Anhang

S. Wendzel, *Tunnel und verdeckte Kanäle im Netz*,
DOI 10.1007/978-3-8348-2143-0, © Springer Fachmedien Wiesbaden 2012

Literaturverzeichnis

[1] Accorsi, R., Wonnemann, C.: Detective Information Flow Analysis for Business Processes (Extended Abstract), In: Business Processes, Services Computing and Intelligent Service Management, LNI Volume 147, Bonner Köllen Verlag, Seiten 223–224, 2009.

[2] Accorsi, R., Wonnemann, C.: Informationsfluss-Mechanismen zur Zertifizierung von Cloud-basierten Geschäftsprozessen, Deutscher IT-Sicherheitskongress des BSI, SecuMedia-Verlag Bonn, Mai 2011.

[3] Accorsi, R., Wonnemann, C.: Informationsfluss-Mechanismen zur Zertifizierung Cloud-basierter Geschäftsprozesse (Vortragsfolien), Deutscher Sicherheitskongress des BSI, 2011.

[4] Agat, J.: Transforming out Timing Leaks, Proceedings of the 27th ACM Symp. on Principles of Programming Languages (POPL), ACM Press, Seiten 40–53, 2000.

[5] Agat, J.: Transforming out Timing Leaks in Practice: An Experiment in Implementing, Programming Language-Based Methods for Confidentiality, ein Kapitel aus "Type Based Techniques for Covert Channel Elimination and Register Allocation", Dissertation, Chalmers Tekniska Högskola/Chalmers University Of Technology, Seiten 69–106, 2001.

[6] Ahsan, K.: Covert Channel Analysis and Data Hiding in TCP/IP, Master-Thesis (University of Toronto), 2002.

[7] Anderson, R.: Security Engineering: A Guide to Building Dependable Distributed Systems, Wiley, 2001.

[8] Arends, R., Austein, R., Larson, M. et al.: Protocol Modifications for the DNS Security Extensions (RFC 4035), März 2005.

[9] Badach, A., Hoffmann, E.: Technik der IP-Netze. Funktionsweise, Protokolle und Dienste, 2. Auflage, Carl Hanser Verlag München Wien, 2007.

[10] Baliga, A., Kilian, J.: On covert collaboration, in Proc. 9th Workshop on Multimedia and Security, ACM / New York, Seiten 25–34, 2007.

[11] Becker, K.-B.: Internetzensur in China. Aufbau und Grenzen des chinesischen Kontrollsystems, VS Research, 1. Auflage, 2011.

[12] Berk, V., Giani, A., Cybenko, G.: Detection of Covert Channel Encoding in Network Packet Delays, Technical Report TR536, Rev. 1, Dep. of Computer Science, Dartmouth College, November 2005.

[13] Bidou, R., Raynal, F.: Covert Channels, 2005.

[14] Bishop, M.: Computer Security: Art and Science, Addison Wesley, November, 2002.

[15] Borland, T.: Guide to Encrypted Dynamic Covert Channels, 24. Dezember 2008. URL: *http://turboborland.blogspot.com/2008/12/guide-to-encrypted-dynamic-covert.html*.

[16] Cabuk, S., Brodley, C. E., Shields, C.: IP Covert Timing Channels: Design and Detection, In Proc. 11th ACM Conference on Computer and Communications Security (CCS '04), Seiten 178–187, 2004.

[17] Cabuk, S., Brodley, C. E., Shields, C.: IP Covert Channel Detection, ACM Transactions on Information and System Security (TISSEC), Volume 12, Issue 4, Seiten 22:1–22:29, April 2009.

[18] Carpenter, B., Moore, K.: Connection of IPv6 Domains via IPv4 Clouds (RFC 3056), Februar 2001.

[19] Castro, S. und das Gray World Team: How to cook a covert channel, Hackin9 01/2006, S. 50–57.

[20] Conta, A., Deering, S.: Generic Packet Tunneling in IPv6 Specification, RFC 2473, Dezember 1998.

[21] daemon9: LOKI2 (the implementation), Phrack Magazine, Volume 7, Issue 51, September 1997.

[22] Department of Defence: Trusted Computer System Evaluation Criteria (TCSEC, DoD 5200.28-STD), 26. Dezember 1985.

[23] Dittmann, J., Franz, E., Schneidewind, A.: Steganographie und Wasserzeichen. Aktueller Stand und neue Herausforderungen, Informatik Spektrum Vol. 28. No. 6, Seiten 453–461, Dezember 2005.

