

Contents

1	General Information	2
1.1	Personal	2
1.2	Brief Biography	2
1.3	Education	2
1.4	Honors	2
1.5	Professional Associations	3
2	Research	3
2.1	Research Summary	3
2.2	Publications	4
2.3	Software Systems	7
2.4	Talks and Panels	11
2.5	Funding	11
3	Teaching	11
3.1	Teaching in Wuppertal	11
3.2	Teaching at Purdue University	12
3.3	Teaching at UCLA	12
3.4	Teaching at DU	12
4	Service	12
4.1	Service to BUGH Wuppertal	12
4.2	Service to Purdue University	12
4.3	Service to the University of Denver	12
4.4	Reviews	13
4.5	Conferences	13

1 General Information

1.1 Personal

University of Denver	christian@grothoff.org
Department of Computer Science	http://grothoff.org/christian/
2360 S. Gaylord Street	Phone (priv): +1-720-363-0519
Denver, CO 80208-4310	Phone (work): +1-303-871-2453

Born February 28, 1977 in Germany. Citizen of Germany. Permanent Resident of the USA.

1.2 Brief Biography

Christian Grothoff is an assistant professor for computer science at the University of Denver, Colorado. 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

2008-	Joint appointment in ECE at the University of Denver, CO
2006-	Assistant Professor in CS at the University of Denver, CO
2005-2006	PhD student in CS at UCLA, CA
2000-2005	PhD student in CS at Purdue University, West Lafayette, IN
2000-2003	M.S. in CS at Purdue University, West Lafayette, IN
1996-2001	1. Staatsexamen (\approx B.S.) in chemistry at BUGH Wuppertal
1996-2000	Diplom II (\approx M.S) in mathematics at BUGH Wuppertal

1.4 Honors

2002	Upsilon Pi Epsilon Honor Society (Purdue)
2000	DAAD Fellowship
1999-2000	Delphi Automotive sponsored Thesis
1998-2000	Kurt-Hansen Fellowship

1.5 Professional Associations

Christian Grothoff is member of the Electronic Frontier Foundation, member of IEEE, associate member of the Free Software Foundation, and maintainer of two applications that are part of the GNU project.

2 Research

2.1 Research Summary

Grothoff’s research spans the areas of programming languages, compilers, software engineering, networking and security.

His doctoral dissertation explores practical extensions to type-systems in modern object-oriented languages that will help programmers to manage references. The use of references is pervasive in object-oriented software, but the imminent possibility of unexpected side-effects due to aliasing is a source of hard-to-find bugs. One approach to this problem is to limit aliasing to a certain scope, such as a Java package. He developed Kacheck/J [3], a tool that uses static type analysis to infer types such that it can be guaranteed that instances of a particular type will never be aliased from outside of its defining package. The tool can also report paths along which possible violations of this property may occur. Based on the constraints developed for Kacheck/J, other researchers have developed encapsulation checkers for Enterprise Java Beans (EJBs) and a programming discipline for memory scopes in real-time Java. Another possible source of errors is the confusion of local vs. remote references that can occur in languages with a non-uniform memory model, such as [10]. In particular, references to distributed arrays where the index determines the place at which the value is stored are difficult to manage. Grothoff’s dissertation develops a type system based on dependent types that allows the compiler to statically verify that accesses are local and within the bounds of distributed arrays.

Using the idea of hiding information in the noise inherent in natural language translation, Grothoff led a team to develop “Lost in Translation” (LiT), a natural language steganographic encoder [4]. LiT is unique in that the pervasiveness of errors in translation makes it plausible for a translation containing an embedded message to co-exist with the original cover text and even alternative translations.

