



Contents

1	General Information	2
1.1	Contact	2
1.2	Brief Biography	2
1.3	Education and Employment History	2
1.4	Honors and Awards	2
2	Research	3
2.1	Publications	3
2.2	Software Systems	9
2.3	Talks and Panels	10
2.4	Funding	12
3	Teaching	14
3.1	Teaching at Purdue University	14
3.2	Teaching at UCLA	14
3.3	Teaching at the University of Denver	14
3.4	Teaching at Technische Universität München	15
3.5	Theses supervision	15
4	Service	16
4.1	Service to BUGH Wuppertal	16
4.2	Service to Purdue University	16
4.3	Service to the University of Denver	16
4.4	Service to the Technische Universität München	17
4.5	Reviews	17
4.6	Conferences	18

1 General Information

1.1 Contact

Inria DÉCENTRALISÉ	<code>christian@grothoff.org</code>
Inria Rennes Bretagne Atlantique	<code>http://grothoff.org/christian/</code>
263 Avenue du General Leclerc	Phone (priv): +33-2-99-38-26-03
Campus Universitaire de Beaulieu	Phone (work): +33-2-99-84-71-45
F-35042 Rennes Cedex	Fax (work): +33-2-99-84-71-71
France	

1.2 Brief Biography

Christian Grothoff is leading the DÉCENTRALISÉ research team at Inria Rennes researching future Internet architectures to shelter us from state-sponsored criminals performing human rights violations at scale. He is also an independent investigative journalist for The Intercept, Heise and Der Spiegel, reporting on mass surveillance and Internet espionage. Previously, he was on the faculty of the Technische Universität München leading an Emmy-Noether research group in the area of computer networks. He earned his PhD in computer science from UCLA, an M.S. in computer science from Purdue University, and both a Diplom II in mathematics and the first Staatsexamen in chemistry from the Bergische Universität Gesamthochschule (BUGH) Wuppertal. His research interests include compilers, programming languages, software engineering, networking and security.

1.3 Education and Employment History

1996–2000	Diplom II (\approx M.S) in mathematics at BUGH Wuppertal
1996–2001	1. Staatsexamen (\approx B.S.) in chemistry at BUGH Wuppertal
2000–2003	M.S. in CS at Purdue University, West Lafayette, IN
2000–2005	PhD student in CS at Purdue University, West Lafayette, IN
2005–2006	PhD student in CS at UCLA, CA
2006–2009	Assistant Professor in CS at the University of Denver, CO
2008–2009	Joint appointment in ECE at the University of Denver, CO
2009–2014	Emmy Noether research group leader at TU München
2014	Independent Journalist for Heise, The Intercept, Der Spiegel
2014–	DÉCENTRALISÉ Research Team leader at Inria Rennes

1.4 Honors and Awards

1998–2000	Kurt-Hansen Fellowship
2000	DAAD Fellowship
2000–2001	Barmenia Award for best graduates in mathematics
2002	Upsilon Pi Epsilon Honor Society (Purdue)
2009–2014	DFG Emmy Noether Award

2 Research

2.1 Publications

h-index: 16, *g*-index: 33 (according to Arnet Miner, based on 32 publications).

References

Refereed Journal Articles

- [1] Christian Grothoff. “An Excess-Based Economic Model for Resource Allocation in Peer-to-Peer Networks”. *Wirtschaftsinformatik*, 3-2003, pages 285–292, June 2003 (30% accepted).
- [2] Krzysztof Palacz, Jason Baker, Chapman Flack, Christian Grothoff, Hiroshi Yamauchi, Jan Vitek “Engineering a Customizable Intermediate Representation”. *Science of Computer Programming*, Volume 57 Issue 3, pages 357–378. Elsevier 2005
(supercedes “Engineering a Customizable Intermediate Representation” in the *Proceedings of the ACM SIGPLAN Workshop on Interpreters, Virtual Machines and Emulators, (IVME’03)*, pages 1–12. ACM SIGPLAN, 2003 (19% accepted)).
- [3] Christian Grothoff, Jens Palsberg, and Jan Vitek. “Encapsulating objects with confined types”. *ACM Transactions on Programming Languages and Systems*, Volume 29 Issue 6. ACM Press, 2007
(supercedes “Encapsulating objects with confined types” in the *Proceedings of the 16th ACM SIGPLAN conference on Object-oriented programming, systems, languages, and applications (OOPSLA 2001)*, pages 241–253. ACM SIGPLAN, 2001 (19% accepted)).
- [4] Christian Grothoff. “The Runabout”. In *Software Practice and Experience*, Volume 38, pages 1531–1560. Wiley InterScience, 2008
(supercedes “Walkabout revisited: The runabout”. in *Proceedings of the European Conference on Object-oriented Programming (ECOOP 2003)*, pages 103–125. Springer-Verlag (LNCS 2743), 2003 (20% accepted)).
- [5] Christian Grothoff, Krista Grothoff, Ludmila Alkhutova, Ryan Stutsman, and Mikhail Atallah. “Lost In Translation”. In *Journal of Computer Security*, Volume 17 Issue 3, pages 269–304, IOS Press, 2009 (9% accepted)
(supercedes “Translation-based steganography” in *Proceedings of the Information Hiding Workshop (IH 2005)*, pages 219–233. Springer-Verlag, 2005 (31% accepted) and “Lost in Just the Translation” in