[24] Dommety, G.: Key and Sequence Number Extensions to GRE, RFC 2890, September 2000.

[25] Dürmuth, M.: Novel Classes of Side Channels and Covert Channels, Dissertation, Universität des Saarlandes, 2009.

[26] Eckert, C.: IT-Sicherheit: Konzepte, Verfahren, Protokolle, 6. Auflage, Oldenbourg Wissenschaftsverlag, 2009.

[27] Eßer, H.-G.: Ausnutzung verdeckter Kanäle am Beispiel eines Web-Servers, Diplomarbeit (RWTH Aachen), Februar 2005.

[28] Fadlalla, Y. A. H.: Approaches to Resolving Covert Storage Channels in Multilevel Secure Systems, Ph.D. Thesis, University of New Brunswick, 1996.

[29] Farinacci, D., Li, T. Hanks, S., Meyer, D., Traina, P.: Generic Routing Encapsulation (GRE), RFC 2784, März 2000.

[30] Fisk, G., Fisk, M., Papadopoulos, C. und Neil, J.: Eliminating Steganography in Internet Traffic with Active Wardens, In Proc. Information Hiding Conference 2003, Lecture Notes in Computer Science, Volume 2578, Seiten 18–35, 2003.

[31] Gianvecchio, S., Wang, H.: Detecting Covert Timing Channels: An Entropy-Based Approach, In Proc. ACM Conference on Computer and Communications Security (CCS), Seiten 307–316, 2007.

[32] Giani, A., Berk, V. H., Cybenko, G. V.: Data Exfiltration and Covert Channels, In: Sensors, and Command, Control, Communications, and Intelligence (C3I) Technologies for Homeland Security and Homeland Defense V, 2006.

[33] Giffin, J., Greenstadt, R., Litwack, P., Tibbetts, R.: Covert messaging through TCP timestamps, In Proc. 2nd int. Conf. on privacy enhancing technologies, Seiten 194–208, 2003.

[34] Gilligan, R. E.: Simple Internet Transition Overview (Version 01), IETF Draft, November 1994.

[35] Girling, C.G.: Covert Channels in LAN's, In Proc. IEEE Transactions on Software Engineering, Volume SE-13, Issue 2, Seiten 292–296, Februar 1987.

[36] Goltz, J. P.: Under the radar: A look at three covert communications channels, GIAC security essentials (GSEC), 2003.

[37] Grossman, D.: New Terminology and Clarifications for Diffserv, RFC 3260, April 2002.

[38] Hagen, S.: IPv6. Grundlagen, Funktionalität, Integration, 2. Auflage, Sunny Edition, Dezember 2009.

[39] Hamzeh, K., Pall, G., Verthein, W. et al.: Point-to-Point Tunneling Protocol (PPTP), RFC 2637, Juli 1999.

[40] Handley, M., Paxson, V., Kreibich, C.: Network Intrusion Detection: Evasion, Traffic Normalization, and End-to-End Protocol Semantics, SSYM'01 Proceedings of the 10th conference on USENIX Security Symposium, Volume 10, Seiten 115–131, 2001.

[41] Hanks, S., Li, T., Traina, P.: Generic Routing Encapsulation (GRE), RFC 1701, October 1994.

[42] Hanks, S., Li, T., Traina, P.: Generic Routing Encapsulation over IPv4 networks, RFC 1702, October 1994.

[43] Heiny, F.: Seminar KNX/IP-Router (Foliensatz), Weinzierl Engineering GmbH, Februar 2009.

[44] Hoffman, P.: Algorithms for Internet Key Exchange version 1 (IKEv1), RFC 4109, Mai 2005.

[45] Holzmann, G. J.: Design and Validation of Computer Protocols, Prentice Hall, 1991.

[46] Hu, W.-M.: Reducing Timing Charmers with Fuzzy Time, 1991 Symposium on Security and Privacy, IEEE Computer Society, Seiten 8–20, 1991.

[47] Huitema, C.: Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs), RFC 4380, Februar 2006.

[48] IANA (Internet Assigned Numbers Authority): SMI Network Management Private Enterprise Codes, *http://www.iana.org/assignments/enterprise-numbers*, Januar 2012.

[49] IANA (Internet Assigned Numbers Authority): Point-to-Point (PPP). Protocol Field Assignments, *http://www.iana.org/assignments/ppp-numbers*, November 2011.