Grothoff conceived, created and continues to maintain the GNUnet peer-to-peer framework. GNUnet is the first system that combines anonymity with economics. The GNUnet anonymity protocol (GAP) [7] provides a basis

on which to build an anonymous routing service using peers that have a vested interest in serving requests from other peers; this vested interest derives from the fact that serving other peers' requests is how they themselves gain anonymity. GNUnet also provides a novel censorship-resistant content encoding [6] which allows peers to verify the integrity of routed content without gaining information about queries or responses. This verification enables GNUnet to use an excess-based economy [1] to reward peers that contribute resources. GNUnet is an official GNU project, which Grothoff continues to maintain and extend in cooperation with a worldwide group of developers.

Grothoff developed the Runabout [5], a practical Java library that adds two-argument dispatch to Java without necessitating changes to the compiler or JVM. The Runabout achieves dispatching performance comparable to double dispatch by combining introspection with dynamic code generation. This key idea has since inspired other researchers to extend the approach, resulting in the development of Java libraries that support multi-argument dispatch and mixins.

Grothoff's master's thesis [20] in mathematics developed heuristics for a combinatorial location problem. The problem was to find a small number of cost-effective assembly plans that would also satisfy engineering requirements and the diverse requirements of a customer base. The problem originated from industry and the computed solutions provided significant economic benefits compared to existing practice, with savings amounting to millions of dollars.

2.2 Publications

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*, accepted. ACM Press, 2006 (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, Krista Grothoff, Ludmila Alkhutova, Ryan Stutsman, and Mikhail Atallah. “Lost In Translation”. In *Journal of Computer Security*, 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)).
- [5] Christian Grothoff. “The Runabout”. In *Software Practice and Experience*, accepted (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)).

Refereed Conference Papers

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

- [6] 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 (AS-CIP 2002)*, pages 107–120. Springer-Verlag (LNCS 2384), 2002 (38% accepted).
- [7] 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).
- [8] 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).
- [9] 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).
- [10] 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).
- [11] 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).
- [12] 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.
- [13] 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, 2007 (22% accepted).
- [14] Christian Grothoff, Chris GauthierDickey. “Bootstrapping of Peer-to-Peer Networks.” In *International Workshop on Dependable and Sustainable Peer-to-Peer Systems*, 2008 (accepted).
- [15] Chris GauthierDickey and Christian Grothoff. “Bootstrapping of Peer-to-Peer Networks”. In *International Workshop on Dependable and Sustainable Peer-to-Peer Systems (P2P-DAS 2007)*. IEEE Computer Society, 2008.

Other Papers

- [16] Christian Grothoff. “Turbo Vision: Bug in Outline”. *DOS International* 7’95, page 169. DMV Daten- und Medien-Verlag Poing, July 1995.
- [17] Christian Grothoff. “Ein Stethoskop für die CPU”. *DOS International* 11’96, pages 272–273. DMV Daten- und Medien-Verlag Feldkirchen, November 1996.
- [18] Christian Grothoff. “Schwerpunkt: Ökologische Steuerreform”. In *Hochschul Umwelt Info (HUI) 2’96*, pages 18-28. Bundeskoordination Studentischer Ökologearbeit (BSÖ), 1996.
- [19] Dr. Martin Rocholl et al. “Ökologische Steuerreform, Positionspapier des deutschen Naturschutzrings (DNR)”. *Koordinationsstelle DNR-Projekt Ökologische Finanzreform*, June 1997.
- [20] Christian Grothoff. “Ein Kombinatorisches Standortproblem”. *Diplomarbeit, Fachbereich Mathematik, BUGH Wuppertal*, 2000.
- [21] Christian Grothoff. “Recycling Garbage Theory”. *Purdue University, CSD TR#04-012*, 2004.
- [22] Christian Grothoff. “Reading File Metadata with extract and libextractor”. In *LinuxJournal* 6’2005, pages 86–88. SSC Publishing, 2005.
- [23] Christian Grothoff. “Expressive Type Systems for Object-Oriented Languages”. *PhD Thesis, University of California, Los Angeles*, 2006.
- [24] 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.