Proceedings of the 2006 ACM Symposium on Applied Computing, pages 338–345, ACM, 2006 (19% accepted)).

- [6] Kai Christian Bader, Christian Grothoff, and Harald Meier “Comprehensive and relaxed search for oligonucleotide signatures in hierarchically-clustered sequence datasets”. In *Bioinformatics*, pages 1546–1554, Oxford University Press, 2011 27(11).
- [7] Kai Christian Bader, Mikhail J. Atallah, and Christian Grothoff “Efficient Relaxed Search in Hierarchically-Clustered Sequence Datasets”. In *ACM Journal of Experimental Algorithmics*, Vol. 17, No. 1, Article 1.4, June 2012.

Refereed Conference Papers

The following papers are *not* preliminary versions of the journal articles listed above.

- [8] Krista Bennett, Christian Grothoff, Tzvetan Horozov, and Ioana Patrascu. “Efficient Sharing of Encrypted Data”. In *Proceedings of the 7th Australasian Conference on Information Security and Privacy (ACISP 2002)*, pages 107–120. Springer-Verlag (LNCS 2384), 2002 (38% accepted).
- [9] Krista Bennett and Christian Grothoff. “gap — Practical Anonymous Networking”. In *Designing Privacy Enhancing Technologies (PET 2003)*, pages 141–160. Springer-Verlag (LNCS 2760), 2003 (27% accepted).
- [10] Ronaldo A. Ferreira and Christian Grothoff and Paul Ruth. “A Transport Layer Abstraction for Peer-to-Peer Networks”. In *Proceedings of the 3rd International Symposium on Cluster Computing and the Grid (GRID 2003)*, pages 398–403. IEEE Computer Society, 2003 (48% accepted).
- [11] Neil Glew, Jens Palsberg, and Christian Grothoff. “Type-safe optimisation of plugin architectures”. In *Proceedings of the Static Analysis Symposium (SAS’05)*, pages 135–154. Springer Verlag (LNCS 3672), 2005 (34% accepted).
- [12] Philippe Charles, Christopher Donawa, Kemal Ebcioglu, Christian Grothoff, Allan Kielstra, Vivek Sarkar, and Christoph Von Praun. “X10: An object-oriented approach to non-uniform cluster computing”. In *Proceedings of the 20th ACM SIGPLAN conference on Object-oriented programming, systems, languages, and applications (OOPSLA 2005)*. ACM SIGPLAN, pages 519–538, 2005 (18% accepted).