[50] IANA (Internet Assigned Numbers Authority): IPv6 Global Unicast Address Assignments, *http://www.iana.org/assignments/ipv6-unicast-address-assignments* August 2008.

[51] Jacobson, V.: Compressing TCP/IP Headers for Low-Speed Serial Links, RFC 1144, February 1990.

[52] Jankowski, B., Mazurczyk, W., Szczypiorski, K.: Information Hiding Using Improper Frame Padding, In Proc. 14th International Telecommunications Network Strategy and Planning Symposium (NETWORKS), Seiten 1–6, 2010.

[53] Ji, L., Liang, H., Song, Y., Niu, X.: A Normal-Traffic Network Covert Channel, In Proc. International Conference on Computational Intelligence and Security, Seiten 499-503, 2009.

[54] Kang, M. H., Moskowitz, I. S.: A Pump for Rapid, Reliable, Secure Communication, Proceedings of the 1st ACM Conference on Computer and Communication Security, Seiten 119–129, November 1993.

[55] Kang, M. H., Moskowitz, I. S., Chincheck, S.: The Pump: A Decade of Covert Fun, 21st. Annual Computer Security Applications Conference, Seiten 352–360, Dezember 2005.

[56] Kappes, M.: Netzwerk- und Datensicherheit. Eine praktische Einführung, Teubner-Verlag Wiesbaden, 2009.

[57] Kastner, W., Neugschwandtner, G., Soucek, S. und Newman, H. M.: Communication Systems for Building Automation and Control, In Proceedings of the IEEE, Vol. 93, No. 6, Seiten 1178–1203, 2005.

[58] Kaufman, C. (Hrsg.): Internet Key Exchange (IKEv2) Protocol, Dezember 2005.

[59] Kemmerer, R. A.: Shared resource matrix methodology: an approach to identifying storage and timing channels, ACM Transactions on Computer Systems (TOCS), ACM, Volume 1, Issue 3, Seiten 256–277, 1983.

[60] Kemmerer, R. A., Porras, P. A.: Covert Flow Trees: A Visual Approach to Analyzing Covert Storage Channels, IEEE Transactions on Software Engineering, Volume 17. No. II, Seiten 1166–1185, November 1991.

[61] Kemmerer, R. A.: A Practical Approach to Identifying Storage and Timing Channels: Twenty Years Later, In Proc. Annual Computer Security Applications Conference (ACSAC), Seiten 109–118, Dezember 2002.

[62] Kemmerer, R. A.: So You Think You Can Dance?, 23. Annual Computer Security Applications Conference (ACSAC 2007), Seiten 3–17, 2007.

[63] Kent, S.: IP Encapsulating Security Payload (ESP), RFC 4303, Dezember 2005.

[64] Kent, S., Atkinson, R.: IP Authentication Header, RFC 2402, November 1998.

[65] Kelsey, J., Schneier, B., Wagner, D., Hall, C.: Side channel cryptanalysis of product ciphers, In Computer Security (ESORICS 98), LNCS 1485, Seiten 97–110, 1998.

[66] Khan, H., Javed, Y., Mirza, F. und Khayam, S. A.: Embedding a Covert Channel in Active Network Connections, Lecture Notes in Computer Science, Volume 2578, Seiten 18–35, 2003.

[67] Kirkman, T. W.: Statistics to Use, Kapitel zum Kolmogorov-Smirnov-Test, *http://www.physics.csbsju.edu/stats*, College of Saint Benedict Saint John's University, 1996.

[68] Kohno, T., Broido, A., claffy, k.: Remote Physical Device Fingerprinting, IEEE Transactions on Dependable and Secure Computing, No. 2, Seiten 93–108, 2005.

[69] König, H.: Protocol Engineering. Prinzip, Beschreibung und Entwicklung von Kommunikationsprotokollen, 1. Aufl., Vieweg+Teubner, 2003.

[70] Krätzer, C., Dittmann, J.: Früherkennung von verdeckten Kanälen in VoIP-Kommunikation, IT-Frühwarnsysteme, BSI-Workshop, Bundesamt für Sicherheit in der Informatik, Bonn, S. 209–214, 2006.

[71] Kurose, J. F., Ross, K. W.: Computer Networking – A Top-Down Approach Featuring the Internet, Pearson Education, 3rd Int. Ed., 2005.

[72] Lampson, B.W.: A Note on the Confinement Problem, Communications of the ACM, Volume 16, Number 10, Seiten 613–615, 1973.