2.3 Software Systems

Unless otherwise noted, Christian Grothoff is the primary author of each of the applications and tools listed below.

doodle

Doodle is a desktop search engine based on suffix trees. The focus of the design is on low memory consumption and fast search. Doodle has been

integrated by other developers into Evidence, the file manager for the next-generation of the Enlightenment window manager.

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 130,000 lines of C code, developed with contributions from over 30 developers worldwide. The documentation is partially translated into 25 languages. GNUnet is currently ranked in the top 500 out of almost 40,000 software projects in terms of popularity in the *freshmeat.net* database. Grothoff has published four papers on GNUnet.

Hitsuji

Hitsuji is a framework for control flow analysis of large Java applications. The framework currently implements class hierarchy analysis, 0-CFA (using subsets or unification) and a type-safe variant of 0-CFA called TSMI (again using subsets or unification).

i18nHTML

i18nHTML is a collection of PHP files that can be used to write webpages that visitors can translate into their respective native languages. Webpages internationalized with i18nHTML can be updated without losing existing translations of sentences that were not changed.

Jamit

Jamit, the Java Access Modifier Inference Tool was originally written by Ted Witkamp and Vids Samanta under Grothoff's direction. Grothoff has since taken over maintenance of the codebase. Jamit infers the tightest access modifiers for Java code that will still allow the code to compile. The analysis is useful in increasing security, guiding the programmer to places where encapsulation could be increased, eliminating dead code, and possibly

allowing later analyses to perform additional optimizations based on the tighter access rules.

Kacheck/J

Kacheck/J is an encapsulation checker for Java. It infers which types are confined according to the definition given in [3]. Objects of confined type do not escape their enclosing package. The fact that references to objects of confined type are limited to their defining package can be useful in managing aliasing. Kacheck/J is the first kind of tool that performs this kind of type-checking or type-inference operation on extremely large codebases. For example, processing Eclipse (over 30,000 classes including JDK) can be performed in a couple of minutes on a modern machine.

GNU libextractor

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. *libextractor* is a GNU package. 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* currently supports the following formats: HTML, PDF, PS, OLE2 (DOC, XLS, PPT), OpenOffice (sxw), StarOffice (sdw), DVI, MAN, MP3 (ID3v1 and ID3v2), OGG, WAV, JPEG, EXIV2, GIF, PNG, TIFF, DEB, RPM, TAR(.GZ), ZIP, ELF, REAL, RIFF (AVI), MPEG, QT and ASF. *libextractor* consists of more than 80,000 lines of C and C++ code with bindings to Java, Perl, Python and PHP.

GNU libmicrohttpd

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. The initial design of the API was done together with Dr. GauthierDickey and given in his networking class as a course project. The first release used code produced by the students as a starting point. *libmicrohttpd* is a GNU package.

LiT

LiT, short for Lost in Translation, is a steganographic encoder written by Ryan Stutsman under supervision from Christian Grothoff. LiT hides infor-

mation in the noise that is inherent in natural language translation.

OVMM

OVMM is a real-time Java Virtual Machine developed over the course of over three years by a group at Purdue University. Christian Grothoff was involved in the design and development from the start and contributed to most parts of the system.

Runabout

The Runabout is an extension of the Java libraries that adds two-argument multi-dispatch to Java without changing the language or the VM. Like the Walkabout, the Runabout uses reflection to find visit methods. But instead of invoking the visit methods with reflection, the Runabout uses dynamic code generation to create code at runtime that will invoke the appropriate visit method. This puts the Runabout closer to MultiJava, a Java source compiler that compiles Java with multi-methods to ordinary Java bytecode. Unlike MultiJava, the Runabout runs when the application is executed, and not at compile time. Writing code with the Runabout is very similar to writing visitors or multi methods with MultiJava.

The dispatch in the Runabout is only about a factor of 3 slower than ordinary uni- or double dispatch (on Sun's JDK 1.4.1 for 10 million invocations) while saving huge amounts of trivial code and adding extensibility to the dispatch that could not be achieved otherwise. The original proposal has since spawned various successor projects by other researchers, including the Sprintabout and Poly/J.