- [13] Mangala Gowri, Christian Grothoff, and Satish Chandra. “Deriving object typestates in the presence of inter-object references”. In *Proceedings of the 20th ACM SIGPLAN conference on Object-oriented programming, systems, languages, and applications (OOPSLA 2005)*. ACM SIGPLAN, pages 77–96, 2005 (18% accepted).
- [14] Rajkishore Barik, Christian Grothoff, Rahul Gupta and Vinayaka Pandit. “Optimal Bitwise Register Allocation using Integer Linear Programming”. In *Languages and Compilers for High Performance Computing, 19th International Workshop, LCPC 2006*. Springer Verlag, pages 267–282, 2006.
- [15] Nathan S. Evans, Chris GauthierDickey and Christian Grothoff. “Routing in the Dark: Pitch Black”. In *23rd Annual Computer Security Applications Conference (ACSAC 2007)*. IEEE Computer Society, pages 305–314, 2007 (22% accepted).
- [16] Chris GauthierDickey and Christian Grothoff. “Bootstrapping of Peer-to-Peer Networks”. In *International Workshop on Dependable and Sustainable Peer-to-Peer Systems (DAS-P2P 2008)*. IEEE Computer Society, pages 205–208, 2008 (47% accepted).
- [17] Nathaniel Nystrom, Vijay Saraswat, Jens Palsberg and Christian Grothoff. “Constrained Types for Object-Oriented Languages”. In *Proceedings of the 23rd ACM SIGPLAN conference on Object-oriented programming, systems, languages, and applications (OOPSLA 2008)*. ACM SIGPLAN, 2008 (28% accepted).
- [18] Nathan S. Evans, Roger Dingledine and Christian Grothoff. “A Practical Congestion Attack on Tor Using Long Paths”. In *Proceedings of the 18th USENIX Security Symposium (USENIX Security '09)*. USENIX Association, pages 33–50, 2009 (15% accepted).
- [19] Nathan S. Evans, Chris GauthierDickey, Christian Grothoff, Krista Grothoff, Jeff Keene and Matthew J. Rutherford. “Simplifying Parallel and Distributed Simulation with the DUP System”. In *Proceedings 43rd Annual Simulation Symposium (ANSS-43 2010)*. Society for Modeling & Simulation International, pages 208–215, 2010.
- [20] Kai Christian Bader, Tilo Eißler, Nathan Evans, Chris GauthierDickey, Christian Grothoff, Krista Grothoff, Jeff Keene, Harald Meier, Craig Ritzdorf and Matthew J. Rutherford. “DUP: A Distributed Stream Processing Language”. In *IFIP International Conference on Network and Parallel Computing (NPC 2010)*, pages 232–246, 2010 (26% accepted).

- [21] Andreas Müller, Nathan Evans, Christian Grothoff and Samy Kamkar. “Autonomous NAT Traversal”. In *10th IEEE International Conference on Peer-to-Peer Computing (IEEE P2P 2010)*, pages 61–64, 2010 (23% accepted).
- [22] Christian Grothoff. “The Free Secure Network Systems Group: Secure Peer-to-Peer Networking and Beyond”. In *Proceedings of the First SysSec Workshop (SysSec 2011)*, pages 55–56, 2011 (69% accepted).
- [23] Michael Herrmann and Christian Grothoff. “Privacy-Implications of Performance-Based Peer Selection by Onion-Routers: A Real-World Case Study using I2P”. In *Privacy Enhancing Technologies Symposium (PETS 2011)*, pages 155–174, 2011 (24% accepted).
- [24] Nathan Evans and Christian Grothoff. “Beyond Simulation: Large-Scale Distributed Emulation of P2P Protocols”. In *4th Workshop on Cyber Security Experimentation and Test (CSET ’11)*, http://www.usenix.org/events/cset11/tech/final_files/Evans.pdf, 2011 (40% accepted).
- [25] Nathan Evans and Christian Grothoff. “ R^5N : Randomized Recursive Routing for Restricted-Route Networks”. In *5th International Conference on Network and System Security (NSS 2011)*, pages 316–321, 2011 (42% accepted).
- [26] Nathan Evans, Bart Polot and Christian Grothoff. “Efficient and Secure Decentralized Network Size Estimation”. In *IFIP International Conference on Networking (Networking 2012)*, pages 304–317, 2012 (28% accepted).
- [27] Matthias Wachs, Christian Grothoff and Ramakrishna Thurimella. “Partitioning the Internet”. In *7th International Conference on Risks and Security of Internet and Systems (CRISIS 2012)*, pages 1–8, 2012 (35% accepted).
- [28] Matthias Wachs, Martin Schanzenbach and Christian Grothoff. “On the Feasibility of a Censorship Resistant Decentralized Name System”. In *6th International Symposium on Foundations & Practice of Security (FPS 2013)*, 2013.
- [29] Christian Grothoff, Bart Polot and Carlo von Loesch. “The Internet is Broken: Idealistic Ideas for Building a NEWGNU Network”. In *W3C/IAB Workshop on Strengthening the Internet Against Pervasive Monitoring (STRINT)*, 2014.
- [30] Bart Polot and Christian Grothoff. “CADET: Confidential Ad-hoc Decentralized End-to-End Transport”. In *13th IEEE IFIP Annual Mediterranean Ad Hoc Networking Workshop (MedHocNet)*, 2014.