[73] Lau, J., Townsley, M., Goyret, I.: Layer Two Tunneling Protocol – Version 3 (L2TPv3), RFC 3931, März 2005.

[74] Lechner, D., Granzer, W., Kastner, W.: Security for KNXnet/IP, Konnex Scientific Conference, 2008.

[75] Leech, M., Ganis, M., Lee, Y., et al.: SOCKS Protocol Version 5, RFC 1928, March 1996.

[76] Lewandowski, G., Lucena, N.B., Chapin, S.J.: Analyzing network-aware active wardens in IPv6, In Proc. 8th International Conference on Information Hiding (IH'06), Seiten 58–77, 2007.

[77] Li, W., He, G.: Towards a Protocol for Autonomic Covert Communication, In Proc. 8th Conf. on Autonomic and Trusted Computing, Seiten 106–117, 2011.

[78] Li, X., Zhang, Y., Chong, F.T., Zhao, B.Y.: A Covert Channel Analysis of a real Switch, unfertiger "final report", Dep. of Computer Science, University of California, Santa Barbara, 2011.

[79] Li, Z., Goyal, A. und Chen, Y.: Honeynet-based Botnet Scan Traffic Analysis, Advances in Information Security/Botnet Detection, In Proc. Advances in Information Security, Volume 36, Springer, S. 25–44, 2008.

[80] Maña, A., Rudolph, C., Hoffmann, M. et al.: Towards Semantic Resolution of Security in Ambient Environments, In Proc. Developing Ambient Intelligence, Seiten 13–22, Springer Paris, 2008.

[81] Mantel, H.: On the Composition of Secure Systems, Proceedings of the 2002 IEEE Symposium on Security and Privacy, Oakland, Seiten 88–101, 2002.

[82] McHugh, J.: Covert Channel Analysis. Technical Memo 5540:080A, Naval Research Laboratory, 1995.

[83] McHugh, J.: An Information Flow Tool for Gypsy: An Extended Abstract Revisited, In Proc. of Annuall Computer Security Applications Conference, Seiten 191–201, 2001.

[84] McGregor, G.: The PPP Internet Protocol Control Protocol (IPCP), RFC 1332, May 1992.

[85] Merz, H., Hansemann, T., Hübner, C.: Building Automation. Communication Systems with EIB/KNX, LON and BACnet, Springer Series on Signals and Communication Technology, Springer-Verlag Berlin Heidelberg, 2009.

[86] Microsoft: Überblick zu Teredo, März 2004. Online verfügbar auf *http://www.microsoft.com/germany/technet/datenbank/articles/600330.mspx*

[87] Moskowitz, I.S., Kang, M.H.: Covert channels – here to stay?, In Proc. of the Ninth Annual Conference on Computer Assurance (COMPASS '94), Seiten 235–243, 1994.

[88] Murdoch, S. J.: Covert channel vulnerabilities in anonymity systems, Technical Report Number 706, University of Cambridge (Computer Laboratory), Dezember 2007.

[89] Murdoch, S. J., Lewis, S.: Embedding Covert Channels into TCP/IP, In Proc. Information Hiding Conference 2005, Lecture Notes in Computer Science, Volume 3727, Springer Berlin/Heidelberg, Seiten 247–261, 2005.

[90] Myers, C. A., Liskov B.: Protecting privacy using the decentralized label model, ACM Transactions on Software Engineering and Methodology (TOSEM), Volume 9, Issue 4, Seiten 410–442, 2000.

[91] Naval Research Laboratory: Network Pump Brochure, Januar 2009.

[92] National Computer Security Center: A Guide to Understanding Covert Channel Analysis of Trusted Systems, NCSC-TG-030, Library No. S-240,572, Version 1, November 1993.

[93] Nordmark, E., Gilligan, R.: Basic Transition Mechanisms for IPv6 Hosts and Routers, RFC 4213, October 2005.

[94] Obermann, K., Horneffer, M.: Datennetztechnologien für Next Generation Networks. Ethernet, IP, MPLS und andere, 1. Aufl., Vieweg+Teubner, 2009.

[95] Ogurtsov, N., Orman, H., Schroeppel, R., OMalley, S., Spatscheck, O.: Covert Channel Elimination Protocols, Technical Report, Department of Computer Science, University of Arizona, 1996.

