhn: Compromising emanations: eavesdropping risks of computer displays. Technical Report UCAM-CL-TR-577, University of Cambridge, Computer Laboratory, December 2003.

Patents

[23] Markus Günther Kuhn, Ross John Anderson: Low cost countermeasure against compromising electromagnetic computer emanations. UK Patent GB2333883, 2002-09-17. (also: U.S. Patent US6721423)

[24] Markus Günther Kuhn, Ross John Anderson: Software piracy detector sensing electromagnetic computer emanations. UK Patent GB2330924, 2003-08-06.

[25] Christoph L. Schuba, Ivan V. Krsul, Diego Zamboni, Eugene H. Spafford, Aurobindo M. Sundaram, Markus G. Kuhn: Network protection for denial of service attacks. US Patent US6725378, 2004-04-20.

[26] Markus Günther Kuhn: Positioning system. UK Patent GB2413448, 2007-03-07.

Other academic publications

[27] Gunther Hellmann, Markus G. Kuhn, Markus Prosch, Manfred Spreng, H. Stefan: Entscheidungen zur EEG/MEG-Datenspeicherung: Untersuchungen zu Kosten, Kompression und Langzeitarchivierung, Epilepsie-Blätter, Gemeinsame Tagung der Deutschen, Italienischen und Österreichischen Sektion der Internationalen Liga gegen Epilepsie, Meran, 1993.

[28] Manfred Spreng, Gunther Hellmann, Markus G. Kuhn, K.-D. Reinartz, H. Stefan: Bearbeitung von evozierten Potentialen und Epilepsie-EEG/MEG mit unüberwacht lernenden Klassifikatoren, Biomedizinische Technik, Graz, 1993.

[29] Manfred Spreng, Gunther Hellmann, Markus G. Kuhn, K.-D. Reinartz, H. Stefan: Unsupervised EEG/ECoG/MEG Classification in Epilepsy Using Array Processors, in: M. Eiselt, U. Zwiener, H. Witte (ed.): Quantitative and topological EEG and MEG analysis, Universitätsverlag Druckhaus Mayer, Jena, 1993.

[30] Gunther Hellman, Markus G. Kuhn, Markus Prosch, Manfred Spreng: Extensible biosignal (EBS) file format: simple method for EEG data exchange, Electroencephalography and Clinical Neurophysiology, Vol. 99, No. 5, November 1996, Elsevier Science, pp. 426–431.

[31] Christoph Schuba, Ivan Krsul, Markus G. Kuhn, Eugene Spafford, Aurobindo Sundaram, Diego Zamboni: Analysis of a Denial of Service Attack on TCP, in Proceedings of the 1997 IEEE Symposium on Security and Privacy, Oakland, California, May 5–7, 1997.

[32] M.A. Bashar, G. Krishnan, Markus G. Kuhn, Eugene H. Spafford, Samuel S. Wagstaff Jr.: Low-threat security patches and tools, Proceedings International Conference on Software Maintenance, Bari, Italy, 1–3 October 1997, IEEE Computer Society, 1997, pp. 306–313, ISBN 0-8186-8013-X.

[33] Ross J. Anderson, Markus G. Kuhn: Soft Tempest – An Opportunity for NATO, in Information Systems Technology (IST) Symposium "Protecting NATO Information Systems in the 21st Century", Washington, DC, USA, 25–27 October 1999, NATO Research and Technology Organization (RTO), RTO-MP-27, AC/323(IST)TP/3, chapter 5, May 2000.

[34] Simon W. Moore, Ross J. Anderson, Markus G. Kuhn: Improving Smartcard Security using Self-timed Circuit Technology, Fourth ACiD-WG Workshop, Grenoble, ISBN 2-913329-44-6, 2000.

[35] Andreas Pfitzmann, Hannes Federrath, Markus Kuhn: Anforderungen an die gesetzliche Regulierung zum Schutz digitaler Inhalte unter Berücksichtigung der Effektivität technischer Schutzmechanismen (Technischer Teil). A study commissioned by Deutscher Multimedia Verband (dmmv) e.V. and Verband Privater Rundfunk & Telekommunikation (VPRT) e.V., 2002-03-13.

Popular journal and trade press articles

[36] Markus Kuhn: Am Anschlag : V.34: der neue Modemstandard für 28 000 Bit/s, iX 2/1995, pp. 144–153, Verlag Heinz Heise, Germany, ISSN 0935-9680.

[37] Markus Kuhn: In die Röhre geguckt : Unerwünschte Abstrahlung erlaubt Lauschangriffe, c't 24/1998, pp. 90–97, Verlag Heinz Heise, Germany, ISSN 0724-8679.

[38] Markus Kuhn, Oliver Kömmerling: Physical Security of Smartcards, Information Security Technical Report, Vol. 4, No. 2, Elsevier Advanced Technology, 1999, pp. 28–41, ISSN 1363-4127.

Talks

[39] Markus G. Kuhn: Probability Theory for Pickpockets, DREI'97 workshop talk, Ruttgers University, New Jersey, USA, 1997-08-14.

[40] Markus G. Kuhn: Attacks on Pay-TV Access Control Systems, University of Cambridge, Computer Laboratory, Security Seminar talk, 1997-12-09.

[41] Markus G. Kuhn: Hardware Security – Smartcards and other Tamper-Resistant Modules, University of Cambridge, Computer Laboratory, Departmental Seminar talk, 1998-02-04.

[42] Markus G. Kuhn: Hardware Sicherheit – Chipkarten und andere Sicherheitsprozessoren, Universität Erlangen-Nürnberg, Regionales Rechenzentrum Kolloquium, 1998-02-17.

[43] Markus G. Kuhn: Electromagnetic eavesdropping on computers, University of Cambridge, Computer Laboratory, Departmental Seminar talk, 2002-06-12.

[44] Markus G. Kuhn: Leap-second considerations in distributed computer systems, ITU-R SRG 7A Colloquium on the UTC timescale, Torino, Italy, 2003-05-29.

[45] Markus G. Kuhn: Positioning Security – from electronic warfare to cheating RFID and road-tax systems. escar – Embedded Security in Cars, 4th Workshop, 14–15 November 2006, Berlin.

Software packages

[46] Markus G. Kuhn: JBIG-KIT – bi-level image data compression package. Version 1.6, 2004-06-11.

[47] Markus G. Kuhn: OTPW – one-time password package. Version 1.3, 2003-09-30.

[48] Markus G. Kuhn, et al.: UCS-Fonts – Unicode fonts and tools for X11, 1998–2003.

Online version: `http://www.cl.cam.ac.uk/~mgk25/publications.html`

2008-01-31