- [31] Alejandra Morales Ruiz, Wilfried Daniels, Danny Hughes and Christian Grothoff. “Cryogenic: Enabling Power-Aware Applications on Linux”. In *2nd International Conference on ICT for Sustainability (ICT4S)*, 2014 (49% accepted).
- [32] Matthias Wachs, Fabian Oelmann and Christian Grothoff. “Automatic Selection and Resource Allocation for Resilient Communication in Decentralized Networks”. In *IEEE International Conference on Peer-to-Peer Computing (P2P)*, 2014.
- [33] Matthias Wachs, Martin Schanzenbach and Christian Grothoff. “A Censorship-Resistant, Privacy-Enhancing and Fully Decentralized Name System”. In *13th International Conference on Cryptology and Network Security (CANS)*, pages 127–142. Springer Verlag (LNCS 8813), 2014 (29% accepted).

Non Peer-Reviewed Publications

- [34] Christian Grothoff. “Turbo Vision: Bug in Outline”. *DOS International* 7’95, page 169. DMV Daten- und Medien-Verlag Poing, July 1995.
- [35] Christian Grothoff. “Ein Stethoskop für die CPU”. *DOS International* 11’96, pages 272–273. DMV Daten- und Medien-Verlag Feldkirchen, November 1996.
- [36] Christian Grothoff. “Schwerpunkt: Ökologische Steuerreform”. In *Hochschul Umwelt Info (HUI) 2’96*, pages 18-28. Bundeskoordination Studentischer Ökologearbeit (BSÖ), 1996.
- [37] Dr. Martin Rocholl et al. “Ökologische Steuerreform, Positionspapier des deutschen Naturschutzrings (DNR)”. *Koordinationsstelle DNR-Projekt Ökologische Finanzreform*, June 1997.
- [38] Christian Grothoff. “Ein Kombinatorisches Standortproblem”. *Diplomarbeit, Fachbereich Mathematik, BUGH Wuppertal*, 2000.
- [39] Christian Grothoff. “Recycling Garbage Theory”. *Purdue University, CSD TR#04-012*, 2004.
- [40] Christian Grothoff. “Reading File Metadata with extract and libextractor”. In *LinuxJournal* 6’2005, pages 86–88. SSC Publishing, 2005.
- [41] Christian Grothoff. “Expressive Type Systems for Object-Oriented Languages”. *PhD Thesis, University of California, Los Angeles*, 2006.
- [42] Andrew Hunt and Christian Grothoff. “Multiple Vulnerabilities in Pidgin” CRISP Security Advisory 2007-1.

- [43] Nils Durner, Nathan Evans and Christian Grothoff. “Vielleicht anonym? Die Enttarnung von StealthNet-Nutzern.” In *c’t magazin für computer technik* 31’2007, pages 218–221. Heise Zeitschriften Verlag, 2007 (circulation: \approx 400,000).
- [44] Nils Durner and Christian Grothoff. “Vulnerability in Subversion” CRISP Security Advisory 2007-2.
- [45] Nils Durner, Nathan Evans and Christian Grothoff. “Anonymisierende Peer-to-Peer-Netze im Überblick” In *iX magazin für professionelle informationstechnik* 9’2008, pages 88–94. Heise Zeitschriften Verlag, 2008 (circulation: \approx 50,000).
- [46] Christian Grothoff. “URIs do not refer to unique files in Allmydata Tahoe” CRISP Security Advisory 2008-1.
- [47] Nils Durner, Nathan Evans and Christian Grothoff. “Unerkannt im Internet” In *iX special: Sicher im Netz* 10’2008, pages 42–49. Heise Zeitschriften Verlag, 2008.
- [48] Christian Grothoff. “Decentralized Open Network Services for a Resilient Economy and Free Society” In *FP8 Expert Group: Services in the future Internet*, European Commission, 2011 (invited).
- [49] Bart Polot and Christian Grothoff. “Performance Regression Monitoring with Gauger”. In *LinuxJournal* 9’2011, pages 68–75. SSC Publishing, 2011.
- [50] Christian Grothoff “A Benchmark for HTTP 2.0 Header Compression.” presented at *HTTPBIS WG (IETF 87)*, 2013.
- [51] Christian Grothoff, Matthias Wachs, Hellekin Wolf and Jacob Appelbaum. “Special-Use Domain Name of Peer-to-Peer Name Systems” submitted as draft-grothoff-iesg-special-use-p2p-names-00 to IETF.
- [52] Julian Kirsch, Christian Grothoff, Monika Ermert, Jacob Appelbaum, Laura Poitras and Henrik Moltke. “NSA/GCHQ: Das HACIENDA-Programm zur Kolonisierung des Internet” In *Heise Online* 8’2014. Heise Zeitschriften Verlag, 2014.
- [53] Julian Kirsch, Christian Grothoff, Monika Ermert, Jacob Appelbaum, Laura Poitras and Henrik Moltke. “NSA/GCHQ: The HACIENDA-Programm for Internet Colonization” In *Heise Online* 8’2014. Heise Zeitschriften Verlag, 2014.
- [54] Julian Kirsch, Christian Grothoff, Jacob Appelbaum and Holger Kenn. “TCP Stealth” submitted as draft-kirsch-iesg-tcp-stealth-00 to IETF.