[96] Ogurtsov, N., Orman, H., Schroeppel, R., OMalley, S., Spatscheck, O.: Experimental Results of Covert Channel Limitation in One-Way Communication Systems, Vortragsfolien, University of Arizona, 1997.

[97] OpenBSD Project: PF: Scrub (Packet Normalization), *http://www.openbsd.org/faq/pf/scrub.html*, Juli 2008.

[98] Orebaugh, A., Biles, S., Babbin, J.: Snort Cookbook, O'Reilly Media, Inc., März 2005.

[99] Perkins, C.: IP Encapsulation within IP, RFC 2003, Oktober 1996.

[100] Petersohn, H.: Data Mining. Verfahren, Prozesse, Anwendungsarchitektur, Oldenbourg Wissenschaftsverlag GmbH, 2005.

[101] Petitcolas, F. A. P., Anderson, R. J., Kuhn, M. G.: Information Hiding – A Survey, In. Proc. of the IEEE (special issue on protection of multimedia content), Vol. 87, Issue 7, Seiten 1062–1078, Juli 1999.

[102] Plötner, J., Wendzel, S.: Praxisbuch Netzwerksicherheit, Galileo Press, Bonn, 2. Auflage, 2007.

[103] Proctor, N. E., Neumann, P. G.: Architectural Implications of Covert Channels, Proceedings of the Fifteenth National Computer Security Conference Baltimore, Seiten 28–43, 1992.

[104] Ray, B., Mishra, S.: Secure and Reliable Covert Channel (ext. Abstr.), CSIIRW'08, May 12-14, ACM, 2008.

[105] Reynolds, J.: Assigned Numbers: RFC 1700 is Replaced by an On-line Database, RFC 3232, Januar 2002.

[106] Reynolds, J., Postel, J.: Assigned Numbers, RFC 1700, Oktober 1994. *Anmerkung:* Dieses RFC hat nur noch historischen Wert. Entsprechend aktuelle Informaitionen sind bei der IANA zu finden.

[107] Rios, R., Onieva, J.A., Lopez, J.: HIDE_DHCP: Covert Communications Through Network Configuration Messages, In Proc. IFIP TC 11 27th International Information Security Conference, Heraklion, Crete, Greece, Springer, 2012 (derzeit im Druck).

[108] Rist, T., Wendzel, S., Masoodian, M., Monigatti, P., André, E.: Creating Awareness for Efficient Energy Use in Smart Homes, In: Intelligent Wohnen. Zusammenfassung der Beiträge zum Usability Day IX, Feuerstein Gerhild, Ritter Walter (Hrsg.), Seiten 162–168, 2011.

[109] Romkey, J.: RFC 1055 – A nonstandard for transmission of IP datagrams over serial lines: SLIP, June 1988.

[110] Roth, J.: Mobile Computing: Grundlagen, Technik, Konzepte, 2. Aufl., dpunkt, 2005.

[111] Rowland, C. H.: Covert Channels in the TCP/IP Protocol Suite, First Monday, Volume 2, Number 5, 5 May 1997.

[112] Rutkowska, J.: The Implementation of Passive Covert Channels in the Linux Kernel, Dezember 2004.

[113] Schea, R.: L2TP: Implementation and Operation, Addison-Wesley Professional, 1st Edition, 2000.

[114] Schmeh, K.: Versteckte Botschaften – Die faszinierende Geschichte der Steganografie, Heise, 2008.

[115] Schear, N., Kintana, C., Zhang, Q., Vahdat, A.: Glavlit: Preventing Exfiltration at Wire Speed, In Proc. 5th ACM Workshop on Hot Topics in Networks (HotNets-V), November 2006.

[116] Schneider, J. M.: Protocol Engineering. A Rule-Based Approach, Vieweg Advanced Studies in Computer Science, Vieweg Verlag Wiesbaden, 1992.

[117] Schneier, B.: Angewandte Kryptographie. Protokolle, Algorithmen und Sourcecode in C, Pearson Studium, 2. Aufl., 2006.

[118] Schrader, T.: Statistische Erkennung von HTTP-Tunneln, Masterarbeit, FernUniversität Hagen, Juli 2006.

[119] Shannon, C. E., Weaver, W.: The Mathematical Theory of Communication, The University of Illinois Press, 1964.

[120] Simmons, G. J.: The Prisoner's Problem and the Subliminal Channel, Advances in Cryptology: Proceedings of CRYPTO '83, Plenum Press, Seiten 51–67, 1984.