X10

X10 is a new high-performance, high-productivity programming language developed by IBM research. Christian Grothoff is part of the core team that developed and continues to evolve the initial prototype compiler and virtual machine.

XTC

XTC is a fork of the OVMM codebase that focuses on delivering an extensible architecture for program analysis and compilation. It contains components

for basic bytecode operations (parsing, management and writing), an SSA-based intermediate representation, and a program analysis framework. XTC currently consists of about 85,000 lines of Java code.

2.4 Talks and Panels

- DefCon 10, on “GNUnet”
- MSPLS 2002, on “The Runabout”
- PET 2004, on “Mix Cascades vs. Peer-to-Peer: Is One Concept Superior?”
- LUG Camp 2005, on “libextractor and GNUnet”
- DefCon 13, on “Lost in Translation”
- SoCal 2005, on “A Type System for Distributed Arrays”
- DefCon 15, on “Routing in the Dark: Pitch Black”
- Rocky Mountain IPv6 Summit, on “Migrating Code to IPv6”

2.5 Funding

- NSF 0416969 “Curriculum Development Initiative in Cyber Trust (CDICT) at the University of Denver” (co-PI, \$296,831)
- WIRED “Innovative Partnership for Job Creation and Employment” (co-PI, \$405,000)

3 Teaching

3.1 Teaching in Wuppertal

- Introduction to networking (after-school program)
- Introduction to computer graphics (after-school program)
- Mathematics (teacher in training, secondary education)
- Chemistry (teacher in training, secondary education)

3.2 Teaching at Purdue University

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

3.3 Teaching at UCLA

- Teaching Assistant for Compilers (undergraduate level)

3.4 Teaching at DU

- Instructor for “Compilers” (graduate level)
- Instructor for “Computer Security” (graduate level)
- Instructor for “Computer Security from a Free Software Perspective” (freshmen seminar, non-majors)
- Instructor for “Programming Languages” (both undergraduate and graduate students)
- Instructor for “UNIX tools” (undergraduate level)

4 Service

4.1 Service to BUGH Wuppertal

Christian Grothoff was a member of the student government (AStA) at the BUGH Wuppertal. He served first in the office for ecologies and later as volunteer system administrator for 50 users.

4.2 Service to Purdue University

Christian Grothoff 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

- Computer Science Facilities Committee (2006-2008)
- Administration of Subversion assignment submission system (2006-2008)

- SECS PROF grant review committee (2006-2007)
- Dean's Advisory Committee (2007-2008)
- Faculty Search Committee (2007-2008)
- University Technology Council (2007-2008)

4.4 Reviews

- ACM SIGPLAN Conference on Object-oriented Programming, Systems, Languages and Applications (OOPSLA)
- ACM Transactions on Programming Languages and Systems (TOPLAS)
- IEEE Conference on E-Commerce Technology (CEC)
- ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI)
- IEEE Transactions on Information Forensics and Security
- Journal of Systems and Software (Elsevier)
- NSF Pannel

4.5 Conferences

- Initiated (with Sanjay Rajopadhye) FRACTAL (Front Range Architecture Compilers Tools And Languages) Workshop series. Co-organized first workshop with Sanjay Rajopadhye.
- Organized FRISC (Front Range Information Security Conference) 2007 (together with Ramki Thurimella and Chris GauthierDickey)
- Organized the Rocky Mountain IPv6 Summit 2008 (together with the Rocky Mountain IPv6 Task Force)
- DU Faculty Mentor for CANVAS (Computer And Network Vulnerability Assessment Simulation) 2008
- Local Organizer for the Rocky Mountain IPv6 Summit 2008 (with the Rocky Mountain IPv6 Task Force)
- Organized FRACTAL 2008 (Front Range Architecture Compilers Tools And Languages) with Manish Vachharajani