- [55] Laura Poitras, Marcel Rosenbach, Michael Sontheimer, Holger Stark, Andy Müller-Maguhn and Christian Grothoff. “Map of the Stars: The NSA and GCHQ Campaign Against German Satellite Companies” In *The Intercept*. 14.9.2014, First Look Media, 2014.
- [56] Andy Müller-Maguhn, Laura Poitras, Marcel Rosenbach, Michael Sontheimer and Christian Grothoff. “Treasure Map: The NSA Breach of Telekom and Other German Firms” In *Spiegel Online International*. 14.9.2014, Spiegel-Verlag, 2014.
- [57] Judith Horchert, Christian Grothoff and Christian Stöcker. “NSA-System Treasuremap: “Jedes Gerät, überall, jederzeit” In *Spiegel Online Netzwelt*. 17.9.2014, Spiegel-Verlag, 2014.

2.2 Software Systems

I am the primary author of each of the applications and tools listed below. The systems are available from their respective webpages which are all linked from <http://grothoff.org/christian/>.

GNUnet

GNUnet is a framework for secure peer-to-peer networking that does not use any centralized or otherwise trusted services. A first service implemented on top of the networking layer allows anonymous censorship-resistant file-sharing. GNUnet uses a simple, excess-based economic model to allocate resources. Peers in GNUnet monitor each others behavior with respect to resource usage; peers that contribute to the network are rewarded with better service.

GNUnet is part of the GNU project. The codebase consists of about 350,000 lines of C code, developed with contributions from over 30 developers worldwide.

GNU libextractor

GNU libextractor is a library used to extract meta-data from files of arbitrary type. It is designed to use plugins that perform the actual extraction. The goal is to provide developers of file-sharing networks and search tools with a universal library to obtain metadata and keywords to match against queries. *libextractor* consists of more than 35,000 lines of C and C++ code with bindings to Java, Perl, Python and PHP.

GNU libmicrohttpd

GNU libmicrohttpd is a library providing a simple, high-level abstraction for implementing HTTP servers. The focus of the project is to provide a

compact, secure, reentrant, HTTP 1.1 compliant and easy to use implementation. In September 2012, GNU libmicrohttpd ranked in the top five out of over 500 “HTTP Server”-related projects in terms of popularity in the <http://freecode.com> database.

2.3 Talks and Panels

2002 DefCon 10, on “GNUnet”

2002 Midwest Society for Programming Languages and Systems, on “The Runabout”

2004 Privacy Enhancing Technologies (PET) Workshop, on “Mix Cascades vs. Peer-to-Peer: Is One Concept Superior?” (Panel)

2005 Linux User Group (LUG) Camp, on “libextractor and GNUnet”

2005 DefCon 13, on “Lost in Translation”

2005 Southern California Workshop on Programming Languages and Systems, on “A Type System for Distributed Arrays”

2006 Front Range Information Security Conference (FRISC), on “Lost in Translation”

2006 International Conference on Object Oriented Programming, Systems Languages and Applications (OOPSLA), on “Young Guns/OO: The Next Generation” (Panel)