[121] Simpson, W.: The Point-to-Point Protocol (PPP), RFC 1661 (STD 51), July 1994.

[122] Simpson, W.: IP in IP Tunneling, RFC 1853, Oktober 1995.

[123] Singh, A., Nordström, O. dos Santos, A., Lu, C.: Stateless Model for the Prevention of Malicious Communication Channels, International Journal of Computers and Applications, Volume 28, Issue 3, Seiten 285–297, ACTA Press, 2006.

[124] Singh, A., Nordström, O., Lu, C., dos Santo, A.L.M.: Malicious ICMP Tunneling: Defense against the Vulnerability, In: Information Security and Privacy (LNCS Vol. 2727), S. 216–236, 2003.

[125] Smart Grid Interoperability Panel, The (Cyber Security Working Group des National Institute of Standards and Technology (NIST) und des US Department of Commerce): NISTIR 7628 – Guidelines for Smart Grid Cyber Security: Volume 3, Supportive Analyses and References, August 2010.

[126] Smeets, M., Koot, M.: Research Report: Covert Channels (University of Amsterdam), February 5, 2006.

[127] Snort Project, The (Sourcefire, Inc.): SNORT Users Manual 2.9.0, *http://www.snort.org/assets/166/snort_manual.pdf*, Januar 2011.

[128] Solomon, J., Glass, S.: Mobile-IPv4 Configuration Option for PPP IPCP, RFC 2290, Februar 1998.

[129] Sourcefire, Inc.: Snort Threat Prevention Components (Whitepaper), *http://www.imerja.com/files/file/White_Papers/Sourcefire/Snort%20Threat- %20Prevention.pdf*, 2009.

[130] Stødle, D.: Ping Tunnel – For those times when everything else is blocked, URL: *http://www.cs.uit.no/˜daniels/PingTunnel/*, June 2009.

[131] Tanenbaum, A.S.: Computernetzwerke, 4. überarb. Aufl., Pearson Studium, 2003.

[132] Taib, A. M., Budiarto, R.: Securing Tunnel Endpoints for IPv6 Transition in Enterprise Networks, In Proc. 2010 International Conference on Science and Social Research (CSSR 2010), Kuala Lumpur, S. 1114–1119, 2010.

[133] Templin, F., Gleeson, T., Talwar, M., Talwar, D.: IETF Draft Intra-Site Automatic Tunnel Addressing Protocol (ISATAP), Draft 17, January, 2004.

[134] Templin, F., Gleeson, T., Thaler, D.: Intra-Site Automatic Tunnel Addressing Protocol (ISATAP, RFC 5214), März 2008.

[135] Thaler, D., Krishnan, S., Hoagland, J.: Teredo Security Updates (RFC 5991), September 2010.

[136] Townsley, W., Valencia, A., Rubens, A., Pall, G., Zorn, G., Palter, B.: Layer Two Tunneling Protocol "L2TP", RFC 2661 (proposed standard), August 1999.

[137] Trimmal, R., Harald, W.: KNXnet/IP (EIBnet/IP) und IP-852, 2008.

[138] Tsai, C.-R., Gligor, V. D.: A Bandwidth Computation Model for Covert Storage Channels and its Applications, Proceedings of the IEEE Symposium on Security and Privacy, Oakland, Californien, Seiten 108–121, April 1988.

[139] Tumoian, E., Anikeev, M.: Network Based Detection of Passive Covert Channels in TCP/IP, In Proc. IEEE Conference on Local Computer Networks 30th Anniversary (LCN'05), Seiten 802–809, 2005.

[140] Valin, J. M., Vos, K., Terriberry, T.: Definition of the Opus Audio Codec (draft-ietf-codec-opus-11), 17. Feb. 2012.

[141] Vogel, T., Dittmann, J., Hillert, R., Krätzer, C.: Design und Evaluierung von Steganographie für Voice-over-IP, Sicherheit 2006, 20-22 Feb. 2006, Magdeburg, 2006.

[142] Wang, C., Ju, S.: The Dilemma of Covert Channels Searching, In Proc. Information Security and Cryptology - ICISC 2005, Lecture Notes in Computer Science, Volume 3935, Springer, Seiten 169–174, 2006.

[143] Washburn, K. und Evans, J.: TCP/IP – Aufbau und Betrieb eines TCP/IP Netzes, Addison-Wesley, 2. Auflage, 1. korrigierter Nachdr. 1998.