2007 DefCon 14, on “Routing in the Dark: Pitch Black”

2008 Rocky Mountain IPv6 Summit, on “Migrating Code to IPv6”

2008 University of Helsinki, on “Secure File-Sharing in the GNUnet Peer-to-Peer Framework”

2008 DefCon 15, on “De-Tor-iorate Anonymity”

2008 University of Dortmund, on “Secure File-Sharing in the GNUnet Peer-to-Peer Framework”

2008 University of Darmstadt, on “Secure File-Sharing in the GNUnet Peer-to-Peer Framework”

2008 Information Technology Study Group (ITSG) Fall Workshop, on “Anonymity” (Panel)

2008 University of California Los Angeles (UCLA), on “The DUP System”

- 2009** University of Mainz, on
“Towards Productive Parallel Programming”
- 2009** Front Range Architecture Compilers Tools And Languages (FRAC-
TAL) Workshop, on
“Productive Parallel Programming for the Masses”
- 2009** Fórum Internacional do Software Livre, on
“Free Software for Privacy” (Keynote)
- 2009** Fórum Internacional do Software Livre, on
“The GNUnet Peer-to-Peer Framework”
- 2009** Fórum Internacional do Software Livre, on
“Tor and GNUnet: The Future of Internet Privacy” (Panel)
- 2010** GI-Beirat der Universitätsprofessoren, on
“Fast Primer Search with DUP”
- 2010** Linux User Group (LUG) Camp, on
“Spas mit paralleler und verteilter Programmierung”
- 2010** Linux User Group (LUG) Camp, on “ARM statt INIT”
- 2010** University of Wuppertal, on
“Distributed Stream Processing with the DUP System”
- 2010** GNU Hacker Meeting (GHM), on
“The GNUnet Peer-to-Peer framework”
- 2012** Linux User Group (LUG) Camp, on “tlsdate”
- 2012** GNU Hacker Meeting (GHM), on “A Quick Introduction to GNU
libmicrohttpd”
- 2013** Linux User Group (LUG) Camp, on “GNU libmicrohttpd”
- 2013** Gulasch Programmier Nacht (GPN), on “GNU libmicrohttpd”
- 2013** University of Amsterdam, on “PRISM and an Agenda for European
Network Security Research”
- 2013** IETF 87, on “A Benchmark for HTTP 2.0 Header Compression”
- 2013** Piratenpartei Berlin, on “Tools for Breaking out of PRISM”
- 2013** GNU Hacker Meeting (GHM), on “The GNU Name System and the
Future of Social Networking with GNUnet”
- 2013** IRILL Paris, on “PRISM and an Agenda for European Network Se-
curity Research”

- 2013** IRISA Rennes, on “Components for Building Secure Decentralized Networks”
- 2013** 30c3, on “The GNU Name System”
- 2013** 30c3 YBTI Assembly, on “Secure Name Systems” (Panel)
- 2014** DAAD Alumni Meeting, on “A Public Key Infrastructure for Social Movements in the Age of Universal Surveillance”
- 2014** MPI SWS, on “Components for Building Secure Decentralized Networks”
- 2014** Council of Europe, on “After Snowden: using law and technology to counter snooping” (Panel)
- 2014** University of Oxford, on “A Public Key Infrastructure for Social Movements in the Age of Universal Surveillance”
- 2014** GNU Hacker Meeting (GHM), on “The GNU Name System (updated)”
- 2014** Dagstuhl (Privacy and Security in an Age of Surveillance), on “We fix the Net!”
- 2014** Free Open Source Software for Academia (fOSSa 2014), on “Taler: Taxable Anonymous Libre Electronic Reserves”
- 2014** Inria/DGA Formal methods and security seminar, on “Décentralisé NOW!”

2.4 Funding

- NSF 0416969 “Curriculum Development Initiative in Cyber Trust at the University of Denver” (co-PI, \$296,831). The primary goal of this grant was to establish a computer security center at the University of Denver. As part of his work on the grant, I helped establish the Colorado Research Institute for Security and Privacy and obtain an NSA designation as a Center for Excellence in Information Assurance for the University of Denver. He also organized several regional conferences and workshops in the area of computer security. The award duration is from September 2004 to August 2009; I became a co-PI on this grant in August 2007.
- WIRED “Innovative Partnership for Job Creation and Employment” (co-PI, \$405,000). The goal of the computer science part of the grant was to establish a new course and certificate program in mainframe administration at the University of Denver and to provide scholarships

for underemployed IT administrators and programmers to help them obtain a certification as mainframe administrators. I was responsible for the computer science portion, which is also supported by IBM with software and equipment valued at approximately \$5,000,000. The program started July 2008 and ended December 2009. In January 2010 IBM announced that one of the scholarship recipients who participated in my Mainframe course won IBM's Master of the Mainframe Contest (1st out of over 3,000 contestants).

- nlnet “Fast and Resilient Routing for GUNet” (PI, \$33,901). The goal of the proposed work was to design and implement a secure P2P routing protocol that will achieve availability and scalability without infringing on the openness of the network. The design targets fully-decentralized, restricted-route networks with malicious participants. The project started January 2009 and ended December 2009 culminating in the GUNet 0.8.1 release which contains a prototype of such an algorithm.
- United States Department of Defense (DoD) Information Assurance Scholarship Program (IASP) Grant (PI, \$2,280 plus option for up to \$354,352). Under this grant, the DoD will fund up to 10 graduate students from the National Defense University to study information security at the University of Denver. The program started July 2009 and ends June 2010. Funding started after I left the US for Technische Universität München; the project was handed over to my co-PI.
- NSF “Collaborative-Research: A Partnership for Developing the IA Workforce”. The goal of this grant is to help the University of the District of Columbia build a quality program in information assurance (co-PI, \$299,978). Funding started after I left the US for Technische Universität München; the project was handed over to another co-PI.
- Deutsche Forschungsgesellschaft “Secure Randomized Peer-to-Peer Routing Protocols” (PI, €1,305,200). This project is about the design, analysis and implementation of new secure and efficient routing protocols for open heterogeneous networks. Funded from September 2009 until August 2014.
- Cloudmark Inc. (\$5,000). Unrestricted gift to lab in appreciation of our work on GNU libmicrohttpd (2010).
- FP7 “OpenLab-Eclectic” (PI, €123,334). This project is about improving tools for resource allocation, execution and observation of experiments in network testbeds (2013-2014, 9 months).

- The Renewable Freedom Foundation “GNUnet” (PI, € 300,000). The goal of the proposed research and development effort is to use cryptography, network protocol design and secure software engineering to build the GNUnet, a fully decentralized secure global network that respects user freedoms, providing users with a free networking platform that protects their privacy in both economic and social contexts and provides them with a neutral, censorship-resistant news distribution mechanism to facilitate informed democratic decision-making processes. Funding started in October 2014 and has been approved for 36 months.

3 Teaching

3.1 Teaching at Purdue University

- Teaching Assistant for “Software Engineering” (graduate level)
- Teaching Assistant for “Programming Languages” (graduate level)

3.2 Teaching at UCLA

- Teaching Assistant for Compilers (undergraduate level)

3.3 Teaching at the University of Denver

- Instructor for “Compilers” (graduate level)
- Instructor for “Computer Security” (graduate level, 2x)
- Instructor for “Computer Security from a Free Software Perspective” (freshmen seminar, non-majors)
- Instructor for “Distributed Stream Processing” (graduate level)
- Instructor for “Introduction to Systems Programming” (undergraduate level)
- Instructor for “Mainframe Administration” (undergraduate, graduate and non-traditional students)
- Instructor for “Programming Languages” (both undergraduate and graduate students, 3x)
- Instructor for “UNIX tools” (undergraduate level)

3.4 Teaching at Technische Universität München

- Co-Instructor for “Masterkurs Rechnernetze” (graduate level)
- Instructor for “Peer-to-Peer Systems and Security” (graduate level)

3.5 Theses supervision

I was the primary advisor for the following theses:

- Nathan Evans: “Routing in the Dark: Pitch Black” (MS, 2009)
- Michael Herrmann: “Privacy-Implications of Performance-Based Peer Selection by Onion-Routers: A Real-World Case Study using I2P” (MS, 2011)
- Nathan Evans: “Methods for Secure Decentralized Routing in Open Networks” (PhD, 2011)
- Safey A. Halim: “Monkey: Automated debugging of deployed distributed systems” (MS, 2012)
- Martin Schanzenbach: “Design and Implementation of a Censorship Resistant and Fully Decentralized Naming System” (MS, 2012)
- Maximilian Szengel: “Distributed Evaluation of Policies for Group Management in Mesh Networks” (MS, 2012)
- Kai C. Bader: “High-performance approaches to the comprehensive computation and evaluation of signatures in bacterial sequence datasets” (PhD, 2013)
- Markus Teich: “Monkey - Generating Useful Bug Reports Automatically” (BS, 2013)
- Gabor X. Toth: “Design of a Social Messaging System Using Stateful Multicast” (MS, 2013)
- Andrey Uzunov: “Speeding up Tor with SPDY” (MS, 2013)
- Alejandra Morales Ruiz: “Cryogenic: Enabling Power-Aware Applications on Linux” (MS, 2014)
- Julian Kirsch: “Improved Kernel-Based Port-Knocking in Linux” (MS, 2014)
- Florian Dold: “Cryptographically Secure, Distributed Electronic Voting” (BS, 2014)