[144] Wendzel, S.: Protocol Channels, Hakin9 (en) 06/09, Seiten 38–40, 2009.

[145] Wendzel, S.: Protocol Hopping Covert Channels, Hakin9 03/2008, Seiten 20–21, 2008.

[146] Wendzel, S.: Protokollwechsel zur Realisierung von Covert Channels und Header-Strukturveränderungen zur Vermeidung von Covert Channels, Diplomarbeit, Hochschule Kempten, Mai 2009.

[147] Wendzel, S., Keller, J.: Low-attention forwarding for mobile network covert channels, In Proc. 12th Conference on Communications and Multimedia Security (CMS 2011), IFIP International Federation for Information Processing, B. de Decker et al. (Eds.), LNCS 7025, pp. 122–133, 2011.

[148] Wendzel, S., Rist, T., André, E., Masoodian, M.: A Secure Interoperable Architecture for Building Automation Applications, in Proc. 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies (ISABEL), Oct 26-29, Barcelona, Spain, 2011.

[149] Wendzel, S.: The Problem of Traffic Normalization Within a Covert Channel's Network Environment Learning Phase, in Proc. Sicherheit 2012 (6. Jahrestagung des Fachbereichs Sicherheit), Darmstadt, N. Suri and M. Waidner (Eds.), LNI vol. 195, pp. 149-161, Gesellschaft für Informatik (GI) / Bonn, 2012.

[150] Wendzel, S., Keller, J.: Design and Implementation of an Active Warden Addressing Protocol Switching Covert Channels, In Proc. The Seventh International Conference on Internet Monitoring and Protection (ICIMP 2012), Stuttgart, IARIA, 2012 (im Druck).

[151] Wendzel, S.: Covert and Side Channels in Buildings and the Prototype of a Building-aware Active Warden, In Proc. 1st IEEE International Workshop on Security and Forensics in Communication Systems (SFCS 2012), Ottawa, IEEE, 2012 (im Druck).

[152] Whistel, L., Turner, R.: A Context-Based Approach to Detecting Miscreant Behavior and Collusion in Open Multiagent Systems, in Proc. CONTEXT 2011, LNAI 6967, S. 300–306, Springer, 2011.

[153] Williams, N., Zander, S., Armitage, G.: A preliminary performance comparison of five machine learning algorithms for practical IP traffic flow classification, ACM SIGCOMM Computer Communications Review, Volume 36, Issue 5, Seiten 5–16, October 2006.

[154] Wolf, M.: Covert channels in LAN protocols, in: Local Area Network Security, LNCS 396, Seiten 89–101, 1989.

[155] Wong, A.C.W., So, A.T.P.: Building automation in the 21st century, In Proc. Fourth International Conference on Advances in Power System Control, Operation and Management, Seiten 819–824, 1997.

[156] Wonnemann, C., Accorsi, R., Müller, G.: On Information Flow Forensics in Business Application Scenarios, 4th IEEE Workshop on Security, Trust, and Privacy for Software Applications, IEEE Computer Press, Seiten 324–328, 2009.

[157] Wray, J. C.: An Analysis of Covert Timing Channels, 1991 Symposium on Security and Privacy, IEEE Computer Society, Seiten 2–7, 1991.

[158] Yarochkin, F. V., Dai, S.-Y. et al.: Towards Adaptive Covert Communication System, In Proc. PRDC, pp. 153-159, 2008.

[159] Zander, S., Armitage, G. und Branch, P.: Covert Channels in the IP Time To Live Field, Centre for Advanced Internet Architectures (Swinburne University of Technology), Dezember 2006.

[160] Zander, S., Armitage, G., Branch, P.: Covert Channels and Countermeasures in Computer Networks, IEEE Communications Magazine, Seiten 136–142, December 2007.

[161] Zander, S., Armitage, G.: CCHEF – Covert Channels Evaluation Framework. Design and Implementation, Centre for Advanced Internet Architectures, Technical Report 080530A, Swinburne University of Technology, Mai 2008.

[162] Zander, S.: CCHEF – Covert Channels Evaluation Framework User Manual, Version 0.1, Mai 2008.

[163] Zander, S.: Performance of Selected Noisy Covert Channels and Their Countermeasures in IP Networks, Ph.D. Thesis, Centre for Advanced Internet Architectures, Faculty of Information and Communication Technologies, Swinburne University of Technology, Melbourne, May, 2010.

Sachverzeichnis