- Supriti Singh: “Comparison of Byzantine fault-tolerant Distributed Hash Tables” (MS, 2014)
- Nicolas Benes: “An Approach for Home Routers to Securely Delete Sensitive Data” (BS, 2014)

4 Service

4.1 Service to BUGH Wuppertal

I was a member of the student representation (AStA) at the BUGH Wuppertal. He served for four years in the office for ecologics and later also as volunteer system administrator for 50 users.

4.2 Service to Purdue University

I served for one year on the graduate student board, and represented the graduate students on the faculty graduate committee for the computer science department.

4.3 Service to the University of Denver

I served as associate director of the DU nanotechnology center and was a senior academic analyst for the Privacy Foundation. I was a founding faculty member for the Colorado Research Institute for Security and Privacy (CRISP), and also served as a member of the Steering Committee for the Rocky Mountain IPv6 Task Force.

- SECS PROF grant review committee (2006-2007)
- Establishment and administration of Subversion assignment submission system (2006-2008)
- Computer Science Facilities Committee (2006-2009)
- Dean’s Advisory Committee (2007-2008)
- University Technology Council (2007-2008)
- Faculty Search Committee (2007-2009)
- Nano-Technology Center Finance Committee (2008-2009)
- PhD Committee for J. Treinen (Advisor: R. Thurimella, 2009)

4.4 Service to the Technische Universität München

I participated in the FP8 Expert Group “Services in the future Internet” for the European Commission in 2011.

I organized five well-attended public talks with Mikhael Atallah (50+ attendees), Jacob Appelbaum (120+ attendees), Richard Stallman (850+ attendees), Roger Dingledine (400+ attendees) and Peter Schaar (250+ attendees).

4.5 Reviews

- ACM SIGPLAN Conference on Object-oriented Programming, Systems, Languages and Applications (OOPSLA)
- IEEE Conference on E-Commerce Technology (CEC)
- ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI)
- International Conference on Compiler Construction (CC)
- IEEE Transactions on Information Forensics and Security
- ACM Transactions on Programming Languages and Systems (TOPLAS)
- USENIX Security
- Journal of Information and Computation
- Journal of Systems and Software (Elsevier)
- Transactions on Aspect-Oriented Software Development
- Transactions on Data Hiding and Multimedia Security
- Information Hiding (IH)
- European Symposium on Programming (ESOP)
- X10 Workshop
- NSF Panel
- Netherlands Organization for Scientific Research
- Privacy Enhancing Technologies (PET)

4.6 Conferences

- 2007** Initiated and organized the Front Range Architecture Compilers Tools And Languages (FRACTAL) workshop series together with Sanjay Rajopadhye.
- 2007** Organized FRISC (Front Range Information Security Conference) together with Ramki Thurimella and Chris GauthierDickey
- 2008** Organized the Rocky Mountain IPv6 Summit together with the Rocky Mountain IPv6 Task Force
- 2008** DU Faculty Mentor for Computer And Network Vulnerability Assessment Simulation (CANVAS)
- 2008** Organized Front Range Architecture Compilers Tools And Languages (FRACTAL) workshop together with Manish Vachharajani
- 2009** Organized the Rocky Mountain IPv6 Summit together with the Rocky Mountain IPv6 Task Force
- 2009** Organized the PhD Symposium for the International Conference on Software Testing (ICST) together with the Jane Hayes and Atif Memon
- 2011** Program Committee member for 8th IFIP International Conference on Network and Parallel Computing (NPC 2011)
- 2013** Program Committee member for IFIP Networking 2013
- 2013** Local organizer for the Tor Hacker Meeting 2013 in Munich
- 2014** Local organizer for the GNU Hacker Meeting 2014 in Munich